Álgebra Conmutativa Computacional

F. J. Lobillo

2019/2020

Capítulo 6

Dimensión

6.1 Dimensión de Krull

Definición 6.1. Sea $V \subseteq \mathbb{F}^n$ una variedad afín irreducible. Se define la dimensión de V como la longitud de la mayor cadena

$$V = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_m$$

de variedades irreducibles. La dimensión de una variedad afín es la mayor dimensión de las variedades irreducibles que aparecen en una descomposición como unión de variedades irreducibles. Es sencillo comprobar que no depende de la descomposición elegida.

Definición 6.2. La dimensión de Krull de un anillo conmutativo R se define como el supremo de las longitudes de cadenas de ideales primos en R. Si $I \subseteq R$ es un ideal, se define la dimensión de I como la dimensión de Krull de R/I. Es inmediato que dicha dimensión coincide con la mayor longitud de las cadenas de ideales primos que contienen a I.

Ejemplo 6.3. La siguiente cadena

$$\langle 0 \rangle \subsetneq \langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \cdots \subsetneq \langle x_1, x_2, \ldots, x_n \rangle$$

de ideales primos (comprobar) en $\mathbb{F}[x_1, \ldots, x_n]$ demuestra que la dimensión de Krull del anillo de polinomios sobre un cuerpo es al menos igual al número de variables.

Proposición 6.4. *Si $\mathbb{F}$ es algebraicamente cerrado, la dimensión de una variedad coincide con la dimensión del ideal asociado.*

Demostración. Consecuencia directa de las biyecciones entre variedades irreducibles e ideales primos. □

6.2 Dimensión de un ideal en $\mathbb{N}^n$

Dado un subconjunto $X \subseteq \mathbb{N}^n$, definimos:

$$T(X) = \{\sigma \subseteq \{1, \ldots, n\} \mid \sigma \cap \operatorname{supp}(\alpha) \neq \varnothing \quad \forall \alpha \in X\}.$$

Lema 6.5.

(1) $T(X) = \varnothing$ *si y solo si* $(0, \ldots, 0) \in X$.

(2) Si $\sigma_1 \in T(X)$ *y* $\sigma_1 \subseteq \sigma_2$ *entonces* $\sigma_2 \in T(X)$.

(3) Si $\sigma \in T(X_1)$ *y* $X_2 \subseteq X_1$ *entonces* $\sigma \in T(X_2)$.

Demostración. Si $(0, \ldots, 0) \notin X$ entonces $\{1, \ldots, n\} \in T(X)$, de lo que se deduce (1). Las demás son inmediatas. □

Proposición 6.6. *Sea* $E \subseteq \mathbb{N}^n$ *un ideal y sea* $\{\alpha^1, \ldots, \alpha^s\}$ *un conjunto de generadores de* E. *Entonces*

$$T(E) = T(\alpha^1, \ldots, \alpha^s).$$

Demostración. Dado que $\{\alpha^1, \ldots, \alpha^s\} \subseteq E$, por el Lema 6.5 tenemos la inclusión $T(E) \subseteq T(\alpha^1, \ldots, \alpha^s)$. Sea por tanto $\sigma \in T(\alpha^1, \ldots, \alpha^s)$ y supongamos que $\alpha \in T(E)$. Existen $i \in \{1, \ldots, s\}$ y $\beta \in \mathbb{N}^n$ tales que $\alpha = \alpha^i + \beta$. Es claro que $\operatorname{supp}(\alpha^i) \subseteq \operatorname{supp}(\alpha)$ y como $\sigma \cap \operatorname{supp}(\alpha^i) \neq \varnothing$ tenemos que $\sigma \cap \operatorname{supp}(\alpha) \neq \varnothing$. Como α es un elemento cualquiera tenemos que $\sigma \in T(E)$. □

Como consecuencia, si $E = \{\alpha^1, \ldots, \alpha^s\} + \mathbb{N}^n$,

$$T(E) = \{\sigma \subseteq \{1, \ldots, n\} \mid \sigma \cap \operatorname{supp}(\alpha^i) \neq \varnothing \quad \forall i \in \{1, \ldots, s\}\}.$$

Definición 6.7. Sea $E \subseteq \mathbb{N}^n$ un ideal. Definimos la *dimensión* de E como

$$\dim(E) = \begin{cases} n & \text{si } E = \varnothing, \\ 0 & \text{si } E = \mathbb{N}^n, \\ n - \min\{\#\sigma\,;\ \sigma \in T(E)\} & \text{en otro caso.} \end{cases}$$

Definición 6.8. Dado un ideal $E \subseteq \mathbb{N}^n$, se define la *función de Hilbert* de E como la aplicación

$$\begin{aligned} HF_E : \mathbb{N} &\longrightarrow \mathbb{N} \\ s &\longmapsto \#\{\alpha \in \mathbb{N}^n \setminus E\,;\ |\alpha| \leq s\}. \end{aligned}$$

Vamos a conectar función de Hilbert de un ideal $E \subseteq \mathbb{N}^n$ con su dimensión. Sea $m \in \mathbb{N}$ y $\alpha \in \mathbb{N}^n$. Definimos

$$\operatorname{top}_m(\alpha) = \{i \in \{1, \ldots, n\} \mid \alpha_i \geq m\}$$

es decir, los índices donde α supera a m. Definimos también la aplicación

$$\begin{aligned} \mathrm{sh}_m : \mathbb{N}^n &\longrightarrow \mathbb{N}^n \\ \alpha &\longmapsto \beta \text{ con } \begin{cases} \beta_i = m & i \in \mathrm{top}_m(\alpha), \\ \beta_i = \alpha_i & i \notin \mathrm{top}_m(\alpha). \end{cases} \end{aligned}$$

La aplicación anterior representa un "afeitado" de α al nivel m. Es claro que $\mathrm{sh}_m(\mathrm{sh}_m(\alpha)) = \mathrm{sh}_m(\alpha)$ y que $\mathrm{top}_m(\mathrm{sh}_m(\alpha)) = \mathrm{top}_m(\alpha)$. Definimos la siguiente relación de equivalencia sobre $\mathbb{N}^n$:

$$\alpha \sim_m \beta \iff \mathrm{sh}_m(\alpha) = \mathrm{sh}_m(\beta).$$

Lema 6.9. *Sean $m \in \mathbb{N}$ y $F \subseteq \mathbb{N}^n$ tales que para todo $\alpha \in F$, $\mathrm{sh}_m(\alpha) \in F$. Sea además*

$$R_m = \{\beta \in F \mid \mathrm{sh}_m(\beta) = \beta\} = \{\beta \in F \mid \beta_i \leq m, 1 \leq i \leq n\}.$$

Entonces,

(1) $F = \biguplus_{\alpha \in R_m} \left([\alpha]_m \cap F\right)$, donde $\uplus$ denota la unión disjunta y $[\alpha]_m$ es la clase de equivalencia de α respecto a $\sim_m$.

(2) Si $\alpha \in R_m$ entonces $[\alpha]_m \cap F = \{\alpha + \beta \in F \mid \beta_i = 0, \forall i \notin \mathrm{top}_m(\alpha)\}$.

Demostración. La primera parte es consecuencia de que una relación de equivalencia proporciona una partición, y la segunda un sencillo cálculo consecuencia de la definición de sh_m y $\sim_m$. □

Lema 6.10. *Sea* $E = \{\alpha^1, \dots, \alpha^t\} + \mathbb{N}^n$*, llamemos* $m = \max\{\alpha_i^j \mid 1 \leq j \leq t, 1 \leq i \leq n\}$ *y sea* $s \geq nm$*. Entonces*

$$\dim(E) = \max\{\#\operatorname{top}_m(\alpha)\ ;\ \alpha \in \mathbb{N}^n \setminus E, |\alpha| \leq s\}.$$

Demostración. Llamemos $F = \mathbb{N}^n \setminus E$ y $d = \dim(E)$. Supongamos que existe un elemento $\alpha \in F$ tal que $|\alpha| \leq s$ y $\#\operatorname{top}_m(\alpha) > d$. Podemos descomponer $\alpha = \beta + \gamma$ donde

$$\beta_i = \begin{cases} \alpha_i & \text{si } i \in \operatorname{top}_m(\alpha) \\ 0 & \text{si } i \notin \operatorname{top}_m(\alpha) \end{cases} \qquad \gamma_i = \begin{cases} 0 & \text{si } i \in \operatorname{top}_m(\alpha) \\ \alpha_i & \text{si } i \notin \operatorname{top}_m(\alpha) \end{cases}$$

Dado que $\alpha \notin E$ tenemos que $\beta, \gamma \notin E$. Además, tal y como se ha construido β tenemos que $\operatorname{supp}(\beta) = \operatorname{top}_m(\alpha)$. Sea $\sigma = \{1, \dots, n\} \setminus \operatorname{top}_m(\alpha)$. Si $\sigma \in T(E)$ entonces tenemos que $\dim(E) \geq n - |\sigma| = |\operatorname{top}_m(\alpha)| > \dim(E)$, luego $\sigma \notin T(E)$. Existe un índice k tal que $\sigma \cap \operatorname{supp}(\alpha^k) = \varnothing$, es decir, $\operatorname{supp}(\alpha^k) \subseteq \operatorname{top}_m(\alpha) = \operatorname{supp}(\beta)$. Para todo $i \in \operatorname{supp}(\alpha^k)$, tenemos que $\beta_i \geq m \geq \alpha_i^k$, de donde tenemos que $\beta \in E$, lo que es imposible. Hemos demostrado que

$$\max\{\#\operatorname{top}_m(\alpha)\ ;\ \alpha \in \mathbb{N}^n \setminus E, |\alpha| \leq s\} \leq \dim(E).$$

Veamos la otra desigualdad. Existe un $\sigma \in T(E)$ tal que $\#\sigma = n - d$. Consideremos el elemento $\alpha \in \mathbb{N}^n$ definido por

$$\alpha_i = \begin{cases} m & \text{si } i \notin \sigma, \\ 0 & \text{si } i \in \sigma. \end{cases}$$

Es evidente que $|\alpha| \leq s$ y que $\operatorname{supp}(\alpha) = \operatorname{top}_m(\alpha) = \{1, \dots, n\} \setminus \sigma$. Como $\sigma \in T(E)$, para todo $k \in \{1, \dots, t\}$, $\sigma \cap \operatorname{supp}(\alpha^k) \neq \varnothing$, es decir,

para todo k existe un $i_k \in \operatorname{supp}(\alpha^k)$ tal que $i_k \notin \operatorname{supp}(\alpha)$. Esto implica que $\alpha \notin E$. Como $\#\operatorname{top}_m(\alpha) = d$ tenemos que

$$\max\{\#\operatorname{top}_m(\alpha)\ ;\ \alpha \in \mathbb{N}^p \setminus E, |\alpha| \leq s\} \geq \dim(E),$$

lo que completa la demostración. □

Teorema 6.11. *Sea* $E = \{\alpha^1, \ldots, \alpha^t\} + \mathbb{N}^n$, *y* $m = \max\{\alpha_i^j \mid 1 \leq j \leq t, 1 \leq i \leq n\}$. *Entonces existe un único polinomio* $h(x) \in \mathbb{Q}[x]$ *tal que* $\mathrm{HF}_E(s) = h(s)$ *para todo* $s \geq nm$. *Además* $\deg(h) = \dim(E)$.

Demostración. El polinomio que deseamos exista debe satisfacer que

$$h(s) = \#\{\alpha \in \mathbb{N}^n \setminus E\ ;\ |\alpha| \leq s\}$$

para todo $s \geq nm$, luego en caso de existir debe ser único. Para demostrar su existencia vamos a contar los elementos de los conjuntos $F_s = \{\alpha \in \mathbb{N}^n \setminus E\ ;\ |\alpha| \leq s\}$. Sea pues $s \geq nm$. El que $\alpha \in F_s$ implica que $\operatorname{sh}_m(\alpha) \in F_s$. Usando el Lema 6.9, tenemos que

$$\#F_s = \sum_{\alpha \in R_m} \#([\alpha]_m \cap F_s). \tag{6.1}$$

Observemos que para todo $\alpha \in R_m$, $|\alpha| \leq nm \leq s$. Nuevamente por el Lema 6.9 tenemos

$$[\alpha]_m \cap F_s = \{\alpha + \beta \in F_s \mid \beta_i = 0, \forall i \notin \operatorname{top}_m(\alpha)\}$$

si $\alpha \in R_m$. Sea $A_\alpha = \{\alpha + \beta\ ;\ |\beta| \leq s - |\alpha|, \beta_i = 0\, \forall i \notin \operatorname{top}_m(\alpha)\}$, donde $\alpha \in R_m$. Es sencillo comprobar que $[\alpha]_m \cap F_s \subseteq A_\alpha$. Por otra parte, si $|\alpha + \beta| \leq s$, $\beta_i = 0$ si $i \notin \operatorname{top}_m(\alpha)$ y $\alpha + \beta \in E$,

entonces existe un generador α^k tal que $\alpha_i + \beta_i \geq \alpha_i^k$ para cualquier $i = 1, \ldots, n$. Si $i \notin \operatorname{top}_m(\alpha)$ entonces $\alpha_i = \alpha_i + \beta_i$, luego $\alpha_i \geq \alpha_i^k$; por otra parte, si $i \in \operatorname{top}_m(\alpha)$ entonces $\alpha_i = m \geq \alpha_i^k$, es decir, si $\alpha + \beta \in E$ entonces $\alpha \in E$, lo que es imposible. Con esto se demuestra que $A_\alpha \cap E = \varnothing$ y $A_\alpha = [\alpha]_m \cap F_s$. Un sencillo cálculo combinatorio establece que

$$\#A_\alpha = \binom{s - |\alpha| + \#\operatorname{top}_m(\alpha)}{\#\operatorname{top}_m(\alpha)},$$

por lo que podemos dar una mejor descripción de (6.1) cuando $s \geq nm$,

$$\#F_s = \sum_{\alpha \in R_m} \binom{s - |\alpha| + \#\operatorname{top}_m(\alpha)}{\#\operatorname{top}_m(\alpha)}.$$

El polinomio buscado es por tanto

$$h(s) = \sum_{\alpha \in R_m} \binom{s - |\alpha| + \#\operatorname{top}_m(\alpha)}{\#\operatorname{top}_m(\alpha)}. \tag{6.2}$$

Si $k \in \mathbb{N}$ entonces $\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}$, de donde cada sumando de (6.2) tiene grado $\#\operatorname{top}_m(\alpha)$ y coeficiente líder positivo. Vemos con esto que

$$\deg(h) = \max\{\#\operatorname{top}_m(\alpha)\ ;\ \alpha \in R_m\} = \max\{\#\operatorname{top}_m(\alpha)\ ;\ \alpha \in F_s\}.$$

El lema 6.10 garantiza que $\deg(h) = \dim(E)$, lo que termina la demostración del teorema. □

6.3

Función de Hilbert de un ideal

Recordemos que el grado total de un polinomio en $R = \mathbb{F}[x_1, \ldots, x_n]$ es el mayor de los grados de sus monomios, donde el grado de un monomio X^α es $|\alpha| = \alpha_1 + \cdots + \alpha_n$. Para cualquier natural $s \in \mathbb{N}$, denotamos

$$R_s = \mathbb{F}[x_1, \ldots, x_n] = \langle X^\alpha \,;\ |\alpha| \leq s \rangle_{\mathbb{F}}$$

el subespacio vectorial formado por todos aquellos polinomios cuyo grado total es menor o igual que s.
Sea $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ un ideal. Denotamos

$$I_s = R_s \cap I,$$

es decir, los polinomios en I cuyo grado total está acotado por s. Observemos que R_s e I_s tienen dimensión finita, y por tanto el espacio vectorial cociente R_s/I_s también.

Definición 6.12. Se define la función de Hilbert de I como

$$\begin{aligned} HF_{R/I} : \mathbb{N} &\longrightarrow \mathbb{N} \\ s &\longmapsto \dim_{\mathbb{F}} (R_s/I_s)\,. \end{aligned}$$

Teorema 6.13. *Sea* I *un ideal no nulo de* $R = \mathbb{F}[x_1, \ldots, x_n]$ *y fijemos* $\leq$ *un orden graduado. Entonces* $HF_{R/I} = HF_{\exp(I)}$.

Demostración. Basta ver que $\{X^\alpha + I_s \,;\ \alpha \notin \exp(I), |\alpha| \leq s\}$ es una base de R_s/I_s como espacio vectorial sobre $\mathbb{F}$. Sea $G = \{g_1, \ldots, g_t\}$

una base de Gröbner para I. Dado $f \in R_s$, por el algoritmo de la división (Teorema 3.4) tenemos que

$$f = q_1 g_1 + \cdots + q_t g_t + r$$

donde $\varnothing = \operatorname{supp}(r) \cap \bigcup_{i=1}^{t} \exp(g_i) + \mathbb{N}^n$ y $\exp(r), \exp(q_i g_i) \leq \exp(f)$ para $1 \leq i \leq t$. Por una parte, como el orden es graduado y $f \in R_s$, tenemos que $r, q_1 g_1, \ldots, q_t g_t \in R_s$, de donde deducimos que $q_1 g_1 + \cdots + q_t g_t \in I_s$ y por tanto $f - r \in I_s$. Por otra parte $\bigcup_{i=1}^{t} \exp(g_i) + \mathbb{N}^n = \exp(I)$ por ser G una base de Gröbner, por lo que $\operatorname{supp}(r) \subseteq \mathbb{N}^n \setminus \exp(I)$, lo que junto al hecho de que $r \in R_s$ implica que $\{X^\alpha + I_s \,;\, \alpha \notin \exp(I), |\alpha| \leq s\}$ es un conjunto de generadores para R_s/I_s. Finalmente la independencia lineal es consecuencia directa del Lema 3.11. □

6.4 Dependencia entera

Definición 6.14. Sean $R \subseteq S$ anillos conmutativos y sea $I \subseteq R$ un ideal. Un elemento $\psi \in S$ se dice entero sobre I si existe un polinomio

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

tal que $a_1, \ldots, a_n \in I$ y $f(\psi) = 0$. La extensión $R \subseteq S$ se dice entera si todo elemento de S es entero sobre R.

Decimos que S es finitamente generado sobre R si existen $\psi_1, \ldots, \psi_s \in S$ tales que, para cualquier $\psi \in S$, $\psi = r_1 \psi_1 + \cdots + r_s \psi_s$ para ciertos $r_1, \ldots, r_s \in R$.

Proposición 6.15. *Dado $\psi \in S$, las siguientes afirmaciones son equivalentes:*

(a) ψ *es entero sobre* I.

(b) $R[\psi]$ *es finitamente generado sobre* R *y* $\psi \in \sqrt{\langle I \rangle_{R[\psi]}}$.

(c) Existe un subanillo $S' \subseteq S$ *tal que* $R[\psi] \subseteq S'$, S' *es finitamente generado sobre* R, *y* $\psi \in \sqrt{\langle I \rangle_{S'}}$.

Demostración. Supongamos que ψ es entero sobre R y sea f el polinomio dado en la Definición 6.14. Como su coeficiente líder es 1, todo elemento $g \in R[x]$ puede escribirse como $g = qf + r$ con $\deg(r) < \deg(f)$. Como $g(\psi) = r(\psi)$, tenemos que $R[\psi]$ está generado por el conjunto $\{1, \psi, \ldots, \psi^{m-1}\}$. Por otra parte, $\psi^m \in \langle I \rangle_{R[\psi]}$, por lo que $\psi \in \sqrt{\langle I \rangle_{R[\psi]}}$. Esto demuestra que (a) implica (b).
La implicación de (b) a (c) es trivial tomando $S' = R[\psi]$. Supongamos por tanto que se da (c), sean $\psi_1, \ldots, \psi_s$ los generadores de S' y supongamos que $\psi^l \in \langle I \rangle_{S'}$. Tenemos que para cada $1 \leq i \leq s$,

$$\psi^l \psi_i = \sum_{k=1}^{s} r_{ik} \psi_k$$

para algunos $r_{ik} \in I$. En consecuencia

$$\sum_{k=1}^{s} (\psi^l \delta_{ik} - r_{ik}) \psi_k = 0$$

para $r_{ik} \in I$. Denotemos

$$M = [\psi^m \delta_{ik} - r_{ik}]_{1 \leq i,k \leq s},$$

y tenemos

$$M\,(\psi_1,\ldots,\psi_s)^T = 0.$$

Multiplicando a la izquierda por $(M^*)^T$, la adjunta traspuesta, tenemos que

$$\det(M)I_k\,(\psi_1,\ldots,\psi_s)^T = 0,$$

es decir,

$$\det(M)\psi_k = 0, 1 \leq k \leq s.$$

Como $1 \in S'$, existen $a_1,\ldots,a_s \in R$ tales que $\sum_{k=1}^{s} a_k\phi_k = 1$. Como consecuencia

$$\det(M) = 0$$

Sea

$$f(x) = \det\left[x^m\delta_{ik} - r_{ik}\right]_{1\leq i,k\leq s}.$$

Es una operación directa comprobar que f es un polinomio de los requeridos en la Definición 6.14, y que $f(\psi) = 0$. □

Las demostraciones de los siguientes corolarios se dejan como ejercicio.

Corolario 6.16. *Si S es finitamente generado sobre R, entonces S es entero sobre R. Además, $\psi \in S$ es entero sobre $I \subseteq R$ si y solo si $\psi \in \sqrt{\langle I\rangle_S}$.*

Corolario 6.17. *Si $\psi_1,\ldots,\psi_n \in S$ son elementos enteros sobre I, entonces $R[\psi_1,\ldots,\psi_n]$ es finitamente generado sobre R y, para cada $1 \leq i \leq n$, $\psi_i \in \sqrt{\langle I\rangle_{R[\psi_1,\ldots,\psi_n]}}$.*

Corolario 6.18. *Si S es entero sobre R y T entero sobre S, entonces T es entero sobre R.*

Corolario 6.19. *El conjunto* $\overline{R}$ *de todos los elementos de* S *que son enteros sobre* R *es un subanillo de* S *que recibe el nombre de clausura entera. Además* $\sqrt{\langle I\rangle_{\overline{R}}}$ *es el conjunto de todos los elementos de* S *que son enteros sobre* I.

6.5 Normalización de Noether

Sea $A = \mathbb{F}[x_1, \ldots, x_n]/I$. Los elementos $f_1 + I, \ldots, f_r + I \in A$ se dicen algebraicamente dependientes si existe $g \in \mathbb{F}[y_1, \ldots, y_r]$ tal que $g(f_1 + I, \ldots, f_r + I) = 0$. En caso contrario se dicen algebraicamente independientes.

Lema 6.20. *Sea* $f \in \mathbb{F}[x_1, \ldots, x_n]$ *un polinomio no constante.*

(a) Existe un cambio de variable $x_i = y_i + x_n^{r_i}$ *para* $1 \leq i \leq n-1$ *tal que*

$$f = ax_n^m + \rho_1 x_n^{m-1} + \cdots + \rho_{m-1}x_n + \rho_m$$

con $a \in \mathbb{F} \setminus \{0\}$, *y* $\rho_1, \ldots, \rho_m \in \mathbb{F}[y_1, \ldots, y_{n-1}]$.

(b) Si $\mathbb{F}$ *es infinito, el mismo resultado puede obtenerse con un cambio de variable de la forma* $x_i = y_i + a_i x_n$ *con* $a_i \in \mathbb{F}$ *para cada* $1 \leq i \leq n-1$.

Demostración. Sea $f = \sum_\alpha c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Realizando el cambio de

variable tenemos

$$\begin{aligned} f &= \sum_{\alpha} c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n} \\ &= \sum_{\alpha} c_\alpha (y_1 + x_n^{r_1})^{\alpha_1} \cdots (y_{n-1} + x_n^{r_{n-1}})^{\alpha_{n-1}} x_n^{\alpha_n} \\ &= \sum_{\alpha} c_\alpha x_n^{r_1\alpha_1 + \cdots + r_{n-1}\alpha_{n-1} + \alpha_n} + \sum_{\alpha} c_\alpha \lambda_\alpha \end{aligned}$$

donde $\deg_{x_n}(\lambda_\alpha) < r_1\alpha_1 + \cdots + r_{n-1}\alpha_{n-1} + \alpha_n$. Sea $k-1$ el mayor exponente al que aparece elevada cualquier variable en f. Para cualquier $\alpha \in \operatorname{supp}(f)$, los elementos $k^{n-1}\alpha_1 + \cdots + k\alpha_{n-1} + \alpha_n$ son distintos, por lo que la asignación $r_i = k^{n-i}$ nos da el cambio de variable requerido.

Supongamos ahora que $\mathbb{F}$ es infinito y sea $f = f_0 + f_1 + \cdots + f_m$ la descomposición en componentes homogéneas respecto al grado total ($\deg(f_i) = i$ si $f_i \neq 0$). Por tanto,

$$\begin{aligned} f_m &= \sum_{\substack{\alpha \\ |\alpha|=m}} c_\alpha x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} x_n^{\alpha_n} \\ &= \sum_{\substack{\alpha \\ |\alpha|=m}} c_\alpha (y_1 + a_1 x_n)^{\alpha_1} \cdots (y_{n-1} + a_{n-1} x_n)^{\alpha_{n-1}} x_n^{\alpha_n} \\ &= f_m(a_1, \ldots, a_{n-1}, 1) x_n^m + \sum_{\substack{\alpha \\ |\alpha|=m}} c_\alpha \lambda_\alpha \end{aligned}$$

donde $\deg_{x_n}(\lambda_\alpha) < m$. Por tanto también tenemos

$$f = f_m(a_1, \ldots, a_{n-1}, 1) x_n^m + f'.$$

donde $\deg_{x_n}(f') < m$. Como $\mathbb{F}$ es infinito, existen $a_1, \ldots, a_{n-1} \in \mathbb{F}$ tales que $f(a_1, \ldots, a_{n-1}, 1) \neq 0$, lo que demuestra el lema. □

Lema 6.21. *Sea* $A = \mathbb{F}[x_1, \ldots, x_n]$ *y sea* $I = \langle f \rangle \subseteq A$ *con* f *no constante. Existen* $y_1, \ldots, y_n \in A$ *tales que*

(a) $y_1, \ldots, y_n$ *son algebraicamente independientes sobre* $\mathbb{F}$*,*

(b) A *es finitamente generado sobre* $\mathbb{F}[y_1, \ldots, y_n]$*,*

(c) $I \cap \mathbb{F}[y_1, \ldots, y_n] = \langle y_n \rangle$*.*

Demostración. Sea $y_n = f$ e $y_1, \ldots, y_{n-1}$ los elementos obtenidos en el Lema 6.20. Tenemos que $A = \mathbb{F}[y_1, \ldots, y_n][x_n]$, y dado que

$$0 = f - y_n = a x_n^m + \rho_1 x_n^{m-1} + \cdots + \rho_m - y_n,$$

x_n es entero sobre $\mathbb{F}[y_1, \ldots, y_n]$. En particular A es finitamente generado sobre $\mathbb{F}[y_1, \ldots, y_n]$, y por la Proposición 6.15, A es entero sobre $\mathbb{F}[y_1, \ldots, y_n]$. Los elementos $y_1, \ldots, y_n$ son algebraicamente independientes puesto que en caso contrario $\mathbb{F}(y_1, \ldots, y_n)$, y con él $\mathbb{F}(x_1, \ldots, x_n)$ tendría grado de trascendencia menor que n. Veamos que $I \cap \mathbb{F}[y_1, \ldots, y_n] = \langle y_n \rangle$. Para ello sea $g \in I \cap \mathbb{F}[y_1, \ldots, y_n]$. Por una parte

$$g = hf = hy_n$$

con $h \in A$. Como A es entero sobre $\mathbb{F}[y_1, \ldots, y_n]$, tenemos que

$$h^s + a_1 h^{s-1} + \cdots + a_s = 0,\ s > 0, a_i \in \mathbb{F}[y_1, \ldots, y_n],$$

de donde deducimos que

$$f^s + a_1 y_n f^{s-1} + \cdots + a_s y_n^s = 0,$$

lo que implica que $y_n \mid f$. □

Lema 6.22. *Sea* $A = \mathbb{F}[x_1, \ldots, x_n]$ *y sea* $I \subseteq A$ *un ideal. Existe un número natural* $\delta \leq n$ *y elementos* $y_1, \ldots, y_n \in A$ *tales que*

(a) $y_1, \ldots, y_n$ *son algebraicamente independientes sobre* $\mathbb{F}$*,*

(b) A *es finitamente generado sobre* $\mathbb{F}[y_1, \ldots, y_n]$*,*

(c) $I \cap \mathbb{F}[y_1, \ldots, y_n] = \langle y_{\delta+1}, \ldots, y_n \rangle$*.*

Demostración. Si $I = \{0\}$ no hay nada que demostrar, así que supongamos que I tiene un polinomio no constante f. Si $n = 1$, tenemos el resultado por el Lema 6.21 ya que I es principal. Supongamos por tanto $n > 1$ y sea $\mathbb{F}[y_1, \ldots, y_n]$ construido como en el Lema 6.21. Para aplicar el principio inducción supongamos que el teorema se cumple para el ideal $I \cap \mathbb{F}[y_1, \ldots, y_{n-1}]$. Existen elementos $t_1, \ldots, t_{n-1} \in \mathbb{F}[y_1, \ldots, y_{n-1}]$ algebraicamente independientes tales que $\mathbb{F}[y_1, \ldots, y_{n-1}]$ es finitamente generado sobre $\mathbb{F}[t_1, \ldots, t_{n-1}]$ e $I \cap \mathbb{F}[y_1, \ldots, y_{n-1}] = \langle t_{\delta+1}, \ldots, t_{n-1} \rangle$ para algún $\delta < n$. Como consecuencia $\mathbb{F}[y_1, \ldots, y_{n-1}, y_n]$ es finitamente generado sobre $\mathbb{F}[t_1, \ldots, t_{n-1}, y_n]$, lo que implica que A es finitamente generado sobre $\mathbb{F}[t_1, \ldots, t_{n-1}, y_n]$. Por tanto $t_1, \ldots, t_{n-1}, y_n$ son algebraicamente independientes sobre $\mathbb{F}$ utilizando de nuevo el grado de trascendencia como en la demostración del Lema 6.21.
Cualquier $g \in I \cap \mathbb{F}[t_1, \ldots, t_{n-1}, y_n]$ puede escribirse como

$$g = g^* + h y_n$$

con

$$g^* \in I \cap \mathbb{F}[y_1, \ldots, y_{n-1}] = \langle t_{\delta+1}, \ldots, t_{n-1} \rangle$$

y

$$h \in \mathbb{F}[t_1, \ldots, t_{n-1}, y_n].$$

Por lo tanto

$$I \cap \mathbb{F}[t_1, \ldots, t_{n-1}, y_n] = \langle t_{\delta+1}, \ldots, t_{n-1}, y_n \rangle,$$

lo que demuestra el Lema. □

Teorema 6.23 (Normalización de Noether)**.** *Sea* $A = \mathbb{F}[x_1, \ldots, x_n]/J$ *y sea* $I \subseteq A$ *un ideal. Existen números naturales* $\delta \leq d$ *y elementos* $y_1, \ldots, y_d \in A$ *tales que*

(a) $y_1, \ldots, y_d$ *son algebraicamente independientes sobre* $\mathbb{F}$*,*

(b) A *es finitamente generado sobre* $\mathbb{F}[y_1, \ldots, y_d]$*,*

(c) $I \cap \mathbb{F}[y_1, \ldots, y_d] = \langle y_{\delta+1}, \ldots, y_d \rangle$*.*

Demostración. Por el Lema 6.22, existen $y_1, \ldots, y_n \in \mathbb{F}[x_1, \ldots, x_n]$ tales que

$$J \cap \mathbb{F}[y_1, \ldots, y_n] = \langle y_{d+1}, \ldots, y_n \rangle.$$

La imagen de $\mathbb{F}[y_1, \ldots, y_n]$ en A es isomorfa a $\mathbb{F}[y_1, \ldots, y_d]$ y A es finitamente generada sobre dicha imagen. Aplicamos de nuevo el Lema 6.22 a $I' = I \cap \mathbb{F}[y_1, \ldots, y_d]$. Existen $t_1, \ldots, t_d \in \mathbb{F}[y_1, \ldots, y_d]$ tales que $\mathbb{F}[y_1, \ldots, y_d]$ es finitamente generada sobre $\mathbb{F}[t_1, \ldots, t_d]$ y $I' \cap \mathbb{F}[t_1, \ldots, t_d] = \langle t_{\delta+1}, \ldots, t_d \rangle$. Como A es finitamente generada sobre $\mathbb{F}[t_1, \ldots, t_d]$, estos elementos demuestran el teorema. □

6.6 Dependencia entera y función de Hilbert

Teorema 6.24. *Sea $\leq$ un orden graduado en $R = \mathbb{F}[x_1, \ldots, x_n]$ y sea $I \subseteq R$ un ideal. Entonces* $\dim(\exp(I))$ *coincide con el máximo número de elementos de R/I algebraicamente independientes.*

Demostración. Sea $\sigma \in T(\exp(I))$ y sea $\{x_{i_1}, \ldots, x_{i_r}\} = \{x_i \,;\, i \notin \sigma\}$. Veamos que $\{x_{i_1} + I, \ldots, x_{i_r} + I\}$ es un conjunto de elementos algebraicamente independiente. Para ello sea $f \in \mathbb{F}[x_{i_1}, \ldots, x_{i_r}] \cap I$. Como $f \in I$, si $f \neq 0$ tenemos que $\exp(f) \in \exp(I)$, pero $\operatorname{supp}(\exp(f)) \cap \sigma = \varnothing$, una contradicción. Necesariamente $f = 0$. Como ningún polinomio satisface

$$f(x_{i_1} + I, \ldots, x_{i_r} + I) = 0,$$

tenemos que $x_{i_1} + I, \ldots, x_{i_r} + I$ son algebraicamente independientes. Como consecuencia $\dim(\exp(I)) \leq r$.

Para ver la desigualdad contraria, supongamos que $f_1 + I, \ldots, f_r + I \in \mathbb{F}[X]/I$ son algebraicamente independientes. Sea N el mayor de los grados totales de los elementos $f_1, \ldots, f_r$. Si $g \in \mathbb{F}[y_1, \ldots, y_r]$ tiene grado total $\leq s$, tenemos que $g(f_1, \ldots, f_r) \in \mathbb{F}[x_1, \ldots, x_n] = R$ tiene grado total $\leq Ns$, esto implica que la aplicación

$$\begin{aligned} \alpha : \mathbb{F}[y_1, \ldots, y_r]_s &\to R_{Ns}/I_{Ns} \\ g(y_1, \ldots, y_r) &\mapsto g(f_1, \ldots, f_r) + I_{Ns} \end{aligned}$$

está bien definida y es $\mathbb{F}$-lineal. Supongamos que $\alpha(g) = 0$. Entonces

$$0 = g(f_1, \ldots, f_r) + I_{Ns} = g(f_1 + I, \ldots, f_r + I),$$

lo que contradice que $\{f_1 + I, \ldots, f_r + I\}$ son algebraicamente independientes. Por consiguiente

$$\dim \mathbb{F}[y_1, \ldots, y_r]_s \leq HF_{R/I}(Ns).$$

Como $\dim \mathbb{F}[y_1, \ldots, y_r]_s = \binom{r+s}{s} = \binom{r+s}{r}$, que es un polinomio de grado r en s, tenemos que para s suficientemente grande, $HF_{R/I}(Ns)$ es un polinomio acotado por otro de grado menor o igual que r. Por tanto el grado de $HF_{R/I}(Ns)$, y en consecuencia el de $HF_{R/I}(s)$, es mayor o igual que r, lo que implica que $\dim(\exp(I)) \geq r$. □

6.7 Teoremas de Cohen y Seidenberg

Lema 6.25. *Sea $R \subseteq S$ una extensión entera, $J \subseteq S$ un ideal e $I = J \cap R$. Entonces*

1. *S/J es una extensión entera de R/I.*
2. *Si J contiene un elemento que no es divisor de cero, entonces $I \neq \langle 0 \rangle$.*

Demostración. Si observamos que R/I está canónicamente dentro de S/J, la dependencia entera de S/J sobre R/I se sigue directamente de la Definición 6.14.
Sea $\psi \in J$ no divisor de cero y sea

$$\psi^m + r_1\psi^{m-1} + \cdots + r_m = 0.$$

Si $r_m = 0$, como ψ no es divisor de cero tenemos que

$$\psi^{m-1} + r_1\psi^{m-2} + \cdots + r_{m-1} = 0,$$

por lo que no perdemos generalidad si suponemos que $r_m \neq 0$. En consecuencia $0 \neq r_m \in J \cap R = I$. □

Lema 6.26 (Krull)**.** *Sea* $I \subseteq R$ *un ideal y sea* $C \subseteq R$ *un subconjunto multiplicativamente cerrado tan que* $I \cap C = \varnothing$*. El conjunto*

$$\mathcal{I} = \{J \subseteq R\,;\ J \textit{ es ideal}, I \subseteq J, J \cap C = \varnothing\}$$

tiene un elemento maximal. Dicho elemento maximal es primo.

Demostración. Sea $\{J_\lambda\}_{\lambda\in\Lambda} \subseteq \mathcal{I}$ una cadena respecto de la inclusión. Sea $J = \bigcup_{\lambda\in\Lambda} J_\lambda$. Es inmediato comprobar que $I \subseteq J$ y que $J \cap C = \varnothing$, por lo que $J \in \mathcal{I}$. Podemos aplicar el Lema de Zorn y concluir que $\mathcal{I}$ tiene un elemento maximal. Sea P uno de dichos elementos maximales. Sean $a_1, a_2 \notin P$ y supongamos que $a_1a_2 \in P$. Como $a_i \notin P$, por la maximalidad de P tenemos que $(\langle a_i\rangle + P) \cap C \neq \varnothing$. Existen $r_1, r_2 \in R$ y $p_1, p_2 \in P$ tales que $r_1a_1 + p_1, r_2a_2 + p_2 \in C$. Como C es multiplicativamente cerrado, tenemos que

$$(r_1a_1 + p_1)(r_2a_2 + p_2) \in C.$$

Por otra parte

$$(r_1a_1+p_1)(r_2a_2+p_2) = r_1r_2a_1a_2+r_1a_1p_2+r_2a_2p_1+p_1p_2 \in P,$$

por lo que $P \cap C = \varnothing$ lo que contradice que $P \in \mathcal{I}$. Por tanto $a_1a_2 \notin P$ y P es primo. □

Observemos que $P \subseteq R$ es primo si y solo si $R \setminus P$ es multiplicativamente cerrado. También es inmediato comprobar que si $R \subseteq S$ es una extensión de anillos y $Q \subseteq S$ es un ideal primo, entonces $Q \cap R$ también es primo.

Proposición 6.27. *Sea* $R \subseteq S$ *una extensión entera. Entonces:*

1. *Dado un ideal primo* $P \subseteq R$*, existe otro ideal primo* $Q \subseteq S$ *tal que* $P = Q \cap S$.
2. *Si* $Q_1 \subseteq Q_2 \subseteq S$ *son ideales primos tales que* $Q_1 \cap R = Q_2 \cap R$*, entonces* $Q_1 = Q_2$.

Demostración. Sea $P \subseteq R$ primo y sea $C = R \setminus P$. Por el Corolario 6.19, cualquier $\psi \in \langle P \rangle_S$ satisface una ecuación del tipo

$$\psi^n + r_1\psi^{n-1} + \cdots + r_n = 0, \quad n > 0, r_i \in P.$$

Si $\psi^n \in \langle P \rangle_S \cap C$, tenemos que en particular $\psi^n \in R$, por lo que $\psi^n \in P$. Al ser P primo tenemos que $\psi \in P$, lo que contradice que $\psi \in C$. Por tanto $\langle P \rangle_S \cap C = \varnothing$. Por el Lema 6.26 existe un primo $Q \subseteq S$ tal que $\langle P \rangle_S \subseteq Q$ y $Q \cap C = \varnothing$. Esta última identidad implica que $Q \cap R = P$.
Supongamos ahora que $Q_1 \cap R = Q_2 \cap R = P$ con $Q_1, Q_2 \subseteq S$ primos. Por el Lema 6.25 S/Q_1 es entero sobre R/P. Observemos que Q_2/Q_1 es un ideal primo de S/Q_1 ya que $S/Q_2 \cong (S/Q_1)/(Q_2/Q_1)$, y además $Q_2/Q_1 \cap R/P = \langle 0 \rangle$. De nuevo por el Lema 6.25 concluimos que $Q_2/Q_1 = \langle 0 \rangle$, es decir, $Q_2 = Q_1$. □

Corolario 6.28. *Sea* $R \subseteq S$ *una extensión entera. Si* $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$ *es una cadena de ideales primos en* S *y* $P_i = Q_i \cap R$ *para* $0 \leq i \leq n$*, entonces* $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$.

Corolario 6.29. *Sea* $R \subseteq S$ *una extensión entera y sea* $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ *una cadena de ideales primos en* R*. Para cualquier* $Q_0 \subseteq S$ *primo tal que* $P_0 = Q_0 \cap R$*, existe una cadena* $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$ *de ideales primos en* S *tal que* $P_i = Q_i \cap R$*,* $0 \leq i \leq n$

Demostración. Por inducción, si hemos construido $Q_0 \subsetneq \cdots \subsetneq Q_i$, por la Proposición 6.27 aplicada al ideal primo P_{i+1}/P_i en $R/P_i \subseteq S/Q_i$, existe un ideal primo Q_{i+1}/Q_i en S/Q_i tal que $Q_{i+1}/Q_i \cap R/P_i = P_{i+1}/P_i$, lo que implica que $Q_{i+1} \cap R = P_{i+1}$. □

Corolario 6.30. *Si* $R \subseteq S$ *una extensión entera,* $\dim(R) = \dim(S)$.

6.8 Dimensión de Krull e independencia algebraica

Ejercicios sobre Dimensión

Ejercicio 6.1. Encuentra $\dim(E)$ para

$$E = \{(1,1,0),(0,1,1),(1,0,1)\} + \mathbb{N}^3$$
$$E = \{(1,2,0,1),(3,0,1,0),(1,1,1,1),(5,0,6,0)\} + \mathbb{N}^4$$
$$E = \{(2,1,1,0,1,1),(0,0,1,3,3,0),$$
$$(1,0,0,1,7,1),(1,0,1,3,3,2)\} + \mathbb{N}^6$$

Ejercicio 6.2. Demuestra que

$$\#\{\alpha \in \mathbb{N}^n \,;\ |\alpha| \leq s\} = \binom{n+s}{n}.$$

Como ayuda sugiero calcular previamente $\#\{\alpha \in \mathbb{N}^n \,;\ |\alpha| = s\}$.

Ejercicio 6.3. Sea $E = \{\alpha^1, \ldots, \alpha^t\} + \mathbb{N}^n$ y sea $I = \left\langle X^{\alpha^1}, \ldots, X^{\alpha^t} \right\rangle \subseteq \mathbb{F}[X]$. Sea $\sigma \in T(E)$. ¿Qué relación existe entre $\mathbf{V}(\langle x_i \,;\ i \in \sigma\rangle)$ y $\mathbf{V}(I)$?

Ejercicio 6.4. Sea $E = E + \mathbb{N}^n$. Demuestra que $\dim(E) = 0$ si y solo si para cada $1 \leq i \leq n$, existe un $l_i \in \mathbb{N}$ tal que $(0, \ldots, l_i, \ldots, 0) \in E$.

Ejercicio 6.5. Sea $E = \{\alpha^1, \ldots, \alpha^t\} + \mathbb{N}^n$ y sea $I = \left\langle X^{\alpha^1}, \ldots, X^{\alpha^t} \right\rangle \subseteq \mathbb{F}[X]$. Si $\dim(E) = 0$, ¿cómo es $\mathbf{V}(I)$?

Ejercicio 6.6. Demuestra que si $E = \{\alpha^1, \ldots, \alpha^t\} + \mathbb{N}^n$ con $t \leq n$, entonces $\dim(E) \geq n - t$.

Ejercicio 6.7. Sea $E = \{\alpha^1, \ldots, \alpha^t\} + \mathbb{N}^n$ y sea $I = \left\langle X^{\alpha^1}, \ldots, X^{\alpha^t} \right\rangle \subseteq \mathbb{F}[X]$. Calcula $\sqrt{I}$.

Ejercicio 6.8. Demuestra que el polinomio

$$p(x) = \binom{x}{d} = \frac{x(x-1)\cdots(x-d+1)}{d!}$$

toma un valor entero para cada entero.

Ejercicio 6.9. Sea $I = \langle x^3 - xyz, y^4 - xyz^2, xy - z^2 \rangle$. Encuentra bases para I_3 e I_4.

Ejercicio 6.10. Calcula el polinomio de Hilbert de los siguientes ideales

$$\langle x^3y, xy^2 \rangle \subseteq \mathbb{F}[x, y]$$
$$\langle x^3y^2 + 3x^2y^2 + y^3 + 1 \rangle \subseteq \mathbb{F}[x, y]$$
$$\langle x^3yz^5, xy^3z^2 \rangle \subseteq \mathbb{F}[x, y, z]$$
$$\langle x^3 - yz^2, y^4 - x^2yz \rangle \subseteq \mathbb{F}[x, y, z]$$

Calcula también en cada caso el menor s_0 a partir del cual la función de Hilbert coincide con el polinomio de Hilbert.

Ejercicio 6.11. Demuestra que si S es finitamente generado sobre R, entonces S es entero sobre R. Demuestra que $\psi \in S$ es entero sobre $I \subseteq R$ si y solo si $\psi \in \sqrt{\langle I \rangle_S}$.

Ejercicio 6.12. Si $\psi_1, \ldots, \psi_n \in S$ son elementos enteros sobre I, entonces $R[\psi_1, \ldots, \psi_n]$ es finitamente generado sobre R y, para cada $1 \leq i \leq n$, $\psi_i \in \sqrt{\langle I \rangle_{R[\psi_1, \ldots, \psi_n]}}$.

Ejercicio 6.13. Si S es entero sobre R y T entero sobre S, entonces T es entero sobre R.

Ejercicio 6.14. El conjunto $\overline{R}$ de todos los elementos de S que son enteros sobre R es un subanillo de S que recibe el nombre de clausura entera. Además $\sqrt{\langle I \rangle_{\overline{R}}}$ es el conjunto de todos los elementos de S que son enteros sobre I.

Bibliografía

[1] Thomas Becker, Volker Weispfenning, and Heinz Kredel. *Gröbner Bases. A Computational Approach to Commutative Algebra.* Number 141 in Graduate Texts in Mathematics. Springer Science+Business Media, 1993.

[2] David A. Cox, John Little, and Donald O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Text in Mathematics. Springer, fourth edition, 2015.

[3] Ernst Kunz. *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser, 1985.

[4] Serge Lang. *Undergraduate Algebra*. Undergraduate Text in Mathematics. Springer, second edition, 1990.