Álgebra Conmutativa Computacional

F. J. Lobillo

2019/2020

Índice general

Capítulo 1

Anillos e ideales

1.1 Anillos conmutativos

Definición 1.1. Un *anillo* es un conjunto R sobre el que hay definidas dos operaciones $+ : R \times R \to R$ y $\cdot : R \times R \to R$ (denominadas suma y producto) que satisfacen las siguientes propiedades:

Asociativa de la suma. Para cualesquiera $r, s, t \in R$,

$$r + (s + t) = (r + s) + t.$$

Conmutativa de la suma. Para cualesquiera $r, s \in R$,

$$r + s = s + r.$$

Elemento neutro para la suma. Existe un elemento $0 \in R$ tal que

$$r + 0 = r$$

para cualquier $r \in R$.

Elemento opuesto para la suma. Para cualquier $r \in R$, existe $-r \in R$ tal que

$$r + (-r) = 0.$$

Asociativa del producto. Para cualesquiera $r, s, t \in R$,

$$r(st) = (rs)t.$$

Elemento neutro para el producto. Existe $1 \in R$, tal que

$$r1 = 1r = r$$

para todo $r \in R$.

Distributiva de la suma respecto del producto. Para todos $r, s, t \in R$,

$$r(s + t) = rs + rt$$

y

$$(r + s)t = rt + st.$$

Un anillo se dice *conmutativo* si satisface la propiedad

Conmutativa del producto. Para cualesquiera $r, s \in R$,

$$rs = sr.$$

Proposición 1.2. *Los elementos neutros para la suma y el producto son únicos. El opuesto de un elemento es único.*

Demostración. Si $0, 0' \in R$ son elementos neutros para la suma

$$0 = 0 + 0' = 0'.$$

La unicidad del elemento neutro para el producto es análoga. Si $-r, r'$ son opuestos para r,

$$-r = -r + 0 = -r + (r + r') = (-r + r) + r' = 0 + r' = r'.$$

□

Definición 1.3. Dado un anillo conmutativo R, un elemento r es una *unidad* si tiene inverso para el producto, es decir, si existe $r^{-1} \in R$ tal que

$$rr^{-1} = 1.$$

El conjunto de la unidades se denota $\mathcal{U}(R)$. Se dice que $r \in R$ es un *divisor de cero* si existe $s \in R \setminus \{0\}$ tal que $rs = 0$.

Proposición 1.4. *Sea R un anillo. Para cualesquiera $r, s \in R$,*

1. $r0 = 0$,
2. $(-r)s = -(rs) = r(-s)$,
3. *si $r \in \mathcal{U}(R)$, su inverso es único,*
4. *si $r, s \in \mathcal{U}(R)$, $rs \in \mathcal{U}(R)$ y $(rs)^{-1} = s^{-1}r^{-1}$.*

Demostración. Rara cualquier $r \in R$,

$$0 = -(r0) + r0 = -(r0) + r(0 + 0) = \\ -(r0) + (r0 + r0) = (-(r0) + r0) + r0 = 0 + r0 = r0.$$

Dado que

$$(-r)s + rs = (-r + r)s = 0s = 0,$$

se tiene que $(-r)s = -(rs)$ por la unicidad del opuesto. La unicidad del inverso es análoga a la unicidad del opuesto. Finalmente

$$rs(s^{-1}r^{-1}) = r(ss^{-1})r^{-1} = r1r^{-1} = rr^{-1} = 1,$$

de donde $s^{-1}r^{-1} = (rs)^{-1}$ y $rs \in \mathcal{U}(R)$. □

Definición 1.5. Un anillo conmutativo en el que 0 es el único divisor de cero recibe el nombre de *dominio de integridad*. Observemos que R es dominio de integridad si y solo si para cualesquiera $r, s \in R$, si $rs = 0$ entonces $r = 0$ o $s = 0$.
Un *cuerpo* es un anillo conmutativo en el que todo elemento no nulo es una unidad, es decir, $\mathcal{U}(R) = R \setminus \{0\}$.

Ejemplo 1.6. Son anillos conmutativos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $R[x]$ donde R es un anillo conmutativo, $\mathbb{Z}_n$, $\mathbb{F}_q$. De los anteriores, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_q$ son cuerpos.

Ejemplo 1.7. Sean A_1, A_2 dos anillos. Es un ejercicio rutinario comprobar que $A_1 \times A_2$ es un nuevo anillo en el que las operaciones se realizan componente a componente, es decir,

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

y

$$(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2).$$

El cero y el uno de este nuevo anillo son, respectivamente, $(0_1, 0_2)$ y $(1_1, 1_2)$, y el opuesto se calcula

$$-(a_1, a_2) = (-a_1, -a_2).$$

1.2

Subanillos e ideales

Definición 1.8. Dado un anillo A, un subconjunto $B \subseteq A$ es un subanillo si

- $0 \in B$ y $1 \in B$;
- dados $a, b \in B$, $a - b \in B$;
- dados $a, b \in B$, $ab \in B$.

Es inmediato comprobar que un subanillo vuelve a ser un anillo con las operaciones heredadas. Pero no todo subconjunto que sea un anillo con las operaciones heredadas es un subanillo, como vamos a comprobar con el siguiente ejemplo.

Ejemplo 1.9. En $\mathbb{Z}_6$ consideramos el subconjunto $\{0, 2, 4\}$. Es sencillo verificar que $\{0, 2, 4\}$ es cerrado para la suma, opuesto y producto. Como

$$4 \times 0 = 0, 4 \times 2 = 2, 4 \times 4 = 4,$$

tenemos que $\{0, 2, 4\}$ es un anillo en el que el elemento neutro para el producto es 4.

En adelante, y salvo que específicamente se indique lo contrario, todos los anillos tratados en este curso son anillos conmutativos.

Definición 1.10. Dado un anillo conmutativo A, un subconjunto no vacío $I \subseteq A$ es un ideal si

- dados $a, b \in I$, $a + b \in I$;

- dados $a \in I$ y $b \in A$, $ab \in I$.

Se denota por $I \leq A$.

Observación 1.11. Si $a, b \in I$, entonces $a - b = a + (-1)b \in I$, por lo que I es un subgrupo abeliano de A.

Proposición 1.12. *Sea A un anillo conmutativo y sea $I \subseteq A$ un subgrupo abeliano. I es un ideal de A si y sólo si A/I es un anillo conmutativo con respecto a las operaciones $(a + I) + (b + I) = (a + b) + I$ y $(a + I)(b + I) = ab + I$.*

Demostración. Por ser I un subgrupo abeliano sólo tenemos que ocuparnos de que el producto está bien definido. Supongamos que $a + I = a' + I$, es decir, $a - a' \in I$. Si I es ideal, $a + I = a' + I$ y $b + I = b' + I$ tenemos que

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I,$$

luego el producto está bien definido. Recíprocamente, si el producto está bien definido tenemos que $(0 + I)(b + I) = 0 + I$, por tanto, si $a \in I$

$$ab + I = (a + I)(b + I) = (0 + I)(b + I) = 0 + I,$$

es decir, $ab \in I$, lo que implica que I es un ideal. □

Dados ideales $I, J \leq A$, se define

$$I + J = \{x + y \mid x \in I, y \in J\}$$

y

$$IJ = \{x_1y_1 + \cdots + x_ty_t \mid x_i \in I, y_i \in J, 1 \leq i \leq y\}$$

Proposición 1.13. $I + J$, $I \cap J$ *e* IJ *son ideales de* A. $I + J$ *es el menor ideal que contiene tanto a* I *como a* J. $IJ \subseteq I \cap J$.

Demostración. Ejercicio. □

Dado $F \subseteq A$, definimos

$$\langle F \rangle = \{a_1 f_1 + \cdots + a_s f_s \mid a_1, \ldots, a_s \in A, f_1, \ldots, f_s \in F\}.$$

Proposición 1.14. $\langle F \rangle$ *es el menor ideal de* A *que contiene a* F.

Demostración. Es inmediato comprobar que si un ideal contiene a F, debe contener a $\langle F \rangle$. Comprobemos que es un ideal. Sean $a_1 f_1 + \cdots + a_s f_s, b_1 g_1 + \cdots + b_t g_t \in \langle F \rangle$. Tenemos que

$$(a_1 f_1 + \cdots + a_s f_s) + (b_1 g_1 + \cdots + b_t g_t) = \\ a_1 f_1 + \cdots + a_s f_s + b_1 g_1 + \cdots + b_t g_t \in \langle F \rangle.$$

Por otra parte, si $a \in A$ y $a_1 f_1 + \cdots + a_s f_s \in \langle F \rangle$,

$$a(a_1 f_1 + \cdots + a_s f_s) = (aa_1) f_1 + \cdots + (aa_s) f_s \in \langle F \rangle,$$

lo que demuestra que $\langle F \rangle$ es un ideal. □

Definición 1.15. $\langle F \rangle$ recibe el nombre de ideal generado por F. Por convenio, $0 = \langle \varnothing \rangle$. Un ideal I se dice finitamente generado si existen $f_1, \ldots, f_s \in I$ tales que $I = \langle f_1, \ldots, f_s \rangle$.

Proposición 1.16. *Sean* $I = \langle F \rangle$ *y* $J = \langle G \rangle$. *Entonces* $I + J = \langle F \cup G \rangle$ *y* $IJ = \langle fg \mid f \in F, g \in G \rangle$.

Demostración. Ejercicio. □

1.3 Morfismos de anillos

Definición 1.17. Sean A y B dos anillos. Una aplicación $f : A \to B$ es un morfismo de anillos si $f(0) = 0$, $f(1) = 1$, $f(a + b) = f(a) + f(b)$ y $f(ab) = f(a)f(b)$.

Observación 1.18. Como consecuencia de la definición, si $f : A \to B$ es un morfismo de anillos tenemos que

$$0 = f(0) = f(b + (-b)) = f(b) + f(-b),$$

luego $f(-b) = -f(b)$ para cualquier $b \in A$. En consecuencia,

$$f(a - b) = f(a + (-b)) = f(a) + f(-b) = f(a) - f(b),$$

luego f es morfismo de grupos abelianos.

Proposición 1.19. *Sea* $f : A \to B$ *un morfismo de anillos. Entonces* $\mathrm{im}(f)$ *es un subanillo de* B *y* $\ker(f)$ *un ideal de* A. *Además* $\mathrm{im}(f) \cong A/\ker(f)$.

Demostración. Es sencillo comprobar que $\mathrm{im}(f)$ es un subanillo. Como f es un morfismo de grupos abelianos, es también inmediato que $\ker(f)$ es un subgrupo abeliano de A. Si $a \in \ker(f)$ y $b \in A$,

$$f(ab) = f(a)f(b) = 0f(b) = 0,$$

luego $ab \in \ker(f)$, i.e. $\ker(f)$ es un ideal de A. Por último definimos $\phi : A/\ker(f) \to \mathrm{im}(f)$ mediante $\phi(a+\ker(f)) = f(a)$. Esta aplicación

está bien definida porque si $a + \ker(f) = a' + \ker(f)$,

$$\begin{aligned}\phi(a + \ker(f)) = f(a) = f(a - a' + a') \\ = f(a - a') + f(a') = f(a') = \phi(a' + \ker(f)).\end{aligned}$$

Es sencillo comprobar que ϕ es un morfismo de anillos biyectivo. □

Dos ideales $I, J \leq A$ se dicen coprimos si $A = I + J$.

Lema 1.20. *Sean* I, J, K *ideales de* A. *Entonces* $I + J = A$ *e* $I + K = A$ *si y sólo si* $I + (J \cap K) = A$.

Demostración. Es inmediato que si $I+(J\cap K) = A$ tenemos que $I+J = A$ e $I + K = A$. Supongamos por tanto que $I + J = A$ e $I + K = A$. Existen $a, a' \in I$ $b \in J$ y $c \in K$ tales que $1 = a + b$ y $1 = a' + c$. Por tanto

$$1 = a+b = a+b(a'+c) = a+ba'+bc = (a+ba')+bc \in I+(J\cap K),$$

luego $I + (J \cap K) = A$. □

Teorema 1.21 (Teorema Chino del Resto)**.** *Sean* $I_1, \ldots, I_t$ *ideales de* A *coprimos dos a dos, es decir* $I_i + I_j = A$ *para cualesquiera* $i \neq j$. *Entonces* $A/(I_1 \cap \cdots \cap I_t) \cong (A/I_1) \times \cdots \times (A/I_t)$.

Demostración. Sea $f : A \to (A/I_1) \times \cdots \times (A/I_t)$ el morfismo de anillos definido por $f(a) = (a + I_1, \ldots, a + I_t)$. Veamos que es sobreyectivo. Para ello, dados $a_1, \ldots, a_t \in A$ tenemos que encontrar un $x \in A$ tal que $x + I_i = a_i + I_i$ para cada $1 \leq i \leq t$. Aplicando iteradamente el Lema 1.20, tenemos que $A = I_i + \bigcap_{j\neq i} I_j$, por lo que existen

$b_i \in I_i$ y $c_i \in \bigcap_{j \neq i} I_j$ tales que $1 = b_i + c_i$. Sea $x = a_1c_1 + \cdots + a_tc_t$. Dado que

$$\begin{aligned} x + I_i &= a_1c_1 + \cdots + a_tc_t + I_i = a_ic_i + I_i \\ &= a_i(1 - b_i) + I_i = a_i - a_ib_i + I_i = a_i + I_i, \end{aligned}$$

tenemos que f es sobreyectiva. Por otra parte, $f(a) = 0$ si y solo si $a \in I_i$ para cualquier $1 \leq i \leq t$, de donde $\ker(f) = I_1 \cap \cdots \cap I_t$. El teorema se sigue por tanto de la Proposición 1.19. □

Ejercicios sobre Anillos

Todos los anillos considerados en esta relación de ejercicios son conmutativos salvo que se especifique lo contrario.

Ejercicio 1.1. Dados anillos A_1 y A_2, comprueba que $A_1 \times A_2$ con las operaciones definidas en el Ejemplo 1.7 es un anillo. Calcula sus unidades $\mathcal{U}(A_1 \times A_2)$.

Ejercicio 1.2. Un elemento $e \in A$ se dice idempotente si $e^2 = e$. Demuestra que si e es idempotente, $1 - e$ también lo es. Demuestra que $A = \langle e \rangle \oplus \langle 1 - e \rangle$, es decir, $A = \langle e \rangle + \langle 1 - e \rangle$ y $\{0\} = \langle e \rangle \cap \langle 1 - e \rangle$.

Ejercicio 1.3. Un elemento $x \in A$ se dice nilpotente si $x^n = 0$ para algún $n \in \mathbb{N}$. Demuestra que si x es nilpotente, $1 - x$ y $1 + x$ son unidades de A.

Ejercicio 1.4. Demuestra que el conjunto de los elementos nilpotentes de un anillo conmutativo A es un ideal.

Ejercicio 1.5. Sea $p \in \mathbb{Z}$ primo y sea $R = \left\{ \frac{m}{n} \in \mathbb{Q} \mid p \nmid n \right\}$. Demuestra que R es un subanillo.

Ejercicio 1.6. Demuestra la Proposición 1.13.

Ejercicio 1.7. Demuestra la Proposición 1.16.

Ejercicio 1.8. Demuestra que $I(J + K) = IJ + IK$ para ideales $I, J, K \leq A$. ¿Es cierta la identidad $I \cap (J + K) = (I \cap J) + (I \cap K)$?

Ejercicio 1.9. Demuestra que si $I + J = A$, entonces $IJ = I \cap J$.

Ejercicio 1.10. Un ideal $P \lneq A$ en un anillo conmutativo se dice primo si, para cualesquiera $a, b \in A$, si $ab \in P$ entonces $a \in P$ o $b \in P$. Demuestra que $\langle p \rangle \subseteq \mathbb{Z}$ es un ideal primo si y solo si p es un número primo.

Ejercicio 1.11. Un ideal $M \lneq A$ de un anillo conmutativo se dice maximal si no existe otro ideal $J \leq A$ tal que $M \subsetneq J \subsetneq A$. Demuestra que todo ideal maximal es primo.

Ejercicio 1.12. Demuestra que $P \leq A$ es primo si y solo si A/P es un dominio de integridad. Demuestra que $M \leq A$ es maximal si y solo si A/M es un cuerpo.

Capítulo 2

Sistemas de ecuaciones y variedades afines

2.1 Polinomios en varias variables

Sea A un anillo conmutativo y $X = \{x_1, \ldots, x_n\}$ variables distintas. Recordemos que $\mathbb{N}^n$ es un semigrupo conmutativo donde la suma se realiza componente a componente.
Dada una aplicación $f : \mathbb{N}^n \to A$, se define el soporte de f como

$$\operatorname{supp}(f) = \{\alpha \in \mathbb{N}^n \mid f(\alpha) \neq 0\}.$$

Se define el anillo de polinomios $A[x_1, \ldots, x_n]$ como el conjunto de aplicaciones

$$A[X] = A[x_1, \ldots, x_n] = \{f : \mathbb{N}^n \to A \mid \#\operatorname{supp}(f) < \infty\}$$

con suma heredada de la suma en A, es decir, $(f+g)(\alpha) = f(\alpha)+g(\alpha)$, y producto definido por

$$(fg)(\alpha) = \sum_{\beta+\gamma=\alpha} f(\beta)g(\gamma).$$

Teorema 2.1. *$A[x_1, \ldots, x_n]$ es un anillo conmutativo.*

Demostración. Lo único no trivial son las propiedades que involucran al producto. Es sencillo comprobar que el producto es conmutativo y que la aplicación que lleva el $0 = (0, \dots, 0)$ en el uno de A y cero a todos los demás es el elemento neutro del producto. Lo único algo más tedioso es comprobar las propiedades asociativa y distributiva. Sean por tanto $f, g, h \in A[x_1, \dots, x_n]$. Tenemos que

$$\begin{aligned}((fg)h)(\alpha) &= \textstyle\sum_{\lambda+\delta=\alpha}(fg)(\lambda)h(\delta)\\ &= \textstyle\sum_{\lambda+\delta=\alpha}\sum_{\beta+\gamma=\lambda}(f(\beta)g(\gamma))h(\delta)\\ &= \textstyle\sum_{\beta+\gamma+\delta=\alpha} f(\beta)g(\gamma)h(\delta)\end{aligned}$$

y análogamente

$$(f(gh))(\alpha) = \textstyle\sum_{\beta+\gamma+\delta=\alpha} f(\beta)g(\gamma)h(\delta),$$

por lo que el producto es asociativo. Por otra parte,

$$\begin{aligned}(f(g+h))(\alpha) &= \textstyle\sum_{\beta+\gamma=\alpha} f(\beta)(g+h)(\gamma)\\ &= \textstyle\sum_{\beta+\gamma=\alpha} f(\beta)(g(\gamma)+h(\gamma))\\ &= \textstyle\sum_{\beta+\gamma=\alpha} f(\beta)g(\gamma) + \sum_{\beta+\gamma=\alpha} f(\beta)h(\gamma)\\ &= (fg)(\alpha) + (fh)(\alpha)\\ &= (fg+fh)(\alpha),\end{aligned}$$

por lo que el producto de polinomios es distributivo respecto de la suma. □

Vanos a utilizar la siguiente notación. Para cada $\alpha \in \mathbb{N}^n$, abreviamos

$$X^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

Dado $\alpha \in \mathbb{N}^n$, denotamos por aX^α la aplicación definida por

$$(aX^\alpha)(\beta) = \begin{cases} a & \text{si } \alpha = \beta, \\ 0 & \text{si } \alpha \neq \beta. \end{cases}$$

Observemos que $X^0 = 1$.

Proposición 2.2. *Todo polinomio no nulo* $f \in A[x_1, \ldots, x_n]$ *se escribe de manera única como* $f = \sum_{\alpha \in \operatorname{supp}(f)} a_\alpha X^\alpha$.

Demostración. Si llamamos $a_\alpha = f(\alpha)$ para cada $\alpha \in \mathbb{N}^n$, es inmediato comprobar que

$$f(\beta) = \left(\sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha\right)(\beta)$$

para todo $\beta \in \mathbb{N}^n$. Por otro lado,

$$\left(\sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha\right)(\beta) = \left(\sum_{\alpha \in \operatorname{supp}(f)} a_\alpha X^\alpha\right)(\beta),$$

ya que fuera del soporte los valores que toma el polinomio son cero. □

El elemento $aX^\alpha = ax_1^{\alpha_1} \cdots x_n^{\alpha_n}$ tiene dos significados. Por una parte es un monomio que representa una aplicación concreta de $\mathbb{N}^n$ en A, y por otra parte es un producto múltiple de los polinomios, aX^0 y $x_i = X^{\epsilon_i}$ donde $\epsilon_i = (0, \ldots, \underset{i}{1}, \ldots, 0)$. Como consecuencia del siguiente Lema ambos significados son el mismo.

Lema 2.3. $(aX^\alpha)X^\beta = aX^{\alpha+\beta}$.

Demostración. Si $\gamma \in \mathbb{N}^n$,

$$\begin{aligned}((aX^\alpha)X^\beta)(\gamma) &= \textstyle\sum_{\delta+\lambda=\gamma}(aX^\alpha)(\delta)X^\beta(\lambda)\\ &= \begin{cases} a & \text{si } \delta = \alpha \text{ y } \lambda = \beta \\ 0 & \text{en otro caso}\end{cases}\\ &= (aX^{\alpha+\beta})(\gamma),\end{aligned}$$

por lo que $(aX^\alpha)X^\beta = aX^{\alpha+\beta}$. □

Proposición 2.4. $A[x, y] \cong A[x][y]$.

Demostración. El isomorfismo se define como

$$f \mapsto [j \mapsto [i \mapsto f(i, j)]]$$

para cada $f : \mathbb{N}^2 \to A$. Dejo como ejercicio, natural pero tedioso, comprobar que esta aplicación respeta la suma y el producto. □

Corolario 2.5. $A[x_1, \ldots, x_n] \cong A[x_1] \cdots [x_n]$.

2.2 Órdenes admisibles

En el conjunto de los números naturales consideramos el orden usual heredado de la aritmética, es decir,

$$n \leq m \iff m = n + c.$$

Por supuesto este orden puede extenderse al orden producto en $\mathbb{N}^n$. El orden producto no es un orden total. Denotemos por $\leq_\prod$ al orden

producto en $\mathbb{N}^n$, es decir, $\alpha \leq_{\prod} \beta$ si y sólo si $\alpha_i \leq \beta_i$ para todo índice $1 \leq i \leq n$, o equivalentemente, $\alpha \leq_{\prod} \beta$ si y sólo si $\beta = \alpha + \gamma$ para cierto $\gamma \in \mathbb{N}^n$.

Teorema 2.6 (Lema de Dickson)**.** *Dado un subconjunto* $\varnothing \neq A \subseteq \mathbb{N}^n$*, existen* $\alpha(1), \ldots, \alpha(s) \in A$ *tales que todo* $\alpha \in A$ *se escribe como* $\alpha = \alpha(i) + \gamma$ *para cierto índice* $1 \leq i \leq s$ *y cierto* $\gamma \in \mathbb{N}^n$*.*

Este teorema se puede expresar diciendo que todo subconjunto no vacío de $\mathbb{N}^n$ tiene sólo una cantidad finita de elementos minimales respecto del orden producto.

Demostración. Para simplificar la exposición, diremos que los elementos $\alpha(1), \ldots, \alpha(s) \in A$ que da el teorema son generadores de A.
Demostramos el teorema por inducción en n. Si $n = 1$, el resultado es consecuencia de que el orden usual en $\mathbb{N}$ es un buen orden luego todo subconjunto no vacío de naturales tiene un mínimo.
Supongamos el resultado cierto para $n-1$ y demostrémoslo para n. Sea

$$\overline{A} = \{\alpha \in \mathbb{N}^{n-1} \mid (\alpha, m) \in A \text{ para algún } m \in \mathbb{N}\}.$$

Por hipótesis de inducción existen $\overline{\alpha}(1), \ldots, \overline{\alpha}(s) \in \overline{A}$ generadores de A. Para cada $1 \leq i \leq s$, definimos

$$m_i = \text{mín}\{n \in \mathbb{N} \mid (\overline{\alpha}(i), n) \in A\}$$

y

$$m = \text{máx}\{m_1, \ldots, m_s\}.$$

Para cada $0 \leq \ell \leq m - 1$, sea

$$A_\ell = \{\alpha \in \mathbb{N}^{n-1} \mid (\alpha, \ell) \in A\}$$

y sea $\{\ell_1 < \cdots < \ell_t\} = \{\ell < m \mid A_\ell \neq \varnothing\}$. De nuevo por hipótesis de inducción, para cada $\ell_1 \leq \ell_j \leq \ell_t$ existen $\alpha^{\ell_j}(1), \ldots, \alpha^{\ell_j}(s_j) \in A_{\ell_j}$ generadores de A_{ℓ_j}.
Sea $(\alpha, p) \in A$ con $\alpha \in \mathbb{N}^{n-1}$ y $p \in \mathbb{N}$. Supongamos que $p \geq m$. Como $\alpha \in \overline{A}$, existe $1 \leq i \leq s$ y $\gamma \in \mathbb{N}^{n-1}$ tales que $\alpha = \overline{\alpha}(i) + \gamma$. Dado que $m \geq m_i$ tenemos que $(\alpha, p) = (\overline{\alpha}(i), m_i) + (\gamma, p - m_i)$. Supongamos por el contrario que $p < m$. En este segundo caso $p = \ell_j$ para algún $1 \leq j \leq t$ y $\alpha \in A_{\ell_j}$. Existen por tanto $1 \leq i \leq s_j$ y $\gamma \in \mathbb{N}^{n-1}$ tales que $\alpha = \alpha^{\ell_j}(i) + \gamma$, por lo que $(\alpha, p) = (\alpha, \ell_j) = (\alpha^{\ell_j}(i) + \gamma, \ell_j) = (\alpha^{\ell_j}(i), \ell_j) + (\gamma, 0)$. Acabamos de demostrar que

$$\begin{aligned}\big\{&(\overline{\alpha}(1), m_1), \ldots, (\overline{\alpha}(s), m_s),\\ &(\alpha^{\ell_1}(1), \ell_1), \ldots, (\alpha^{\ell_1}(s_1), \ell_1), \ldots,\\ &(\alpha^{\ell_t}(1), \ell_t), \ldots, (\alpha^{\ell_t}(s_t), \ell_t)\big\}\end{aligned}$$

generan A, lo que demuestra el teorema. □

Un orden total $\leq$ sobre $\mathbb{N}^n$ se dice admisible si $0 = (0, \ldots, 0)$ es mínimo para $\leq$ y para $\alpha, \beta, \gamma \in \mathbb{N}^n$, si $\alpha < \beta$ entonces $\alpha + \gamma < \beta + \gamma$, donde $\alpha < \beta$ tiene el significado habitual, $\alpha \leq \beta$ y $\alpha \neq \beta$.

Lema 2.7. *Todo orden admisible extiende al orden producto, es decir, si $\leq$ es un orden admisible y $\beta = \alpha + \gamma$ entonces $\alpha \leq \beta$.*

Demostración. Inmediato, ya que $0 \leq \gamma$ implica $\alpha \leq \alpha + \gamma = \beta$. □

Veamos algunos ejemplos:

Ejemplo 2.8. *Orden lexicográfico.* Definimos el siguiente orden en $\mathbb{N}^n$:

$$\alpha \leq_{\text{LEX}} \beta \iff \begin{cases} \alpha = \beta & \text{o} \\ \alpha_i < \beta_i & \text{donde } i \text{ es el primer índice en el que } \alpha_i \neq \beta_i. \end{cases}$$

La admisibilidad de este orden es consecuencia inmediata de la admisibilidad del orden natural en $\mathbb{N}$.

Ejemplo 2.9. *Órdenes graduados.* Sea $\omega \in \mathbb{R}^n$. Para cada $\alpha \in \mathbb{N}^n$, definimos el ω-grado de α como

$$\langle \alpha, \omega \rangle = \alpha_1 \omega_1 + \cdots + \alpha_n \omega_n.$$

Un orden admisible $\leq$ se dice ω–*graduado* si $\alpha \leq \beta$ implica que $\langle \alpha, \omega \rangle \leq \langle \beta, \omega \rangle$. Si $\leq$ es un orden admisible sobre $\mathbb{N}^n$, hay una forma natural de definir un orden ω–graduado asociado a $\leq$ y que denotaremos $\leq_\omega$,

$$\alpha \leq_\omega \beta \iff \begin{cases} \langle \alpha, \omega \rangle < \langle \beta, \omega \rangle & \text{o} \\ \langle \alpha, \omega \rangle = \langle \beta, \omega \rangle \text{ y } \alpha \leq \beta. \end{cases}$$

Hay varios casos particulares de esta construcción. Si $\omega = (1, \ldots, 1)$, decimos que el orden es graduado y denotamos el grado (total) como

$$|\alpha| = \langle \alpha, (1, \ldots, 1) \rangle = \alpha_1 + \cdots + \alpha_n.$$

En este caso usamos la notaciones

$$\leq_{(1,\ldots,1)} = \leq_{\text{DEG}}, \quad (\leq_{\text{LEX}})_{\text{DEG}} = \leq_{\text{DEGLEX}}.$$

También empleamos

$$(\leq_{\text{LEX}})_\omega = \leq_{\omega\text{–LEX}}.$$

Ejemplo 2.10. *Orden lexicográfico graduado inverso*. Este orden también es muy empleado

$$\alpha \leq_{\text{DEGREVLEX}} \beta \iff \begin{cases} |\alpha| < |\beta| & \text{o} \\ |\alpha| = |\beta| \quad \text{y} \\ \quad \alpha_i > \beta_i \text{ donde } i \text{ es el último índice en el que } \alpha_i \neq \beta_i. \end{cases}$$

Proposición 2.11. *Todo orden admisible es un buen orden. En particular satisface la Condición de Cadena Descendente.*

Demostración. Sea $\leq$ un orden admisible en $\mathbb{N}^n$ y sea $\varnothing \neq A \subseteq \mathbb{N}^n$. Por el Lema de Dickson (Teorema 2.6) existe $\{\alpha(1), \ldots, \alpha(s)\} \subseteq A$ que lo generan. Todo conjunto finito totalmente ordenado está bien ordenado, luego $\{\alpha(1), \ldots, \alpha(s)\}$ tiene mínimo, al que llamamos $\alpha(i_0)$. Dado $\alpha \in A$,

$$\alpha = \alpha(i) + \gamma \geq \alpha(i) \geq \alpha(i_0),$$

ya que el orden es admisible, luego $\alpha(i_0) = \text{mín}(A)$. □

2.3 Propiedades de los polinomios

Sea $A[x_1, \ldots, x_n]$ un anillo de polinomios con coeficientes en A y fijemos un orden admisible $\leq$ en $\mathbb{N}^n$.
Dado $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha X^\alpha \in A[x_1, \ldots, x_n]$, definimos su

exponente $\exp(f) = \max_{\leq}(\mathrm{supp}(f))$,

monomio líder $\mathrm{lm}(f) = X^{\exp(f)}$,

coeficiente líder $\mathrm{lc}(f) = c_{\exp(f)}$,

término líder $\mathrm{lt}(f) = \mathrm{lc}(f)\,\mathrm{lm}(f) = c_{\exp(f)}X^{\exp(f)}$.

Proposición 2.12. *Dados* $f, g \in A[x_1, \ldots, x_n]$ *no nulos,* $\exp(f+g) \leq \max\{\exp(f), \exp(g)\}$*, y se tiene la igualdad salvo que* $\exp(f) = \exp(g)$ *y* $\mathrm{lc}(f) = -\mathrm{lc}(g)$.

Demostración. Si $\alpha > \max\{\exp(f), \exp(g)\}$, tenemos que $(f+g)(\alpha) = f(\alpha)+g(\alpha) = 0+0 = 0$, luego $\exp(f+g) \leq \max\{\exp(f), \exp(g)\}$. Por otra parte, supongamos sin perder generalidad que $\exp(f) \geq \exp(g)$, por lo que $\max\{\exp(f), \exp(g)\} = \exp(f)$. Tenemos que

$$(f+g)(\exp(f)) = \mathrm{lc}(f) + g(\exp(f)) = \begin{cases} \mathrm{lc}(f) & \text{si } \exp(f) > \exp(g) \\ \mathrm{lc}(f) + \mathrm{lc}(g) & \text{si } \exp(f) = \exp(g) \end{cases}$$

por lo que $(f+g)(\max\{\exp(f), \exp(g)\}) = 0$ si y sólo si $\exp(f) = \exp(g)$ y $\mathrm{lc}(f) + \mathrm{lc}(g) = 0$. □

Proposición 2.13. *Dados* $f, g \in A[x_1, \ldots, x_n]$ *no nulos,* $\exp(fg) \leq \exp(f) + \exp(g)$*, y se tiene la igualdad salvo que* $\mathrm{lc}(f)\,\mathrm{lc}(g) = 0$.

Demostración. Sea $\alpha > \exp(f)+\exp(g)$. Si $\beta+\gamma = \alpha$, necesariamente $\beta > \exp(f)$ o $\gamma > \exp(g)$, por lo que

$$(fg)(\alpha) = \sum_{\beta+\gamma=\alpha} f(\beta)g(\gamma) = 0.$$

Consequentemente $\exp(fg) \leq \exp(f) + \exp(g)$.
Si $\beta + \gamma = \exp(f) + \exp(g)$ y $\beta < \exp(f)$, tenemos que $\gamma > \exp(g)$, por lo que

$$(fg)(\exp(f) + \exp(g)) = \sum_{\beta+\gamma=\exp(f)+\exp(g)} f(\beta)g(\gamma) = \mathrm{lc}(f)\,\mathrm{lc}(g),$$

por lo que $\exp(fg) < \exp(f) + \exp(g)$ si y solo si $\mathrm{lc}(f)\,\mathrm{lc}(g) = 0$. □

Corolario 2.14. *Si* A *es un dominio,* $A[x_1, \ldots, x_n]$ *también lo es.*

2.4 Espacio afín y ecuaciones polinómicas

Sea $\mathbb{F}$ un cuerpo. El espacio $\mathbb{F}^n$ recibe el nombre de espacio afín de dimensión n.
Asociado a cada polinomio $f = \sum_{\alpha\in\mathbb{N}^n} c_\alpha X^\alpha \in \mathbb{F}[x_1, \ldots, x_n]$ tenemos la aplicación de evaluación definida por

$$\mathrm{ev}_f : \mathbb{F}^n \to \mathbb{F},\ \left[\mathrm{ev}_f(a_1, \ldots, a_n) = \sum_{\alpha\in\mathbb{N}^n} c_\alpha a_1^{\alpha_1} \cdots a_n^{\alpha_n}\right]$$

Proposición 2.15. *Supongamos que* $\mathbb{F}$ *es infinito. Entonces* $\mathrm{ev}_f = 0$ *si y sólo si* $f = 0$.

Demostración. Inducción en n. Si $n = 1$, el resultado es consecuencia de que todo polinomio en $\mathbb{F}[x_1]$ de grado m tiene como máximo m raíces. Por tanto si un polinomio se anula en infinitos valores, tiene que ser necesariamente el polinomio 0.
Supongamos el resultado cierto para polinomios en $\mathbb{F}[x_1, \ldots, x_{n-1}]$ y sea $f \in \mathbb{F}[x_1, \ldots, x_n]$ tal que $f(a_1, \ldots, a_n) = 0$ para cualquier

$(a_1, \ldots, a_n) \in \mathbb{F}^n$. Por la Proposición 2.4,

$$f(x_1, \ldots, x_n) = \sum_{i=0}^{m} g_i(x_1, \ldots, x_{n-1}) x_n^i.$$

Sea $(a_1, \ldots, a_{n-1}) \in \mathbb{F}^{n-1}$. Llamemos $c_i = g_i(a_1, \ldots, a_{n-1})$ y sea $\overline{f} = \sum_{i=0}^{m} c_i x_n^i$. Para cualquier $a_n \in \mathbb{F}$ tenemos que

$$\begin{aligned} \overline{f}(a_n) &= \sum_{i=0}^{m} c_i a_n^i \\ &= \sum_{i=0}^{m} g_i(a_1, \ldots, a_{n-1}) a_n^i = f(a_1, \ldots, a_n) = 0, \end{aligned}$$

luego por el caso $n = 1$ tenemos que $c_i = 0$ para cada $0 \leq i \leq m$, es decir, $g_i(a_1, \ldots, a_{n-1}) = 0$ para cada $0 \leq i \leq m$. Por hipótesis de inducción tenemos que $g_i(x_1, \ldots, x_{n-1}) = 0$ para cada $0 \leq i \leq m$, por lo que $f(x_1, \ldots, x_n) = 0$. □

Corolario 2.16. *Si $\mathbb{F}$ es infinito y $f, g \in \mathbb{F}[x_1, \ldots, x_n]$, $f = g$ si y sólo si $ev_f = ev_g$.*

En vista de los resultados anteriores podemos identificar cada polinomio con su función de evaluación, por lo que usaremos el mismo símbolo, es decir, $f(a_1, \ldots, a_n) = ev_f(a_1, \ldots, a_n)$. En el caso infinito esto no produce ambigüedad alguna. En el caso finito sí puede producirla, pero el contexto nos aclarará si nos referimos al polinomio o a su función de evaluación. De hecho tenemos este resultado en el caso finito.

Proposición 2.17. *Sea $\mathbb{F}$ un cuerpo finito, y sea $\varphi : \mathbb{F}^n \to \mathbb{F}$ una aplicación. Existe un polinomio $f \in \mathbb{F}[x_1, \ldots, x_n]$ tal que $\varphi = ev_f$.*

Demostración. Inducción en n. Si $n = 1$, podemos tomar como $f \in \mathbb{F}[x_1]$ el polinomio de interpolación en los puntos $\{(c, \varphi(c)) \mid c \in$

$\mathbb{F}\}$. Supongamos el resultado cierto para $n-1$ y sea $\varphi : \mathbb{F}^n \to \mathbb{F}$. Para cada $c \in \mathbb{F}$, definimos $\varphi_c : \mathbb{F}^{n-1} \to \mathbb{F}$ como la aplicación $\varphi_c(a_1,\ldots,a_{n-1}) = \varphi(a_1,\ldots,a_{n-1},c)$. Por hipótesis de inducción existe un polinomio $f_c \in \mathbb{F}[x_1,\ldots,x_{n-1}]$ tal que $\varphi_c(a_1,\ldots,a_{n-1}) = f_c(a_1,\ldots,a_{n-1})$ para cada $(a_1,\ldots,a_{n-1}) \in \mathbb{F}^{n-1}$. Sea

$$f(x_1,\ldots,x_n) = \sum_{c\in\mathbb{F}} f_c(x_1,\ldots,x_{n-1}) \prod_{\substack{d\in\mathbb{F}\\ d\neq c}} \frac{(x_n-d)}{(c-d)}.$$

Por la Proposición 2.4 $f \in \mathbb{F}[x_1,\ldots,x_n]$. Además

$$\begin{aligned} f(a_1,\ldots,a_n) &= \sum_{c\in\mathbb{F}} f_c(a_1,\ldots,a_{n-1}) \prod_{\substack{d\in\mathbb{F}\\ d\neq c}} \frac{(a_n-d)}{(c-d)} \\ &= f_{a_n}(a_1,\ldots,a_{n-1}) \prod_{\substack{d\in\mathbb{F}\\ d\neq a_n}} \frac{(a_n-d)}{(a_n-d)} \\ &= \varphi_{a_n}(a_1,\ldots,a_{n-1}) \\ &= \varphi(a_1,\ldots,a_n), \end{aligned}$$

lo que demuestra el resultado. □

Aunque los resultados anteriores demuestran que no hay una correspondencia entre polinomios y sus evaluaciones, sí tenemos esa correspondencia si los polinomios tienen grado acotado. Concretamente, si $f \in \mathbb{F}[x_1,\ldots,x_n]$, llamamos

$$\deg_i(f) = \max\{\alpha_i \mid \alpha \in \operatorname{supp}(f)\}.$$

Proposición 2.18. *Sea* $\mathbb{F}_q$ *el cuerpo con* q *elementos. Sea* $f \in \mathbb{F}_q[x_1,\ldots,x_n]$ *tal que* $\deg_i(f) < q$. *Entonces* $\operatorname{ev}_f = 0$ *si y sólo si* $f = 0$.

Demostración. Inducción en n. Si $n = 1$, el resultado es consecuencia de que todo polinomio en $\mathbb{F}[x_1]$ de grado m tiene como máximo m

raíces. Por tanto si un polinomio tiene grado menor que q y se anula en q valores, tiene que ser necesariamente el polinomio 0.
Supongamos el resultado cierto para polinomios en $\mathbb{F}_q[x_1,\dots,x_{n-1}]$ y sea $f \in \mathbb{F}_q[x_1,\dots,x_n]$ tal que $\deg_i(f) < q$ para todo $1 \leq i \leq n$, y tal que $f(a_1,\dots,a_n) = 0$ para cualquier $(a_1,\dots,a_n) \in \mathbb{F}^n$. Por la Proposición 2.4,

$$f(x_1,\dots,x_n) = \sum_{i=0}^{m} g_i(x_1,\dots,x_{n-1})x_n^i,$$

con $\deg_j(g_i) < q$ para $0 \leq i \leq m < q$ y $1 \leq j \leq n-1$. Sea $(a_1,\dots,a_{n-1}) \in \mathbb{F}^{n-1}$. Llamemos $c_i = g_i(a_1,\dots,a_{n-1})$ y sea $\overline{f} = \sum_{i=0}^{m} c_i x_n^i$. Para cualquier $a_n \in \mathbb{F}$ tenemos que

$$\begin{aligned}\overline{f}(a_n) &= \sum_{i=0}^{m} c_i a_n^i \\ &= \sum_{i=0}^{m} g_i(a_1,\dots,a_{n-1})a_n^i = f(a_1,\dots,a_n) = 0,\end{aligned}$$

luego por el caso $n = 1$, dado que $m < q$, tenemos que $c_i = 0$ para cada $0 \leq i \leq m$, es decir, $g_i(a_1,\dots,a_{n-1}) = 0$ para cada $0 \leq i \leq m$. Por hipótesis de inducción tenemos que $g_i(x_1,\dots,x_{n-1}) = 0$ para cada $0 \leq i \leq m$, por lo que $f(x_1,\dots,x_n) = 0$. □

Finalizamos la sección con dos propiedades sencillas cuya demostración es consecuencia directa de la definición.

Proposición 2.19. *Dados $f, g \in \mathbb{F}[x_1,\dots,x_n]$ y $(a_1,\dots,a_n) \in \mathbb{F}^n$, se tiene que*

$$(f+g)(a_1,\dots,a_n) = f(a_1,\dots,a_n) + g(a_1,\dots,a_n)$$

y

$$(fg)(a_1,\dots,a_n) = f(a_1,\dots,a_n)g(a_1,\dots,a_n).$$

Demostración. Es consecuencia del Lema 2.3. □

2.5 Variedades afines

Definición 2.20. Sea $F \subseteq \mathbb{F}[x_1, \ldots, x_n]$. Se define la variedad afín asociada a F como

$$\mathbf{V}(F) = \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f(a_1, \ldots, a_n) = 0 \ \forall f \in F\}.$$

Proposición 2.21. *$\varnothing$ y $\mathbb{F}^n$ son variedades afines. La intersección y la unión de dos variedades afines es una variedad afín.*

Demostración. $\varnothing = \mathbf{V}(\{1\})$ y $\mathbb{F}^n = \mathbf{V}(\{0\})$. Es fácil comprobar que $\mathbf{V}(F) \cap \mathbf{V}(G) = \mathbf{V}(F \cup G)$. Por otra parte, dados $F, G \subseteq \mathbb{F}[x_1, \ldots, x_n]$, definimos $FG = \{fg \mid f \in F, g \in G\}$. Veamos que $\mathbf{V}(F) \cup \mathbf{V}(G) = \mathbf{V}(FG)$. Si $(a_1, \ldots, a_n) \in \mathbf{V}(F)$, tenemos que, para cada $f \in F$, $f(a_1, \ldots, a_n) = 0$. Por tanto

$$(fg)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = 0$$

para cualquier g por lo que $\mathbf{V}(F) \subseteq \mathbf{V}(FG)$. Análogamente $\mathbf{V}(G) \subseteq \mathbf{V}(FG)$, de donde $\mathbf{V}(F) \cup \mathbf{V}(G) \subseteq \mathbf{V}(FG)$. Sea $(a_1, \ldots, a_n) \in \mathbf{V}(FG)$ y supongamos que $(a_1, \ldots, a_n) \notin \mathbf{V}(F)$, debe existir un $f_0 \in F$ tal que $f_0(a_1, \ldots, a_n) \neq 0$. Si $g \in G$, como $(a_1, \ldots, a_n) \in \mathbf{V}(FG)$ tenemos que $0 = (f_0 g)(a_1, \ldots, a_n) = f_0(a_1, \ldots, a_n)g(a_1, \ldots, a_n)$, de donde $g(a_1, \ldots, a_n) = 0$ y $(a_1, \ldots, a_n) \in \mathbf{V}(G)$. Con esto demostramos que $\mathbf{V}(FG) \subseteq \mathbf{V}(F) \cup \mathbf{V}(G)$, lo que termina la demostración. □

Proposición 2.22. $\mathbf{V}(F) = \mathbf{V}(\langle F \rangle)$.

Demostración. Como $F \subseteq \langle F \rangle$, es inmediato que $\mathbf{V}(\langle F \rangle) \subseteq \mathbf{V}(F)$. Sea $(a_1, \ldots, a_n) \in \mathbf{V}(F)$ y $f \in \langle F \rangle$. Existen $f_1, \ldots, f_s \in F$ y $g_1, \ldots, g_s \in \mathbb{F}[x_1, \ldots, x_n]$ tales que $f = g_1 f_1 + \cdots + g_s f_s$. Por tanto

$$\begin{aligned} f(a_1, \ldots, a_n) &= g_1(a_1, \ldots, a_n) f_1(a_1, \ldots, a_n) + \\ &\quad + \cdots + g_s(a_1, \ldots, a_n) f_s(a_1, \ldots, a_n) \\ &= g_1(a_1, \ldots, a_n) 0 + \cdots + g_s(a_1, \ldots, a_n) 0 \\ &= 0, \end{aligned}$$

por lo que $(a_1, \ldots, a_n) \in \mathbf{V}(\langle F \rangle)$. □

Proposición 2.23. *Sean* I, J *ideales en* $\mathbb{F}[x_1, \ldots, x_n]$. *Entonces* $\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$.

Demostración. Como $IJ \subseteq I \cap J$, tenemos que $\mathbf{V}(I \cap J) \subseteq \mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$.
Por otra parte, como $I \cap J \subseteq I$ tenemos que $\mathbf{V}(I) \subseteq \mathbf{V}(I \cap J)$. Análogamente $\mathbf{V}(J) \subseteq \mathbf{V}(I \cap J)$, por lo que $\mathbf{V}(I) \cup \mathbf{V}(J) \subseteq \mathbf{V}(I \cap J)$. □

Tenemos la construcción inversa.

Proposición 2.24. *Sea* $A \subseteq \mathbb{F}^n$ *y sea*

$$\mathbf{I}(A) = \{f \in \mathbb{F}[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \ \forall (a_1, \ldots, a_n) \in A\}.$$

Entonces $\mathbf{I}(A)$ *es un ideal de* $\mathbb{F}[x_1, \ldots, x_n]$.

Demostración. Observemos primero que $0 \in \mathbf{I}(A)$. Supongamos que $f_1, f_2 \in \mathbf{I}(A)$. Si $(a_1, \ldots, a_n) \in A$,

$$(f_1 + f_2)(a_1, \ldots, a_n) = f_1(a_1, \ldots, a_n) + f_2(a_1, \ldots, a_n) = 0 + 0 = 0,$$

por lo que $f_1+f_2 \in \mathbf{I}(A)$. Por otra parte, si $f \in \mathbf{I}(A)$, $g \in \mathbb{F}[x_1,\ldots,x_n]$ y $(a_1,\ldots,a_n) \in A$,

$$(gf)(a_1,\ldots,a_n) = g(a_1,\ldots,a_n)f(a_1,\ldots,a_n) \\ = g(a_1,\ldots,a_n)0 = 0,$$

por lo que $gf \in \mathbf{I}(A)$. □

Definición 2.25. Se define el ideal asociado a $A \subseteq \mathbb{F}^n$ como $\mathbf{I}(A)$.

Proposición 2.26. *Si* $F \subseteq \mathbb{F}[x_1,\ldots,x_n]$, $\langle F\rangle \subseteq \mathbf{I}(\mathbf{V}(F))$, *pudiendo ser la inclusión estricta. Si* $A \subseteq \mathbb{F}^n$, $A \subseteq \mathbf{V}(\mathbf{I}(A))$ *y se tiene la igualdad si y solo si* A *es una variedad afín.*

Demostración. Se propone como ejercicio. □

Corolario 2.27. $\mathbf{V}(\mathbf{I}(A))$ *es la menor variedad que contiene a* A.

Demostración. Sea $A \subseteq V$ con V variedad. Tenemos que

$$A \subseteq V \Rightarrow \mathbf{I}(A) \supseteq \mathbf{I}(V) \Rightarrow \mathbf{V}(\mathbf{I}(A)) \subseteq \mathbf{V}(\mathbf{I}(V)).$$

Dado que $\mathbf{V}(\mathbf{I}(V)) = V$ por la Proposición 2.26, tenemos que $\mathbf{V}(\mathbf{I}(A)) \subseteq V$, lo que demuestra el corolario. □

Corolario 2.28. *Sean* $V, W \subseteq \mathbb{F}^n$ *variedades afines. Entonces se tiene que* $V = W \iff \mathbf{I}(V) = \mathbf{I}(W)$.

2.6 Representación paramétrica de variedades

Hemos presentado las variedades a partir de ecuaciones. De esa forma es fácil averiguar si un punto dado del espacio afín pertenece a la variedad o no, pero no es sencillo "fabricar" puntos de la variedad.

Ejemplo 2.29. Sea $V = \mathbf{V}(x^2 + y^2 - 1) \subseteq \mathbb{R}^2$. Una forma de obtener puntos de dicha variedad es la siguiente:

$$x = \frac{1 - t^2}{1 + t^2}$$
$$y = \frac{2t}{1 + t^2}$$

con $t \in \mathbb{R}$.

Sea $R = \mathbb{F}[t_1, \ldots, t_r]$. En $R \times R \setminus \{0\}$ definimos la siguiente relación: $(f, g) \sim (c, d) \iff fd = cg$.

Lema 2.30. $\sim$ *es una relación de equivalencia.*

Demostración. Las propiedades reflexiva y simétrica son triviales. Para comprobar la propiedad transitiva, si $(f, g) \sim (c, d)$ y $(c, d) \sim (a, b)$, tenemos que $fd = cg$ y $cb = ad$. Por tanto

$$fbd = cgb = gad,$$

como $d \neq 0$ y R es un dominio, tenemos que $fb = ag$, es decir, $(f, g) \sim (a, b)$. □

La clase de equivalencia de un par (f, g) se representa por $\frac{f}{g}$.
En $R \times R \setminus \{0\}$ definimos la siguiente aritmética

$$(a, b) + (c, d) = (ad + bc, bd), \quad (a, b)(c, d) = (ac, bd).$$

Lema 2.31. *Si* $(a, b) \sim (a', b')$ *y* $(c, d) \sim (c', d')$, *entonces* $(a, b) + (c, d) \sim (a', b') + (c', d')$ *y* $(a, b)(c, d) \sim (a', b')(c', d')$.

Demostración. De las siguientes identidades, $ab' = a'b$, $cd' = c'd$, deducimos que

$$\begin{aligned}(ad + bc)b'd' &= adb'd' + bcb'd' \\ &= a'bdd' + bb'c'd = (a'd' + b'c')bd,\end{aligned}$$

luego $(ad + bc, bd) \sim (a'd' + b'c', b'd')$. Además

$$(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd),$$

luego $(ac, bd) \sim (a'c', b'd')$. □

Como consecuencia del lema anterior, las operaciones definidas en $R \times R \setminus \{0\}$ pueden extenderse a $(R \times R \setminus \{0\}) / \sim$.

Proposición 2.32. $((R \times R \setminus \{0\}) / \sim, +, \cdot)$ *es un cuerpo.*

Demostración. Ejercicio. □

Definición 2.33. $(R \times R \setminus \{0\}) / \sim$ es el cuerpo de funciones racionales de $\mathbb{F}[t_1, \ldots, t_r]$, y se denota $\mathbb{F}(t_1, \ldots, t_r)$.

Definición 2.34. Una representación paramétrica racional de una variedad afín $V = \mathbf{V}(F) \subseteq \mathbb{F}^n$, consiste en un conjunto de funciones racionales $r_1, \ldots, r_n \in \mathbb{F}(t_1, \ldots, t_r)$ tales que

$$(x_1, \ldots, x_n) \in V \iff \begin{cases} x_1 = r_1(t_1, \ldots, t_r) \\ \qquad \vdots \\ x_n = r_n(t_1, \ldots, t_r) \end{cases}$$

Asociado a las variedades afines tenemos dos problemas a los que daremos respuesta en este curso.

- ¿Tiene toda variedad afín una representación paramétrica racional?
- Dada una representación paramétrica racional, ¿podemos encontrar $F \subseteq \mathbb{F}[x_1, \ldots, x_n]$ tal que $\mathbf{V}(F)$ es la variedad asociada a la representación anterior?.

Ejercicios sobre Sistemas de ecuaciones y variedades afines

Ejercicio 2.1. Demuestra la Proposición 2.4.

Ejercicio 2.2. Comprueba que $\leq_{\text{LEX}}$, $\leq_{\omega-\text{LEX}}$ y $\leq_{\text{DEGREVLEX}}$ son órdenes admisibles.

Ejercicio 2.3. Sea $A = \{(a, b) \in \mathbb{N}^2 \mid a + b \geq 10, ab \leq 21, 25b \leq 60a - 3a^2\}$. Encuentra un conjunto de generadores para A aplicando la demostración del Lema de Dickson.

Ejercicio 2.4. Demuestra la Proposición 2.26.

Ejercicio 2.5. Demuestra la Proposición 2.32.

Ejercicio 2.6. Sea $\varphi : \mathbb{F}_5 \to \mathbb{F}_5$ la aplicación definida por $\varphi(a) = 2^a$. Encuentra un polinomio $f \in \mathbb{F}_5[x]$ tal que $\varphi = \text{ev}_f$.

Ejercicio 2.7. Sea $\varphi : \mathbb{F}_3^2 \to \mathbb{F}_3$ la aplicación definida por $\varphi(a, b) = a^b$. Encuentra un polinomio $f \in \mathbb{F}_3[x, y]$ tal que $\varphi = \text{ev}_f$.

Ejercicio 2.8. Sea $f(x) = x^q - x \in \mathbb{F}_q[x]$. Comprueba que $\text{ev}_f = 0$.

Ejercicio 2.9. "Dibuja" las variedades en $\mathbb{R}^2$

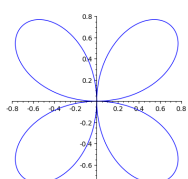
1. $\mathbf{V}(x^2 + 4y^2 + 2x - 16y + 1)$,
2. $\mathbf{V}(x^2 - y^2)$,
3. $\mathbf{V}(2x + y - 1, 3x - y + 2)$.

Ejercicio 2.10. Demuestra que cualquier conjunto finito de puntos es una variedad afín.

Ejercicio 2.11. "Dibuja" las siguientes variedades en $\mathbb{R}^3$:

1. $\mathbf{V}(x^2 + y^2 + z^2 - 1)$,
2. $\mathbf{V}(x^2 + y^2 - 1)$,
3. $\mathbf{V}(xz^2 - xy)$,
4. $\mathbf{V}(x^4 - zx, x^3 - yx)$,
5. $\mathbf{V}(x^2 + y^2 + z^2 - 1, x^2 + y^2 + (z-1)^2 - 1)$,
6. $\mathbf{V}((x-2)(x^2 - y), y(x^2 - y), (z+1)(x^2 - y))$.

Ejercicio 2.12. Consideremos el trébol de cuatro hojas. cuyas coordenadas polares son $r = \sin(2\theta)$, es decir,



$$T = \{(\sin(2\theta)\cos(\theta), \sin(2\theta)\sin(\theta)) \mid 0 \leq \theta \leq 2\pi\}.$$

Demuestra que $T = \mathbf{V}\left((x^2 + y^2)^3 - 4x^2y^2\right)$.

Ejercicio 2.13. Consideremos un robot con tres brazos que se mueve en $\mathbb{R}^2$. El primer brazo está anclado en el origen de coordenadas, tiene longitud 3 y mueve su extremo libremente. El segundo está anclado al extremo del primer brazo, tiene longitud 2 y se mueve libremente. El tercero tiene longitud 1, está anclado al extremo del segundo brazo y se mueve también libremente. Un estado del robot consiste en las coordenadas de los extremos de cada uno de los brazos. Describe el conjunto de los estados posibles como variedad afín. Si (u, v) son las coordenadas del extremo del tercer brazo, demuestra que $u^2 + v^2 \leq 36$, y que cualquier punto en el disco de radio 6 puede ser el extremo del tercer brazo.

Capítulo 3

Bases de Gröbner y Algoritmos Básicos

3.1 Ideales en $\mathbb{N}^n$

Definición 3.1. Un subconjunto $\varnothing \neq M \subseteq \mathbb{N}^n$ se dice ideal si $M = M + \mathbb{N}^n$. Se dice que un ideal $M \subseteq \mathbb{N}^n$ está generado por $F \subseteq M$ si $M = F + \mathbb{N}^n$.

Teorema 3.2 (Lema de Dickson)**.** *Todo ideal en $\mathbb{N}^n$ está finitamente generado.*

Demostración. Consecuencia directa del Teorema 2.6. □

En realidad es sencillo comprobar que los Teoremas 2.6 y 3.2 son equivalentes.
Dado $F \subseteq \mathbb{F}[x_1, \ldots, x_n]$, definimos

$$\exp(F) = \{\exp(f) \mid f \in F \setminus \{0\}\}.$$

Proposición 3.3. *Si $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ es un ideal no nulo, entonces* $\exp(I)$ *es un ideal en $\mathbb{N}^n$.*

Demostración. Sea $\alpha \in \exp(I)$ y $\beta \in \mathbb{N}^n$. Existe $f \in I$ tal que $\exp(f) = \alpha$. Dado que $X^\beta f \in I$ y $\exp(X^\beta f) = \exp(X^\beta)\exp(f) = \beta+\alpha$, tenemos que $\beta + \alpha \in \exp(I)$, lo que demuestra el resultado. □

3.2 División en $\mathbb{F}[x_1, \ldots, x_n]$

Teorema 3.4. *Sea $\leq$ un orden admisible en $\mathbb{N}^n$ y sea $F = \{f_1, \ldots, f_s\}$ un subconjunto en $\mathbb{F}[x_1, \ldots, x_n]$. Todo elemento $f \in \mathbb{F}[x_1, \ldots, x_n]$ puede escribirse como*

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

para ciertos $q_1, \ldots, q_s, r \in \mathbb{F}[x_1, \ldots, x_n]$, donde

- $\operatorname{supp}(r) \cap (\exp(F) + \mathbb{N}^n) = \varnothing$,
- $r = 0$ *o* $\exp(r) \leq \exp(f)$,
- *para cada* $1 \leq i \leq s$, $q_i f_i = 0$ *o* $\exp(f) \geq \exp(q_i f_i)$.

Demostración. Vamos a demostrar que la salida del Algoritmo 1 satisface las propiedades del teorema. Diremos que $p, q_1, \ldots, q_s, r$ es una etapa correcta de la división si

- $p = 0$ o $\exp(p) \leq \exp(f)$,
- $f = p + q_1 f_1 + \cdots + q_s f_s + r$,
- $\operatorname{supp}(r) \cap (\exp(F) + \mathbb{N}^n) = \varnothing$,
- $r = 0$ o $\exp(r) \leq \exp(f)$,

Algorithm 1 Algoritmo de división multivariable

procedure DIVISION($f, f_1, \ldots, f_s$)
  $p \leftarrow f$
  $r \leftarrow 0$
  for $1 \leq i \leq s$ **do**
    $q_i \leftarrow 0$
  while $p \neq 0$ **do**
    $i \leftarrow 1$
    $step \leftarrow 0$
    while $i \leq s$ **and** $step = 0$ **do**
      if $\exp(p) = \exp(f_i) + \gamma$ **then**
        $q_i \leftarrow q_i + \frac{lc(p)}{lc(f_i)} X^\gamma$
        $p \leftarrow p - \frac{lc(p)}{lc(f_i)} X^\gamma f_i$
        $step \leftarrow 1$
      else
        $i \leftarrow i + 1$
    if $step = 0$ **then**
      $r \leftarrow r + lt(p)$
      $p \leftarrow p - lt(p)$
  return $q_1, \ldots, q_s, r$

- para cada $1 \leq i \leq s$, $q_i f_i = 0$ o $\exp(f) \geq \exp(q_i f_i)$.

Observemos primeramente que los valores iniciales $(p, q_1, \ldots, q_s, r) = (f, 0, \ldots, 0, 0)$ son una etapa correcta de la división. Supongamos por tanto que $p, q_1, \ldots, q_s, r$ son una etapa correcta de la división y sean $p', q_1', \ldots, q_s', r'$ los valores de dichas variables después de una ejecución del bucle **while** principal. Vamos a demostrar que se $\exp(p') < \exp(p)$ y $p', q_1', \ldots, q_s', r'$ también son una etapa correcta de la división.

Supongamos en primer lugar que $\exp(p) \in \exp(F) + \mathbb{N}^n$. Sea $i_0 = \min\{1 \leq i \leq s \mid \exp(p) \in \exp(f_i) + \mathbb{N}^n\}$ y sea $\exp(p) = \exp(f_{i_0}) + \gamma$. En este caso el bucle termina con los siguientes nuevos valores:

$$\begin{aligned} p' &= p - \tfrac{lc(p)}{lc(f_{i_0})} X^\gamma f_{i_0}, \\ q_{i_0}' &= q_{i_0} + \tfrac{lc(p)}{lc(f_{i_0})} X^\gamma, \\ q_j' &= q_j \quad \text{si } j \neq i_0, \\ r' &= r. \end{aligned}$$

Por una parte,

$$\exp(X^\gamma f_{i_0}) = \gamma + \exp(f_{i_0}) = \exp(p)$$

y

$$lc\left(\tfrac{lc(p)}{lc(f_{i_0})} X^\gamma f_{i_0}\right) = \tfrac{lc(p)}{lc(f_{i_0})}\, lc(f_{i_0}) = lc(p),$$

por lo que $\exp(p') < \exp(p)$. Por otra parte,

$$\begin{aligned}\exp(q'_{i_0} f_{i_0}) &= \exp\left(q_{i_0} f_{i_0} + \tfrac{\mathrm{lc}(p)}{\mathrm{lc}(f_{i_0})} X^\gamma f_{i_0}\right)\\ &\leq \max\left\{\exp(q_{i_0} f_{i_0}), \exp\left(\tfrac{\mathrm{lc}(p)}{\mathrm{lc}(f_{i_0})} X^\gamma f_{i_0}\right)\right\}\\ &\leq \max\{\exp(f), \exp(p)\}\\ &= \exp(f).\end{aligned}$$

Finalmente,

$$\begin{aligned}f &= p + q_1 f_1 + \cdots + q_s f_s + r\\ &= p - \tfrac{\mathrm{lc}(p)}{\mathrm{lc}(f_{i_0})} X^\gamma f_{i_0} + q_1 f_1 + \cdots + q_s f_s + \tfrac{\mathrm{lc}(p)}{\mathrm{lc}(f_{i_0})} X^\gamma f_{i_0} + r\\ &= p' + q'_1 f_1 + \cdots + q'_s f_s + r',\end{aligned}$$

por lo que hemos demostrado que $p', q'_1, \ldots, q'_s, r'$ son una etapa correcta de la división.
Supongamos por el contrario que $\exp(p) \notin \exp(F) + \mathbb{N}^n$. En este segundo caso el bucle termina con los siguientes nuevos valores:

$$\begin{aligned}p' &= p - \mathrm{lt}(p)\\ q'_j &= q_j \quad \text{para } 1 \leq j \leq s,\\ r' &= r + \mathrm{lt}(p).\end{aligned}$$

Es inmediato que $p' = 0$ o $\exp(p') < \exp(p) \leq \exp(f)$. Además, $\mathrm{supp}(r') \subseteq \mathrm{supp}(r) \cup \{\exp(p)\}$, por lo que $\mathrm{supp}(r') \cap (\exp(F) + \mathbb{N}^n) = \varnothing$. Finalmente

$$\begin{aligned}f &= p + q_1 f_1 + \cdots + q_s f_s + r\\ &= p - \mathrm{lt}(p) + q_1 f_1 + \cdots + q_s f_s + r + \mathrm{lt}(p)\\ &= p' + q'_1 f_1 + \cdots + q'_s f_s + r',\end{aligned}$$

por lo que en este segundo caso $p', q'_1, \ldots, q'_s, r'$ son también una etapa correcta de la división.
Consecuentemente, si el algoritmo termina la salida satisface las condiciones del teorema. Queda verificar que el algoritmo termina. Sean $p_0, p_1, \ldots$ los diferentes valores que va tomando p en cada bucle del algoritmo. Tal y como hemos observado antes, $\exp(p_i) > \exp(p_{i+1})$, por lo que la cadena debe terminar, es decir, debe existir i_0 tal que $p_{i_0} = 0$. □

El polinomio r que obtenemos como salida del Algoritmo 1 recibe el nombre de resto de la división de f por $[f_1, \ldots, f_s]$, y se denota $r = \mathrm{rem}(f, [f_1, \ldots, f_s])$. Debemos observar que en la división el modo en que están ordenados los elementos de F es esencial como el siguiente ejemplo muestra. Por tanto, el resto se obtiene al dividir un polinomio entre una lista ordenada, no entre un subconjunto. Si $F = \{f_1, \ldots, f_s\}$, denotamos $[F] = [f_1, \ldots, f_s]$.

Ejemplo 3.5. Sean $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$ y $f_2 = y^2 - 1$ polinomios en $\mathbb{Q}[x, y]$. En $\mathbb{N}^2$ consideramos el orden lexicográfico con $(1, 0) > (0, 1)$. Vamos a dividir f entre $F = \{f_1, f_2\} = \{f_2, f_1\}$ considerando las dos posibles ordenaciones.

Cuando $\mathbb{F} = \mathbb{F}_q$ es un cuerpo finito, el algoritmo de la división nos permite afinar un poco más la relación entre variedades e ideales.

Lema 3.6. $\mathbf{I}\left(\mathbb{F}_q^n\right) = \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle$.

Demostración. Dado que $a^q - a = 0$ para cualquier $a \in \mathbb{F}_q$, tenemos que

$$\langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle \subseteq \mathbf{I}\left(\mathbb{F}_q^n\right).$$

Sea $f \in \mathbf{I}\left(\mathbb{F}_q^n\right)$. Fijemos el orden LEX en $\mathbb{F}_q[x_1,\ldots,x_n]$. Por el Teorema 3.4

$$f = \sum_{i=1}^{n} h_i(x_i^q - x_i) + r$$

donde

$$\begin{aligned}\varnothing &= \operatorname{supp}(r) \cap \bigcup_{i=1}^{n} \left(\exp(x_i^q - x_i) + \mathbb{N}^n\right) \\ &= \bigcup_{i=1}^{n} \left(\operatorname{supp}(r) \cap \left(\exp(x_i^q - x_i) + \mathbb{N}^n\right)\right).\end{aligned}$$

Dado que $\operatorname{supp}(r) \cap (\exp(x_i^q - x_i) + \mathbb{N}^n)$ implica que $\deg_i(r) < q$, y que $r \in \mathbf{I}\left(\mathbb{F}_q^n\right)$, por el Teorema 2.18 tenemos que $r = 0$, lo que completa la demostración. □

Proposición 3.7. $\mathbf{V}(F) = \mathbf{V}(F \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\})$.

Demostración. Por el Lema 3.6, $\mathbb{F}_q^n = \mathbf{V}\left(\{x_1^q - x_1, \ldots, x_n^q - x_n\}\right)$. Dado que

$$\mathbf{V}(F \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) = \mathbf{V}(F) \cap \mathbf{V}(\{x_1^q - x_1, \ldots, x_n^q - x_n\}),$$

tenemos el resultado. □

3.3 Bases de Gröbner y Teorema de la base de Hilbert

Definición 3.8. Sea I un ideal en $\mathbb{F}[x_1,\ldots,x_n]$ y sea $\leq$ un orden admisible en $\mathbb{N}^n$. Un subconjunto $G = \{g_1,\ldots,g_t\} \subseteq I$ se dice que es una base de Gröbner para I si $\exp(I) = \exp(G) + \mathbb{N}^n$.

Teorema 3.9. *Sea $\leq$ un orden admisible en $\mathbb{N}^n$ y sea I un ideal en $\mathbb{F}[x_1,\ldots,x_n]$ no nulo tiene una base de Gröbner. Si $G = \{g_1,\ldots,g_t\}$ una base de Gröbner para I entonces $I = \langle G\rangle$.*

Demostración. Por la Proposición 3.3 y el Teorema 3.2, I tiene una base de Gröbner, es decir existe $G = \{g_1, \ldots, g_t\} \subseteq I$ tal que

$$\exp(I) = \exp(G) + \mathbb{N}^n.$$

Veamos que $I = \langle G \rangle$. Para ello sea $f \in I$. Por el Teorema 3.4 existen $q_1, \ldots, q_t, r \in \mathbb{F}[x_1, \ldots, x_n]$ tales que

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

y

$$\operatorname{supp}(r) \cap (\{\exp(g_1), \ldots, \exp(g_t)\} + \mathbb{N}^n) = \varnothing.$$

Como $r = f - q_1 g_1 - \cdots - q_t g_t \in I$, si $r \neq 0$ tenemos que

$$\exp(r) \in \operatorname{supp}(r) \cap (\{\exp(g_1), \ldots, \exp(g_t)\} + \mathbb{N}^n) = \varnothing,$$

lo que es contradictorio. Por tanto $r = 0$, es decir, $f = q_1 g_1 + \cdots + q_t g_t$. Con esta identidad demostramos que $I = \langle g_1, \ldots, g_t \rangle$. □

Corolario 3.10 (Teorema de la base de Hilbert)**.** *Todo ideal en el anillo de polinomios $\mathbb{F}[x_1, \ldots, x_n]$ está finitamente generado, es decir, $\mathbb{F}[x_1, \ldots, x_n]$ es un anillo Noetheriano.*

Demostración. Dado que $\{0\} = \langle 0 \rangle$, podemos suponer que $I \neq \{0\}$. El resultado es entonces consecuencia del Teorema 3.9. □

Recordemos que un anillo R es Noetheriano si satisface las siguientes condiciones equivalentes.

1. R satisface la Condición de Cadena Ascendente, es decir, dada una cadena de ideales $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_k \subseteq \cdots$, existe n tal que $I_n = I_m$ para todo $m \geq n$.

2. Todo ideal de R es finitamente generado.

Lema 3.11. *Sea $\leq$ un orden admisible en $\mathbb{N}^n$. Sea $I \leq \mathbb{F}[x_1, \ldots, x_n]$ un ideal distinto de cero. Para cualquier polinomio $f \in \mathbb{F}[x_1, \ldots, x_n]$, existe un único $r \in \mathbb{F}[x_1, \ldots, x_n]$ tal que*

(1) $\operatorname{supp}(r) \cap \exp(I) = \varnothing$,

(2) $f - r \in I$.

Demostración. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para I. Por el Teorema 3.4, $r = \operatorname{rem}(f, [G])$ satisface las propiedades del Lema, ya que $\exp(I) = \exp(G) + \mathbb{N}^n$. Tenemos, por tanto, que demostrar la unicidad. Supongamos que r, r' satisfacen las condiciones del lema. Sean $g, g' \in I$ tales que $f = g + r = g' + r'$. Entonces

$$r - r' = r - f + f - r' = -g + g' \in I.$$

Si $r \neq r'$, $\exp(r - r') \in \exp(I)$ y

$$\exp(r - r') \in \operatorname{supp}(r - r') \subseteq \operatorname{supp}(r) \cup \operatorname{supp}(r'),$$

por lo que

$$\begin{aligned} \varnothing &\neq (\operatorname{supp}(r) \cup \operatorname{supp}(r')) \cap \exp(I) \\ &= (\operatorname{supp}(r) \cap \exp(I)) \cup (\operatorname{supp}(r') \cap \exp(I)) \\ &= \varnothing \cup \varnothing, \end{aligned}$$

una contradicción. Por tanto $r = r'$ y tenemos la unicidad. □

Al elemento r que proporciona el Lema 3.11 lo denotamos $r = \mathrm{rem}(f, I)$. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para I. En la demostración hemos visto que $\mathrm{rem}(f, I) = \mathrm{rem}(f, [G])$. En particular, el resto obtenido al dividir por polinomios que constituyen una base de Gröbner es único, y podemos, en este caso, denotarlo por $\mathrm{rem}(f, G)$.

Corolario 3.12. *Sean $\leq$ un orden admisible en $\mathbb{N}^n$, $I \leq \mathbb{F}[x_1, \ldots, x_n]$ un ideal no nulo, y G una base de Gröbner para I. Entonces $f \in I$ si y solo si* $\mathrm{rem}(f, G) = 0$.

Demostración. Si $\mathrm{rem}(f, G) = 0$ es inmediato que $f \in I$. Por otra parte, si $f \in I$, 0 y $\mathrm{rem}(f, G)$ satisfacen las propiedades del Lema 3.11, por lo que son iguales por la unicidad. □

3.4 Algoritmo de Buchberger

Dados $\alpha, \beta \in \mathbb{N}^n$, definimos

$$\mathrm{lcm}(\alpha, \beta) = (\mathrm{máx}\{\alpha_1, \beta_1\}, \ldots, \mathrm{máx}\{\alpha_n, \beta_n\}).$$

Proposición 3.13. $(\alpha + \mathbb{N}^n) \cap (\beta + \mathbb{N}^n) = \mathrm{lcm}(\alpha, \beta) + \mathbb{N}^n$.

Demostración. Sea $\gamma = \mathrm{lcm}(\alpha, \beta)$. Dado que $\gamma_i = \alpha_i + \delta_i$ para cualquier $1 \leq i \leq s$, tenemos que $\gamma = \alpha + \delta$, por lo que $\gamma + \mathbb{N}^n \subseteq \alpha + \mathbb{N}^n$. Análogamente $\gamma + \mathbb{N}^n \subseteq \beta + \mathbb{N}^n$, por lo que

$$\mathrm{lcm}(\alpha, \beta) + \mathbb{N}^n \subseteq (\alpha + \mathbb{N}^n) \cap (\beta + \mathbb{N}^n).$$

Supongamos que $\lambda \in (\alpha + \mathbb{N}^n) \cap (\beta + \mathbb{N}^n)$. Existen ρ, η tales que $\lambda = \alpha + \rho = \beta + \eta$. Como consecuencia $\lambda_i \geq \alpha_i$ y $\lambda_i \geq \beta_i$ para

cualquier $1 \leq i \leq s$, es decir, $\lambda_i \geq \max\{\alpha_i, \beta_i\}$ para cada $1 \leq i \leq s$. Por tanto $\lambda \in \operatorname{lcm}(\alpha, \beta) + \mathbb{N}^n$, lo que demuestra la segunda inclusión y el resultado. □

Cuando $\gamma \in \alpha + \mathbb{N}^n$, emplearemos la notación $\gamma - \alpha$ para referirnos al elemento δ tal que $\gamma = \alpha + \delta$.

Definición 3.14. Sea $\leq$ un orden admisible en $\mathbb{N}^n$ y $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ no nulos. Sean $\alpha = \exp(f)$, $\beta = \exp(g)$ y $\gamma = \operatorname{lcm}(\alpha, \beta)$. Se define el S-polinomio de f y g como

$$S(f, g) = \operatorname{lc}(g) X^{\gamma - \alpha} f - \operatorname{lc}(f) X^{\gamma - \beta} g.$$

Lema 3.15. $\exp(S(f, g)) < \operatorname{lcm}(\exp(f), \exp(g))$.

Demostración. Sean $\alpha = \exp(f)$, $\beta = \exp(g)$ y $\gamma = \operatorname{lcm}(\alpha, \beta)$. Por las Proposición 2.13, observemos que

$$\exp(\operatorname{lc}(g) X^{\gamma - \alpha} f) = \exp(\operatorname{lc}(f) X^{\gamma - \beta} g) = \gamma$$

y

$$\operatorname{lc}\left(\operatorname{lc}(g) X^{\gamma - \alpha} f\right) = \operatorname{lc}\left(\operatorname{lc}(f) X^{\gamma - \beta} g\right) = \operatorname{lc}(f) \operatorname{lc}(g),$$

luego la Proposición 2.12 demuestra el resultado. □

Lema 3.16. *Sean* $p_1, \ldots, p_s \in \mathbb{F}[x_1, \ldots, x_n]$ *tales que* $\exp(p_i) = \delta$ *para todo* $1 \leq i \leq s$. *Si* $\exp\left(\sum_{i=1}^{s} p_i\right) < \delta$, *existen* $c_{ij} \in \mathbb{F}$ *para cada* $1 \leq i < j \leq s$ *tales que*

$$\sum_{i=1}^{s} p_i = \sum_{i<j} c_{ij} S(p_i, p_j).$$

Demostración. Sea $d_i = \mathrm{lc}(p_i)$. Dado que $\exp\left(\sum_{i=1}^{s} p_i\right) < \delta$, la Proposición 2.12 implica que $\sum_{i=1}^{s} d_i = 0$. Si $i < j$, como $\exp(p_i) = \exp(p_j) = \delta$, tenemos que

$$S(p_i, p_j) = d_j p_i - d_i p_j.$$

Se sigue que

$$\begin{aligned}\sum_{i=1}^{s-1} \frac{1}{d_s} S(p_i, p_s) &= \frac{1}{d_s} \sum_{i=1}^{s-1} (d_s p_i - d_i p_s) \\ &= \sum_{i=1}^{s-1} p_i + \frac{-d_1 - \cdots - d_{s-1}}{d_s} p_s \\ &= \sum_{i=1}^{s-1} p_i + \frac{d_s}{d_s} p_s \\ &= \sum_{i=1}^{s} p_i,\end{aligned}$$

lo que demuestra el resultado. □

Teorema 3.17 (Criterio de Buchberger)**.** *Sea $\leq$ un orden admisible en $\mathbb{N}^n$ y sea $I \leq \mathbb{F}[x_1, \ldots, x_n]$ un ideal no nulo. Sea $G = \{g_1, \ldots, g_t\}$ un conjunto de generadores de I. G es una base de Gröbner para I si y solo si para cualesquiera $1 \leq i < j \leq t$, $\mathrm{rem}(S(g_i, g_j), [G]) = 0$.*

Demostración. Si G es una base de Gröbner, dado que $S(g_i, g_j) \in \langle G \rangle = I$, tenemos que $\mathrm{rem}(S(g_i, g_j), G) = 0$ por el Corolario 3.12. Supongamos por tanto que para cada pareja $1 \leq i < j \leq t$, tenemos que $\mathrm{rem}(S(g_i, g_j), [G]) = 0$. Sea $f \in I$ no nulo. Queremos demostrar que $\exp(f) \in \exp(G) + \mathbb{N}^n$. Sea

$$\delta = \min\left\{\max\{\exp(h_1 g_1), \ldots, \exp(h_t g_t)\} \mid f = \sum_{i=1}^{t} h_i g_i\right\},$$

que existe por ser $\leq$ un buen orden. Por la Proposición 2.12, tenemos que $\exp(f) \leq \delta$. Si $\exp(f) = \delta$, existe $1 \leq i \leq t$ tal que $\exp(f) =$

$\exp(h_i g_i) = \exp(h_i) + \exp(g_i) \in \exp(G) + \mathbb{N}^n$, luego nos queda analizar el caso $\exp(f) < \delta$. Fijemos una expresión $f = \sum_{i=1}^{t} h_i g_i$ con δ mínimo. Sea $\mathbf{i} = \{i_1, \ldots, i_s\} = \{1 \leq i \leq t \mid \exp(h_i g_i) = \delta\}$. Tenemos que

$$\begin{aligned} f &= \sum_{j=1}^{s} h_{i_j} g_{i_j} + \sum_{i \notin \mathbf{i}} h_i g_i \\ &= \sum_{j=1}^{s} \mathrm{lt}(h_{i_j}) g_{i_j} + \sum_{j=1}^{s} (h_{i_j} - \mathrm{lt}(h_{i_j})) g_{i_j} + \sum_{i \notin \mathbf{i}} h_i g_i. \end{aligned}$$

Dado que

$$\exp\left(\sum_{j=1}^{s} (h_{i_j} - \mathrm{lt}(h_{i_j})) g_{i_j} + \sum_{i \notin \mathbf{i}} h_i g_i\right) < \delta,$$

tenemos que $\sum_{j=1}^{s} \mathrm{lt}(h_{i_j}) g_{i_j}$ satisface las condiciones del Lema 3.16, y por tanto

$$\sum_{j=1}^{s} \mathrm{lt}(h_{i_j}) g_{i_j} = \sum_{1 \leq j < k \leq s} c_{jk} S(\mathrm{lt}(h_{i_j}) g_{i_j}, \mathrm{lt}(h_{i_k}) g_{i_k}) \qquad (3.1)$$

para ciertos $c_{jk} \in \mathbb{F}$.

Sean $1 \leq j < k \leq s$ y sea

$$\gamma_{jk} = \mathrm{lcm}(\exp(g_{i_j}), \exp(g_{i_k})).$$

Por la Proposición 3.13, $\delta = \gamma_{jk} + \gamma$ para un cierto $\gamma \in \mathbb{N}^n$. Tenemos

que

$$\begin{aligned}
&S\left(\mathrm{lt}(h_{i_j})g_{i_j}, \mathrm{lt}(h_{i_k})g_{i_k}\right) = \\
&= \mathrm{lc}(\mathrm{lt}(h_{i_k})g_{i_k})\,\mathrm{lt}(h_{i_j})g_{i_j} - \mathrm{lc}(\mathrm{lt}(h_{i_j})g_{i_j})\,\mathrm{lt}(h_{i_k})g_{i_k} \\
&= \mathrm{lc}(h_{i_j})\,\mathrm{lc}(h_{i_k})\left(\mathrm{lc}(g_{i_k})X^{\delta-\exp(g_{i_j})}g_{i_j} - \mathrm{lc}(g_{i_j})X^{\delta-\exp(g_{i_k})}g_{i_k}\right) \\
&= \mathrm{lc}(h_{i_j})\,\mathrm{lc}(h_{i_k})X^{\gamma} \\
&\quad \cdot \left(\mathrm{lc}(g_{i_k})X^{\gamma_{jk}-\exp(g_{i_j})}g_{i_j} - \mathrm{lc}(g_{i_j})X^{\gamma_{jk}-\exp(g_{i_k})}g_{i_k}\right) \\
&= \mathrm{lc}(h_{i_j})\,\mathrm{lc}(h_{i_k})X^{\delta-\gamma_{jk}}S(g_{i_j}, g_{i_k}) \\
&= \mathrm{lc}(h_i)\,\mathrm{lc}(h_{i_k})X^{\delta-\gamma_{jk}}\textstyle\sum_{l=1}^{t} q_l g_l \\
&= \textstyle\sum_{l=1}^{t} b_l g_l,
\end{aligned} \tag{3.2}$$

donde $b_l = \mathrm{lc}(h_{i_j})\,\mathrm{lc}(h_{i_k})X^{\delta-\gamma_{jk}}q_l$ y $q_1, \ldots, q_t, 0$ son la salida del Algoritmo 1. Dado que $q_1, \ldots, q_t$ son la salida del Algoritmo 1, si $q_l g_l \neq 0$ tenemos que $\exp(q_l g_l) \leq \exp(S(g_{i_j}, g_{i_k}))$, por lo que si $b_l q_l \neq 0$,

$$\exp(b_l g_l) \leq X^{\delta-\gamma_{jk}}\exp(S(g_{i_j}, g_{i_k})) < \delta$$

por el Lema 3.15. Juntando las ecuaciones (3.1) y (3.2), tenemos que

$$\textstyle\sum_{j=1}^{s} \mathrm{lt}(h_{i_j})g_{i_j} = \sum_{l=1}^{t} f_l g_l,$$

donde $\exp(f_l g_l) < \delta$. De esta forma

$$f = \textstyle\sum_{l=1}^{t} f_l g_l + \sum_{j=1}^{s}(h_{i_j} - \mathrm{lt}(h_{i_j}))g_{i_j} + \sum_{i\notin \mathbf{i}} h_i g_i$$

es una expresión de f en la que el exponente de todos los sumandos es menor que δ, lo que contradice su minimalidad de δ. Por tanto $\exp(f) = \delta$ y $\exp(f) \in \exp(G) + \mathbb{N}^n$. □

Algorithm 2 Algoritmo de Buchberger

```
procedure GROEBNER(F)
    G ← F.
    repeat
        G' ← G
        for each pair {f, g} ⊆ G' do
            r ← rem(S(f, g), [G'])
            if r ≠ 0 then
                G ← G ∪ {r}
    until G = G'
    return G
```

Teorema 3.18. *El Algoritmo 2 calcula correctamente una base de Gröbner para* $\langle F \rangle$.

Demostración. Si el algoritmo termina la salida es una base de Gröbner para el ideal que genera por el Teorema 3.17. Sean $f, g \in G'$ y $r = \mathrm{rem}(S(f,g), [G'])$. Como

$$r = S(f,g) + \textstyle\sum_{g \in G'} h_g g \in \langle G' \rangle ,$$

tenemos que $\langle G' \rangle = \langle G' \cup \{r\} \rangle$, por lo que $\langle G \rangle = \langle G' \rangle$ al final del blucle **repeat-until**. Por tanto si el algoritmo termina su salida es una

base de Gröbner para $\langle F\rangle$. Queda ver que el algoritmo termina. Sea $r = \mathrm{rem}(S(f,g),[G'])$ con $f,g \in G'$. Como $\mathrm{supp}(r)\cap(\exp(G')+\mathbb{N}^n) = \varnothing$, tenemos que si $r \neq 0$, $\exp(r) \notin \exp(G') + \mathbb{N}^n$, luego

$$\exp(G') + \mathbb{N}^n \subset \exp(G) + \mathbb{N}^n.$$

Esto nos da una cadena ascendente

$$\exp(G_0) + \mathbb{N}^n \subset \exp(G_1) + \mathbb{N}^n \subset \cdots \subset \exp(G_i) + \mathbb{N}^n \subset \cdots,$$

donde G_i son las sucesivas salidas del bucle **repeat-until**, que por el Lema de Dickson (Teorema 3.2) debe estabilizar. Por tanto el algoritmo termina. □

Ejemplo 3.19. Sea $I = \langle f_1, f_2\rangle$ donde f_1, f_2 son los dados en el Ejemplo 3.5. Calculemos una base de Gröbner para I.

Sea M un ideal en $\mathbb{N}^n$. Decimos que A es un conjunto generador minimal de M si $M = A + \mathbb{N}^n$ pero $M \neq (A \setminus \{\alpha\}) + \mathbb{N}^n$ para cualquier $\alpha \in A$.

Lema 3.20. *Sea $A \subseteq \mathbb{N}^n$ y $\alpha \in A$. Si $\alpha \in (A \setminus \{\alpha\}) + \mathbb{N}^n$, entonces $A + \mathbb{N}^n = (A \setminus \{\alpha\}) + \mathbb{N}^n$.*

Demostración. Como $A \subseteq (A \setminus \{\alpha\}) + \mathbb{N}^n$, tenemos que $A + \mathbb{N}^n \subseteq (A \setminus \{\alpha\}) + \mathbb{N}^n$. La inclusión contraria es inmediata. □

Lema 3.21. *Todo ideal $M \subseteq \mathbb{N}^n$ tiene un único conjunto generador minimal.*

Demostración. Supongamos que tenemos dos conjuntos generadores minimales $A = \{\alpha(1),\ldots,\alpha(s)\}$ y $B = \{\beta(1),\ldots,\beta(t)\}$, finitos por

el Lema de Dickson (Teorema 2.6). Como $\alpha(1) \in M$, existen $\beta(i), \gamma$ tales que $\alpha(1) = \beta(i_1) + \gamma$. Como $\beta(i_1) \in M$, $\beta(i_1) = \alpha(j) + \gamma'$, por lo que $\alpha(1) = \alpha(j) + \gamma + \gamma'$. Como A es minimal, el Lema 3.20 implica que $\alpha(j) = \alpha(1)$, por lo que $\alpha(1) = \beta_{i_1}$. Supongamos que $\alpha(l) = \beta_{i_l}$ para $1 \leq l \leq k-1$. El mismo argumento anterior implica que $\alpha(k) = \beta_{i_k}$ para cierto i_k. Reiterando la construcción, $A \subseteq B$. Por simetría, $B \subseteq A$, de donde tenemos la igualdad. □

El Lema 3.21 nos dice que existe un conjunto generador minimal y el Lema 3.20 nos dice como calcularlo. Una base de Gröbner G de I se dice minimal si $\exp(G)$ es un conjunto generador minimal de $\exp(I)$. Si bien los conjuntos generadores minimales son únicos, las bases de Gröbner minimales no lo son.

Ejemplo 3.22. $\{y^2 - 1, x - y\}$ y $\{y^2 - x + y - 1, x - y\}$ son ambas bases de Gröbner minimales para $I = \langle f_1, f_2 \rangle$ con respecto al orden DEGREVLEX, donde f_1, f_2 son los dados en el Ejemplo 3.5

Definición 3.23. Una base de Gröbner reducida para un ideal I es una base de Gröbner G tal que

(1) para todo $g \in G$, $\mathrm{lc}(g) = 1$,

(2) para todo $g \in G$, $\mathrm{supp}(g) \cap (\exp(G \setminus \{g\}) + \mathbb{N}^n) = \varnothing$.

Teorema 3.24. *Todo ideal tiene una única base de Gröbner reducida para un orden admisible dado.*

Demostración. Dado un ideal I, sea $G \subseteq I$ tal que $\exp(G)$ es un conjunto generador minimal de $\exp(I)$. Sea $g \in G$ y sea $r = \mathrm{rem}(g, [G \setminus \{g\}])$. Como $\exp(g) \notin \exp(G \setminus \{g\}) + \mathbb{N}^n$, podemos observar del Algoritmo

1 que $\exp(g) = \exp(r)$, y dado que $g - r \in \langle G \setminus \{g\}\rangle \subseteq I$, tenemos que $r \in I$. Como $\exp(G) = \exp((G \setminus \{g\}) \cup \{r\})$, concluimos que $G' = (G \setminus \{g\}) \cup \{r\}$ es una nueva base de Gröbner en la que $\operatorname{supp}(r) \cap (\exp(G' \setminus \{r\}) + \mathbb{N}^n) = \varnothing$. Reiterando el proceso en cada elemento de G, y dividiendo cada elemento de g por su coeficiente líder, obtenemos una base de Gröbner reducida para I.
Queda demostrar la unicidad. Sean G_1, G_2 dos bases de Gröbner reducidas. Como $\exp(G_1) = \exp(G_2)$ por el Lema 3.21, dado $g_1 \in G_1$ existe un único $g_2 \in G_2$ tal que $\exp(g_1) = \exp(g_2)$. Como $g_1 - g_2 \in I$, $\operatorname{rem}(g_1 - g_2, G_1) = 0$ por el Corolario 3.12. Observemos que

$$\operatorname{supp}(g_1 - g_2) \subseteq (\operatorname{supp}(g_1) \cup \operatorname{supp}(g_2)) \setminus \{\exp(g_1)\}$$

y que para $i \in \{1, 2\}$,

$$\operatorname{supp}(g_i) \setminus \{\exp(g_i)\} \cap (\exp(G_i) + \mathbb{N}^n) = \varnothing,$$

por lo que

$$\operatorname{supp}(g_1 - g_2) \cap (\exp(G_1) + \mathbb{N}^n) = \varnothing,$$

y por el Lema 3.11, $\operatorname{rem}(g_1 - g_2, G_1) = g_1 - g_2$. En consecuencia $g_1 = g_2$, de lo que deducimos que $G_1 = G_2$. □

Corolario 3.25. *Dos ideales en un anillo de polinomios son iguales si y solo si sus bases de Gröbner reducidas son iguales.*

3.5 Aplicación: Sistema de Posicionamiento Global (GPS)

El sistema de posicionamiento global conocido como GPS consta de los siguientes elementos.

- 24 satélites (y 6 de refuerzo) en órbita estable, conocida y transmitida.
- Todos *perfectamente* sincronizados con relojes atómicos.
- Cada uno de ellos emite una señal pseudoaleatoria única junto con información referente a su posición.
- El receptor GPS mide el momento en que recibe las señales de los satélites.
- Como el receptor sabe en qué instante se ha enviado la señal, el retardo en el tiempo que tarda la señal en llegar multiplicado por la velocidad de la luz nos da la distancia *exacta* a la que están los satélites.

Si (x_i, y_i, z_i) es la posición del satélite, t_i el tiempo que tarda en llegar la señal y (x, y, z) la posición del receptor, entonces

$$(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 - (ct_i)^2 = 0$$

donde c es la velocidad de la luz. Si tomamos (x, y, z) como variable tenemos la ecuación de una esfera centrada en (x_i, y_i, z_i) y de radio ct_i.
Si disponemos de los datos de tres satélites, la posición viene determinada por los puntos de la variedad

$$\mathbf{V}\left(\left\langle (x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 - (ct_i)^2 \mid 1 \leq i \leq 3 \right\rangle\right).$$

Una base de Gröbner del ideal está compuesta de un polinomio cuadrático en z junto con dos polinomios lineales en x, y e y, z, por lo que es

sencillo calcular los dos puntos de la variedad. Uno de ellos nos dice la posición.
La sincronización de los relojes (atómicos) de los satélites es extrema, pero el receptor no dispone de un reloj atómico y por tanto su sincronización no es perfecta. Eso quiere decir que hay un retraso o adelanto d del reloj del receptor con respecto de los relojes de los satélites. Si t_i es el tiempo medido por el receptor, la ecuación se convierte en

$$(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 = (c(t_i + d))^2$$

Con al menos cuatro satélites podemos considerar d como variable, por tanto tenemos averiguar la variedad asociada al ideal

$$\left\langle (x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 - (c(t_i + d))^2 \mid 1 \leq i \leq 4 \right\rangle$$

Una base de Gröbner consiste en un polinomio cuadrático en d junto con tres polinomios lineales en x, d, y, d y z, d, por lo que tenemos dos posiciones posibles, una de ellas correctas. Una vez calculado el valor correcto de d, podemos sincronizar el reloj del receptor con los satélites. A partir de ese momento podemos trabajar con ideales de la forma

$$\left\langle (x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 - (ct_i)^2 \mid 1 \leq i \leq 3 \right\rangle$$

como en el primer caso.

Ejercicios sobre Bases de Gröbner y Algoritmos Básicos

Ejercicio 3.1. Demuestra que un anillo satisface la condición de cadena ascendente si y sólo si todo ideal del mismo es finitamente generado.

Ejercicio 3.2. Dados $f = x^7y^2 + x^3y^2 - y + 1$, $f_1 = xy^2 - x$ y $f_2 = x - y^3$ en $\mathbb{Q}[x, y, z]$, calcula la división de f entre $[f_1, f_2]$ con respecto al orden DEGLEX. Realiza más divisiones cambiando la ordenación de los divisores y el orden admisible. Realiza el ejercicio cambiando $\mathbb{Q}$ por $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$ y $\mathbb{F}_5$.

Ejercicio 3.3. Dados $f = xy^2z^2 + xy - yz$, $f_1 = x - y^2$, $f_2 = y - z^3$ y $f_3 = z^2 - 1$ en $\mathbb{Q}[x, y, z]$, calcula la división de f entre $[f_1, f_2, f_3]$ con respecto al orden DEGLEX. Realiza más divisiones cambiando la ordenación de los divisores y el orden admisible.

Ejercicio 3.4. Sean $f = x^3 - x^2y - x^2z + x$, $f_1 = x^2y - z$ y $f_2 = xy - 1$ en $\mathbb{Q}[x, y, z]$, en el que consideramos el orden DEGREVLEX.

(1) Calcula $r_1 = \text{rem}(f, [f_1, f_2])$ y $r_2 = \text{rem}(f, [f_2, f_1])$.

(2) Sea $r = r_1 - r_2$, ¿$r \in \langle f_1, f_2 \rangle$? Si la respuesta es afirmativa escribe $r = p_1f_1 + p_2f_2$.

(3) Calcula $\text{rem}(r, [f_1, f_2])$.

Ejercicio 3.5. Dados $f_1 = x^4y^4 - z$, $f_2 = x^3y^3 - 1$ y $f_3 = x^2y^4 - 2x$ en $\mathbb{Q}[x, y, z]$ con el orden DEGLEX, encuentra, si es posible, $g \in \langle f_1, f_2, f_3 \rangle$ tal que $\text{rem}(g, [f_1, f_2, f_3]) \neq 0$.

Ejercicio 3.6. Demuestra que el cálculo del resto en el Algoritmo 1 es lineal.

Ejercicio 3.7. Si G es una base de Gröbner para I y $G \subseteq G' \subseteq I$, demuestra que G' es también una base de Gröbner para I.

Ejercicio 3.8. Calcula una base de Gröbner para el ideal

$$\langle x^4y^2 - z, x^3y^3 - 1, x^2y^4 - 2z\rangle \subseteq \mathbb{Q}[x, y, z]$$

con respecto al orden DEGLEX. Realiza el ejercicio cambiando $\mathbb{Q}$ por $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$ y $\mathbb{F}_5$.

Ejercicio 3.9. Si $f \in \mathbb{F}[x_1, \ldots, x_n]$ y $f \notin \langle x_1, \ldots, x_n\rangle$, demuestra que $\langle x_1, \ldots, x_n, f\rangle = \mathbb{F}[x_1, \ldots, x_n]$.

Ejercicio 3.10. Demuestra que las variedades afines satisfacen la condición de cadena descendente, es decir, si tenemos una cadena

$$V_1 \supseteq V_2 \supseteq \cdots \supseteq V_i \supseteq \cdots,$$

demuestra que existe $n \in \mathbb{N}$ tal que $V_n = V_{n+k}$ para todo $k \in \mathbb{N}$.

Ejercicio 3.11. Sea $V = \mathbf{V}(x^2 - y, y + x^2 - 4) \subseteq \mathbb{C}^2$. Calcula los puntos de la variedad.

Ejercicio 3.12. Sea $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ un ideal y sea $G = \{g_1, \ldots, g_t\}$ una base de I, es decir, $I = \langle G\rangle$. Demuestra que G es una base de Gröbner para I si y solo si para cualquier $f \in \mathbb{F}[x_1, \ldots, x_n]$,

$$f \in I \iff \operatorname{rem}(f, [G]) = 0.$$

Ejercicio 3.13. Calcula $S(f, g)$ es los siguientes casos,

(1) $f = 4x^2z - 7y^2$, $g = xyz^2 + 3xz^4$

(2) $f = x^4y - z^2$, $g = 3xz^2 - y$

(3) $f = x^7y^2z + 2ixyz$, $g = 2x^7y^2z + 4$

Ejercicio 3.14. ¿Depende $S(f, g)$ del orden admisible empleado?

Ejercicio 3.15. Sea G una base de Gröbner para I. Demuestra que $\text{rem}(f, G) = \text{rem}(g, G)$ si y solo si $f - g \in I$. Demuestra además que

$$\text{rem}(f + g, G) = \text{rem}(f, G) + \text{rem}(g, G)$$

y que

$$\text{rem}(fg, G) = \text{rem}(\text{rem}(f, G)\,\text{rem}(g, G), G).$$

Ejercicio 3.16. Calcula una base de Gröbner para los siguientes ideales.

(1) $I = \langle x^2y - 1, xy^2 - x\rangle$

(2) $I = \langle x^2 + y, x^4 + 2x^2y + y^2 + 3\rangle$

(3) $I = \langle x - z^4, y - z^5\rangle$

Calcula también la base de Gröbner reducida con respecto al orden LEX.

Ejercicio 3.17. Sea

$$I = \langle 3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w\rangle \subseteq \mathbb{Q}[x, y, z, t]$$

Calcula una base de Gröbner reducida para I.

Ejercicio 3.18. Sea $A = (a_{ij}) \in \mathbb{F}^{m\times n}$ y sea $f_i = \sum_{j=1}^{n} a_{ij}x_j$. Consideremos en $\mathbb{N}^n$ el orden LEX. Sea $I = \langle f_1, \ldots, f_m\rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$. Sean $g_1, \ldots, g_t$ los polinomios asociados a las filas no nulas de la forma escalonada reducida de A.

(1) Comprueba que $I = \langle g_1, \ldots, g_t\rangle$.

(2) Calcula $\operatorname{rem}(S(g_i, g_l), [g_1, \ldots, g_t])$. Consejo: obsérvese que solo se emplean g_i y g_l en la división.

(3) Concluye que $\{g_1, \ldots, g_t\}$ es una base de Gröbner reducida para I.

Capítulo 4

Eliminación e implicitación

4.1 Órdenes de eliminación

Dado $0 \leq l \leq n$, denotamos por $\mathbb{N}^n_l = \{\alpha \in \mathbb{N}^n \mid \alpha_i = 0, 1 \leq i \leq l\}$. Es inmediato que $\mathbb{N}^n_l \cong \mathbb{N}^{n-l}$.

Lema 4.1. *Sea* M *un ideal en* $\mathbb{N}^n$ *generado por* A. *Entonces* $M \cap \mathbb{N}^n_l$ *es un ideal en* $\mathbb{N}^{n-l}$ *generado por* $A \cap \mathbb{N}^n_l$.

Demostración. Es inmediato comprobar que $M \cap \mathbb{N}^n_l$ es un ideal en $\mathbb{N}^{n-l}$ via la identificación canónica $\mathbb{N}^n_l \cong \mathbb{N}^{n-l}$. Por otra parte, sea $\gamma \in M \cap \mathbb{N}^n_l$ y sea $\alpha \in A$ tal que $\gamma = \alpha + \beta$. Sea $1 \leq i \leq l$. Como $\alpha_i + \beta_i = \gamma_i = 0$, tenemos que $\alpha_i = \beta_i = 0$, por lo que $\alpha \in A \cap \mathbb{N}^n_l$ y $\beta \in \mathbb{N}^n_l$. Esto demuestra que $M \cap \mathbb{N}^n_l$ está generado por $A \cap \mathbb{N}^n_l$. □

Definición 4.2. Sea $\leq$ un orden admisible en $\mathbb{N}^n$. Decimos que $\leq$ es un orden de l-eliminación si para cualesquiera $\alpha, \beta \in \mathbb{N}^n$, si $\alpha \in \mathbb{N}^n_l$ y $\beta \leq \alpha$, entonces $\beta \in \mathbb{N}^n_l$.

Ejemplo 4.3. El orden LEX es un orden de l-eliminación para cualquier $0 \leq l \leq n$.

Ejemplo 4.4. Supongamos que disponemos de dos ordenes admisibles $\leq_1$ en $\mathbb{N}^l$ y $\leq_2$ en $\mathbb{N}^{n-l}$. Dado un elemento $\alpha \in \mathbb{N}^n$, podemos escribirlo como $\alpha = (\alpha_l, \alpha_{n-l}$ con $\alpha_l \in \mathbb{N}^l$ y $\alpha_{n-l} \in \mathbb{N}^{n-l}$. Observemos que $\alpha \in \mathbb{N}_l^n$ si y solo si $\alpha_l = 0$. Definimos $\leq$ en $\mathbb{N}^n$ mediante

$$\alpha \leq \beta \iff \begin{cases} \alpha_l <_1 \beta_l & \text{o} \\ \alpha_l = \beta_l \text{ y } \alpha_{n-l} \leq_2 \beta_{n-l} \end{cases}.$$

Dejo como ejercicio comprobar que $\leq$ es un orden de l-eliminación.

4.2 Eliminación de variables

Teorema 4.5. *Sea* $I \leq \mathbb{F}[x_1, \ldots, x_n]$ *un ideal no nulo y sea* $\leq$ *un orden de* l*-eliminación. Si* G *es una base de Gröbner para* I*, entonces* $G \cap \mathbb{F}[x_{l+1}, \ldots, x_n]$ *es una base de Gröbner para* $I \cap \mathbb{F}[x_{l+1}, \ldots, x_n]$.

Demostración. Observemos que si $f \in \mathbb{F}[x_1, \ldots, x_n]$ y $\exp(f) \in \mathbb{N}_l^n$, al ser el orden de eliminación, $\operatorname{supp}(f) \subseteq \mathbb{N}_l^n$, por lo que concluimos que $f \in \mathbb{F}[x_{l+1}, \ldots, x_n]$, es decir, $f \in \mathbb{F}[x_{l+1}, \ldots, x_n]$ si solo si $\exp(f) \in \mathbb{N}_l^n$. En consecuencia

$$\exp(F) \cap \mathbb{N}_l^n = \exp\left(F \cap \mathbb{F}[x_{l+1}, \ldots, x_n]\right)$$

para cualquier subconjunto no vacío $F \subseteq \mathbb{F}[x_1, \ldots, x_n]$.
Sea G una base de Gröbner para I. Por el Lema 4.1, $\exp(G) \cap \mathbb{N}_l^n$ genera $\exp(I) \cap \mathbb{N}_l^n$, y dado que

$$\exp(I) \cap \mathbb{N}_l^n = \exp\left(I \cap \mathbb{F}[x_{l+1}, \ldots, x_n]\right)$$

y

$$\exp(G) \cap \mathbb{N}_l^n = \exp\left(G \cap \mathbb{F}[x_{l+1}, \ldots, x_n]\right),$$

$\exp\left(G \cap \mathbb{F}[x_{l+1}, \ldots, x_n]\right)$ genera $\exp\left(I \cap \mathbb{F}[x_{l+1}, \ldots, x_n]\right)$, es decir $G \cap \mathbb{F}[x_{l+1}, \ldots, x_n]$ es una base de Gröbner para $I \cap \mathbb{F}[x_{l+1}, \ldots, x_n]$. □

Como consecuencia del Teorema 4.5 disponemos de un algoritmo para calcular el ideal de eliminación de un ideal I dado mediante un conjunto de generadores F. El proceso es el siguiente:

(I) Fijamos el orden LEX en $\mathbb{N}^n$. Cualquier otro orden de l-eliminación jugaría el mismo efecto.

(II) Calculamos, mediante el algoritmo de Buchberger, una base de Gröbner (reducida) G para I a partir de F.

(III) Calculamos $G \cap \mathbb{F}[x_{l+1}, \ldots, x_n]$.

Ejemplo 4.6. Sea

$$I = \left\langle -x^2y - y^3 - x^2 + xy + y, x^2y - y^3 - xy - y^2 + y \right\rangle \subseteq \mathbb{F}_3[x, y].$$

Si calculamos la base de Gröbner reducida para I obtenemos

$$\left\{x^2 - y^3 + y^2 + y, xy - y^4 - y^3 - y^2 - y, y^7 - y^6 + y^3 + y\right\},$$

por lo que $I \cap \mathbb{F}_3[y] = \langle y^7 - y^6 + y^3 + y \rangle$.

En adelante presentaremos más aplicaciones de la eliminación, pero vamos en un primer momento a dar una de las más sencillas y directas. Sean $I_1 = \langle F_1 \rangle$ y $I_2 = \langle F_2 \rangle$. Recordemos que

$$I_1 + I_2 = \langle F_1 \cup F_2 \rangle$$

y

$$I_1 I_2 = \langle f_1 f_2 \mid f_1 \in F_1, f_2 \in F_2 \rangle,$$

pero no hemos podido dar un método para calcular $I_1 \cap I_2$.

Lema 4.7. *Sea A un anillo y sea $a \in A$. La aplicación*

$$\begin{aligned} \phi_a : A[x] &\to A \\ \textstyle\sum_i a_i x^i &\mapsto \textstyle\sum_i a_i a^i \end{aligned}$$

es un morfismo de anillos tal que $\phi_a(b) = b$ para todo $b \in A$.

Demostración. Ejercicio. □

Teorema 4.8. *Sean $I = \langle F \rangle, J = \langle G \rangle \leq \mathbb{F}[x_1, \ldots, x_n]$ y sea $H = \langle tF, (1-t)G \rangle \leq \mathbb{F}[t, x_1, \ldots, x_n]$. Entonces $I \cap J = H \cap \mathbb{F}[x_1, \ldots, x_n]$.*

Demostración. Sea $F = \{f_1, \ldots, f_s\}$ y $G = \{g_1, \ldots, g_t\}$. Si $f \in I \cap J$,

$$f = tf + (1-t)f = \textstyle\sum_i f h_i f_i + \sum_j (1-t) m_j g_j \in H,$$

por lo que tenemos que $f \in H \cap \mathbb{F}[x_1, \ldots, x_n]$, es decir, tenemos la primera inclusión $I \cap J \subseteq H \cap \mathbb{F}[x_1, \ldots, x_n]$.
Supongamos por el contrario que $f \in H \cap \mathbb{F}[x_1, \ldots, x_n]$. Necesariamente

$$f = \textstyle\sum_i p_i t f_i + \sum_j q_j (1-t) g_j$$

donde $p_i, q_j \in \mathbb{F}[t, x_1, \ldots, x_n]$. Sea

$$\phi_0 : \mathbb{F}[t, x_1, \ldots, x_n] \to \mathbb{F}[x_1, \ldots, x_n]$$

el morfismo de anillos que evalúa la t en 0 descrito en el Lema 4.7 donde $A = \mathbb{F}[x_1, \ldots, x_n]$. Por una parte, $\phi_0(f) = f$ porque $f \in \mathbb{F}[x_1, \ldots, x_n]$. Por otra parte,

$$\phi_0(f) = \phi_0\left(\sum_i p_i t f_i + \sum_j q_j(1-t)g_j\right) = \sum_j \phi_0(q_j)g_j$$

porque ϕ_0 es morfismo de anillos y $g_1, \ldots, g_t \in \mathbb{F}[x_1, \ldots, x_n]$, luego $f \in J$. Evaluando en $t = 1$ obtenemos análogamente que $f \in I$, por lo que $f \in I \cap J$ y $H \cap \mathbb{F}[x_1, \ldots, x_n] \subseteq I \cap J$. □

El Teorema 4.8 permite diseñar un algoritmo para calcular un conjunto de generadores de $I \cap J$ a partir de conjuntos de generadores $F = \{f_1, \ldots, f_s\}$ y $G = \{g_1, \ldots, g_s\}$ de I y J respectivamente.

(I) En $\mathbb{F}[t, x_1, \ldots, x_n]$ consideramos el orden LEX (o cualquier otro de 1-eliminación).

(II) Calculamos una base de Gröbner G_H para el ideal

$$H = \langle tf_1, \ldots, tf_s, (1-t)g_1, \ldots, (1-t)g_t\rangle.$$

(III) Un conjunto de generadores de $I \cap J$ es $G_H \cap \mathbb{F}[x_1, \ldots, x_n]$.

Ejemplo 4.9. En $\mathbb{F}_3[x, y]$ consideramos los ideales

$$I = \langle -x^3 - xy^2, -xy^2 - y^3 + x^2\rangle$$

y

$$J = \langle y^2 - x + y + 1, x^2 + xy + y^2 + x, xy - y^2 - y\rangle$$

Una base de Gröbner para

$$\begin{aligned} H = \langle & t(-x^3 - xy^2), \\ & t(-xy^2 - y^3 + x^2), \\ & (1-t)(y^2 - x + y + 1), \\ & (1-t)(x^2 + xy + y^2 + x), \\ & (1-t)(xy - y^2 - y)\rangle \end{aligned}$$

es

$$\{t - 1, x^2 - y^5 - y^3, xy^2 - y^5, y^7 + y^6 - y^5\},$$

por lo que

$$I \cap J = \langle x^2 - y^5 - y^3, xy^2 - y^5, y^7 + y^6 - y^5\rangle.$$

4.3 Implicitación (cuerpo infinito)

Lema 4.10. *Sea* $I \leq \mathbb{F}[x_1, \ldots, x_n]$ *un ideal no nulo, y sea* $I_l = I \cap \mathbb{F}[x_{l+1}, \ldots, x_n]$. *Sea* $\pi_l : \mathbb{F}^n \to \mathbb{F}^{n-l}$ *la proyección canónica en las últimas* $n - l$ *posiciones. Entonces*

$$\pi_l(\mathbf{V}(I)) \subseteq \mathbf{V}(I_l).$$

Demostración. Sea $(a_1, \ldots, a_n) \in \mathbf{V}(I)$. Dado un polinomio $f \in I_l = I \cap \mathbb{F}[x_{l+1}, \ldots, x_n]$, como $f \in \mathbb{F}[x_{l+1}, \ldots, x_n]$,

$$f(a_1, \ldots, a_n) = f(a_{l+1}, \ldots, a_n) = f(\pi_l(a_1, \ldots, a_n)).$$

Por otra parte, como $f \in I$,

$$f(a_1, \ldots, a_n) = 0.$$

Por tanto $\pi_L(a_1, \ldots, a_n) \in \mathbf{V}(I_l)$. □

El problema de la implicitación consiste en encontrar la variedad algebraica asociada a ecuaciones paramétricas. Concretamente, sean

$$f_1, \ldots, f_n, q_1, \ldots, q_n \in \mathbb{F}[t_1, \ldots, t_r]$$

y sea $W = \mathbf{V}(q_1 \cdots q_n)$. Las evaluaciones de los polinomios permiten definir una aplicación

$$\begin{aligned} \phi : \mathbb{F}^r \setminus W &\to \mathbb{F}^n \\ (a_1, \ldots, a_r) &\mapsto \left(\tfrac{f_1(a_1,\ldots,a_r)}{q_1(a_1,\ldots,a_r)}, \ldots, \tfrac{f_n(a_1,\ldots,a_r)}{q_n(a_1,\ldots,a_r)} \right) \end{aligned}$$

El problema que nos vamos a plantear es calcular la menor variedad que contiene a $\mathrm{im}(\phi)$.
En primer lugar supondremos que la parametrización es polinomial, es decir, $q_1 = \cdots = q_n = 1$.

Teorema 4.11 (Implicitación polinomial)**.** *Sea $\mathbb{F}$ un cuerpo infinito. Sean $f_1, \ldots, f_n \in \mathbb{F}[t_1, \ldots, t_r]$ y sea*

$$\begin{aligned} \phi : \mathbb{F}^r &\to \mathbb{F}^n \\ (a_1, \ldots, a_r) &\mapsto (f_1(a_1, \ldots, a_r), \ldots, f_n(a_1, \ldots, a_r)) . \end{aligned}$$

Sea $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle \subseteq \mathbb{F}[t_1, \ldots, t_r, x_1, \ldots, x_n]$ y sea $J = I \cap \mathbb{F}[x_1, \ldots, x_n]$ el ideal de r-eliminación. Entonces $\mathbf{V}(J)$ es la menor variedad que contiene a $\phi(\mathbb{F}^r)$.

Demostración. Vamos a demostrar que $\mathbf{I}(\phi(\mathbb{F}^r)) = J$, lo que en virtud de la Proposición 2.26 demuestra el teorema. Sea

$$V = \mathbf{V}(x_1 - f_1, \ldots, x_n - f_n) \subseteq \mathbb{F}^{r+n}.$$

Es inmediato comprobar que

$$(a_1, \ldots, a_r, b_1, \ldots, b_n) \in V \iff b_i = f_i(a_1, \ldots, a_r), 1 \leq i \leq n,$$

por lo que $\phi(\mathbb{F}^r) = \pi_r(V)$. Por el Lema 4.10, $\phi(\mathbb{F}^r) = \pi_r(V) \subseteq \mathbf{V}(J)$, lo que implica que $\mathbf{I}(\phi(\mathbb{F}^r)) \supseteq \mathbf{I}(\mathbf{V}(J)) \supseteq J$. Para ver la inclusión contraria, sea $h \in \mathbf{I}(\phi(\mathbb{F}^r)) \subseteq \mathbb{F}[x_1, \ldots, x_n]$. Reordenando las variables como $\mathbb{F}[x_1, \ldots, x_n, t_1, \ldots, t_r]$ consideramos el orden LEX en $\mathbb{N}^{n+r}$ y dividimos $h = h(x_1, \ldots, x_n)$ entre la lista $[x_1 - f_1, \ldots, x_n - f_n]$, para obtener

$$h = q_1(x_1 - f_1) + \cdots + q_n(x_n - f_n) + \rho(t_1, \ldots, t_r)$$

dado que $\mathrm{lt}(x_i - f_i) = x_i$ para todo $1 \leq i \leq n$. Dado $(a_1, \ldots, a_r) \in \mathbb{F}^r$, evaluamos la ecuación anterior en $(b_1, \ldots, b_n, a_1, \ldots a_r)$ con $b_i = f_i(a_1, \ldots, a_r)$, tenemos que

$$0 = h(f_1(a_1, \ldots, a_r), \ldots, f_n(a_1, \ldots, a_r))$$

porque $h \in \mathbf{I}(\phi(\mathbb{F}^r))$ y

$$h(f_1(a_1, \ldots, a_r), \ldots, f_n(a_1, \ldots, a_r)) = \rho(a_1, \ldots, a_r)$$

ya que $b_i - f_i(a_1, \ldots, a_r) = 0$. Por la Proposición 2.15, $\rho = 0$, por lo que

$$h \in \langle x_1 - f_1, \ldots, x_n - f_n \rangle = I.$$

Dado que $h \in \mathbb{F}[x_1, \ldots, x_n]$, concluimos que $h \in J = I \cap \mathbb{F}[x_1, \ldots, x_n]$, lo que termina la demostración. □

En el caso de parametrización polinomial, hemos reducido el problema de la implicitación a un problema de eliminación, lo que podemos resolver mediante el uso de bases de Gröbner.

Ejemplo 4.12. En $\mathbb{Q}[u, v]$ consideramos los polinomios

$$f_x = u^2 - v^2, f_y = u^2 + v^2 + v, f_z = -uv + u + v$$

que nos definen una parametrización polinomial

$$\phi : \mathbb{Q}^2 \to \mathbb{Q}^3.$$

Una base de Gröbner del ideal

$$I = \langle x - u^2 + v^2, y - u^2 - v^2 - v, z + uv - u - v \rangle \subseteq \mathbb{Q}[u, v, x, y, z]$$

con respecto al orden LEX es

$$\begin{aligned}
&\{u^2+\tfrac{1}{2}v-\tfrac{1}{2}x-\tfrac{1}{2}y,\\
&\ uv-u-v+z,\\
&\ ux-uy+3u-2vz+2v-x+y-3z,\\
&\ uz-u-\tfrac{1}{4}vy+vz-\tfrac{9}{16}v\\
&\quad -\tfrac{1}{8}x^2-\tfrac{1}{16}x+\tfrac{1}{8}y^2-\tfrac{7}{16}y-\tfrac{1}{2}z^2+z, v^2+\tfrac{1}{2}v+\tfrac{1}{2}x-\tfrac{1}{2}y,\\
&\ vx+\tfrac{3}{2}vy-2vz+\tfrac{5}{8}v+\tfrac{1}{4}x^2-\tfrac{3}{8}x-\tfrac{1}{4}y^2-\tfrac{5}{8}y+z^2,\\
&\ vy^2-\tfrac{24}{5}vyz+\tfrac{13}{10}vy+\tfrac{32}{5}vz^2-\tfrac{22}{5}vz+\tfrac{17}{16}v-\tfrac{1}{5}x^3+\tfrac{3}{10}x^2y\\
&\quad -\tfrac{2}{5}x^2z-\tfrac{19}{40}x^2+\tfrac{1}{5}xy^2-\tfrac{3}{4}xy-\tfrac{4}{5}xz^2+\tfrac{19}{5}xz-\tfrac{179}{80}x-\tfrac{3}{10}y^3\\
&\quad +\tfrac{2}{5}y^2z+\tfrac{33}{40}y^2+\tfrac{6}{5}yz^2-\tfrac{11}{5}yz-\tfrac{17}{16}y-\tfrac{8}{5}z^3+\tfrac{33}{10}z^2,\\
&\ x^4+3x^3-2x^2y^2+8x^2y+8x^2z^2-28x^2z+14x^2-xy^2\\
&\quad -16xyz+22xy+12xz^2-26xz+5x+y^4-10y^3-8y^2z^2\\
&\quad +44y^2z-64yz^2+10yz+16z^4+16z^3-5z^2\},
\end{aligned}$$

por lo que la menor variedad que contiene a $\mathrm{im}(\phi)$ es

$$\begin{aligned}
\mathbf{V}\big(&x^4+3x^3-2x^2y^2+8x^2y+8x^2z^2-28x^2z+14x^2-xy^2\\
&-16xyz+22xy+12xz^2-26xz+5x+y^4-10y^3-8y^2z^2\\
&+44y^2z-64yz^2+10yz+16z^4+16z^3-5z^2\big)
\end{aligned}$$

Teorema 4.13 (Implicitación racional)**.** *Sea $\mathbb{F}$ un cuerpo infinito. Sean $f_1,\dots,f_n,q_1,\dots,q_n\in\mathbb{F}[t_1,\dots,t_r]$ y sea*

$$\begin{aligned}
\phi : \mathbb{F}^r \setminus W &\to \mathbb{F}^n\\
(a_1,\dots,a_r) &\mapsto \left(\tfrac{f_1(a_1,\dots,a_r)}{q_1(a_1,\dots,a_r)},\dots,\tfrac{f_n(a_1,\dots,a_r)}{q_n(a_1,\dots,a_r)}\right)
\end{aligned}$$

Sea $I = \langle q_1x_1 - f_1, \ldots, q_nx_n - f_n, 1 - q_1 \cdots q_n y \rangle$ *un ideal en el anillo de polinomios* $\mathbb{F}[y, t_1, \ldots, t_r, x_1, \ldots, x_n]$. *Denotemos por* $J = I \cap \mathbb{F}[x_1, \ldots, x_n]$ *al ideal de* $1 + r$*-eliminación. Entonces* $\mathbf{V}(J)$ *es la menor variedad que contiene a* $\phi(\mathbb{F}^r \setminus \mathbf{V}(q_1 \cdots q_n))$.

Demostración. Como en el caso polinomial vamos a demostrar que $\mathbf{I}(\phi(\mathbb{F}^r \setminus \mathbf{V}(q_1 \cdots q_n))) = J$, lo que en virtud de la Proposición 2.26 demuestra el teorema.
Sea

$$V = \mathbf{V}\left(q_1x_1 - f_1, \ldots, q_nx_n - f_n, 1 - q_1 \cdots q_n y\right) \subseteq \mathbb{F}^{1+r+n}$$

Sea $(a_0, a_1, \ldots, a_r, b_1, \ldots, b_n) \in V$. Dado que

$$a_0 q_1(a_1, \ldots, a_r) \cdots q_n(a_1, \ldots, a_r) - 1 = 0,$$

tenemos que $(a_1, \ldots, a_r) \notin \mathbf{V}(q_1 \cdots q_n)$ y

$$b_i = \tfrac{f_i(a_1, \ldots, a_r)}{q_i(a_1, \ldots, a_r)},\ 1 \leq i \leq n,$$

por lo que $\phi(\mathbb{F}^r \setminus \mathbf{V}(q_1 \cdots q_n)) = \pi_{1+r}(V)$. Como consecuencia del Lema 4.10, $\pi_{1+r}(V) \subseteq \mathbf{V}(J)$, lo que implica que

$$\mathbf{I}(\phi(\mathbb{F}^r \setminus \mathbf{V}(q_1 \cdots q_n))) \supseteq \mathbf{I}(\mathbf{V}(J)) \supseteq J.$$

Para ver la inclusión contraria, sea $h \in \mathbf{I}(\phi(\mathbb{F}^r \setminus \mathbf{V}(q_1 \cdots q_n)))$. Sea N el mayor grado de una variable en $h = \sum_\alpha c_\alpha X^\alpha$, es decir, $\alpha_i \leq N$ para todo $\alpha \in \operatorname{supp}(h)$ y todo $1 \leq i \leq n$. Sea $q = q_1 \cdots q_n$. Tenemos que

$$q^N h = \textstyle\sum_\alpha c_\alpha q_\alpha (q_1x_1)^{\alpha_1} \cdots (q_nx_n)^{\alpha_n}$$

donde $q_\alpha = \prod_{i=1}^{n} q_i^{N-\alpha_i}$. Sea

$$H(z_1,\dots,z_n,t_1,\dots,t_r) = \sum_\alpha c_\alpha q_\alpha z_1^{\alpha_1}\cdots z_n^{\alpha_n}.$$

Consideremos en $\mathbb{F}[z_1,\dots,z_n,t_1,\dots,t_r]$ el orden LEX y dividamos H por $[z_1-f_1,\dots,z_n-f_n]$. Tenemos por tanto que

$$H = h_1(z_1-f_1)+\cdots+h_n(z_n-f_n)+\rho$$

donde $\rho\in\mathbb{F}[t_1,\dots,t_r]$. Reemplazando en la ecuación anterior z_i por q_ix_i, tenemos que

$$q^N h = p_1(q_1x_1-f_1)+\cdots+p_n(q_nx_n-f_n)+\rho.$$

Sea $(a_1,\dots,a_r)\in\mathbb{F}^r\setminus\mathbf{V}(q)$. Como $q(a_1,\dots,a_r)\neq 0$, tenemos que $q_i(a_1,\dots,a_r)\neq 0$ para cualquier $1\leq i\leq n$. Sea por tanto $b_i=\frac{f_i(a_1,\dots,a_r)}{q_i(a_1,\dots,a_r)}$. Por una parte

$$(q^N h)(a_1,\dots,a_r,b_1,\dots,b_n) = q(a_1,\dots,a_r)^N h(b_1,\dots,b_n) = 0$$

porque $h\in\mathbf{I}(\phi(\mathbb{F}^r\setminus\mathbf{V}(q)))$. Por otra

$$\left(\sum_{i=1}^{n} p_i(q_ix_i-f_i)+\rho\right)(a_1,\dots,a_r,b_1,\dots,b_n) = \rho(a_1,\dots,a_r),$$

lo que implica que $\rho(a_1,\dots,a_r)=0$ para cualquier $(a_1,\dots,a_r)\in\mathbb{F}^r\setminus\mathbf{V}(q)$. Esto implica que

$$(q\rho)(a_1,\dots a_r)=0$$

para todo $(a_1,\dots,a_r)\in\mathbb{F}^r$. Por la Proposición 2.15, $q\rho=0$, lo que implica que $\rho=0$ ya que $q\neq 0$. Por tanto

$$q^N y^N h = p_1 y^N(q_1x_1-f_1)+\cdots+p_n y^N(q_nx_n-f_n).$$

Como, además,

$$h = q^N y^N h + (1-(qy)^N)h = q^N y^N h + \left(\sum_{j=1}^{N-1}(qy)^i\right)(1-qy)h,$$

tenemos que $h \in \langle q_1 x_1 - f_1, \ldots, q_n x_n - f_n, 1-qy\rangle = I$. Dado que inicialmente $h \in \mathbb{F}[x_1, \ldots, x_n]$, tenemos que $h \in J$. Con esto demostramos que

$$\mathbf{I}(\phi(\mathbb{F}^r \setminus \mathbf{V}(q_1 \cdots q_n))) \subseteq J,$$

lo que termina la demostración. □

Ejemplo 4.14. Vamos a comprobar la parametrización racional de la circunferencia. Para ello sea

$$\begin{aligned}\phi : \mathbb{Q} &\to \mathbb{Q}^2\\ t &\mapsto \left(\tfrac{1-t^2}{1+t^2}, \tfrac{2t}{1+t^2}\right).\end{aligned}$$

Sea

$$I = \left\langle (1+t^2)x-(1-t^2), (1+t^2)y-2t, 1-(1+^2)^2 u\right\rangle \subseteq \mathbb{Q}[u,t,x,y].$$

Una base de Gröbner para I es

$$\left\{u - \tfrac{1}{2}x + \tfrac{1}{4}y^2 - \tfrac{1}{2}, tx + t - y, ty + x - 1, x^2 + y^2 - 1\right\},$$

por lo que la menor variedad que contiene a $\mathrm{im}(\phi)$ es

$$\mathbf{V}(I \cap \mathbb{Q}[x,y]) = \mathbf{V}(\langle x^2 + y^2 - 1\rangle).$$

4.4

Implicitación (cuerpo finito)

Teorema 4.15 (Implicitación polinomial)**.** *Sea* $\mathbb{F}_q$ *un cuerpo con* q *elementos. Sean* $f_1, \ldots, f_n \in \mathbb{F}_q[t_1, \ldots, t_r]$ *y sea*

$$\begin{aligned} \phi : \mathbb{F}^r &\to \mathbb{F}^n \\ (a_1, \ldots, a_r) &\mapsto (f_1(a_1, \ldots, a_r), \ldots, f_n(a_1, \ldots, a_r)) . \end{aligned}$$

Sea $I = \langle x_1 - f_1, \ldots, x_n - f_n, t_1^q - t_1, \ldots, t_r^q - t_r \rangle$*, un ideal en el anillo* $\mathbb{F}_q[t_1, \ldots, t_r, x_1, \ldots, x_n]$*, y sea* $J = I \cap \mathbb{F}_q[x_1, \ldots, x_n]$ *el ideal de* r*-eliminación. Entonces* $\mathbf{V}(J)$ *es la menor variedad que contiene a* $\phi(\mathbb{F}_q^r)$*.*

Demostración. La demostración es análoga a la del Teorema 4.11, empleando la Proposición 3.7 y la Proposición 2.18 en lugar de la 2.15. □

Ejercicios sobre Eliminación e Implicitación

Ejercicio 4.1. Dada la variedad afín definida por las ecuaciones

$$x^2 + 2y^2 = 3$$
$$x^2 + xy + y^2 = 3$$

calcula $I \cap \mathbb{F}[x]$ y $I \cap \mathbb{F}[y]$ donde I es el ideal que define la variedad. Haz el ejercicio para diferentes cuerpos.

Ejercicio 4.2. Calcula los ideales de eliminación I_1 e I_2 para el ideal en $\mathbb{F}[x, y, z]$ correspondiente a las ecuaciones

$$x^2 + y^2 + z^2 = 4$$
$$x^2 + 2y^2 = 5$$
$$xz = 1$$

Haz el ejercicio utilizando varios cuerpos.

Ejercicio 4.3. Sea $\preceq$ un orden admisible en $\mathbb{N}^n$. Definimos para $l \leq n$ el orden

$$\alpha \preceq_l \beta \iff \begin{cases} \alpha_1 + \cdots + \alpha_l < \beta_1 + \cdots + \beta_l & \text{o} \\ \alpha_1 + \cdots + \alpha_l = \beta_1 + \cdots + \beta_l \text{ y } \alpha \preceq \beta. \end{cases}$$

Demuestra que $\preceq_l$ es un orden de l-eliminación.

Ejercicio 4.4. Sea

$$I = \left\langle t^2 + x^2 + y^2 + z^2, t^2 + 2x^2 - xy - z^2, t + y^3 - z^3 \right\rangle \subseteq \mathbb{F}[t, x, y, z].$$

Calcula la base de Gröbner reducida G de $I \cap \mathbb{F}[x, y, z]$ con respecto al orden DEGREVLEX. Comprueba que $G \cup \{t + y^3 - z^3\}$ es una base de Gröbner para I con respecto al orden $(\leq_{\text{DEGREVLEX}})_1$ definido en el Ejercicio 4.3.

Ejercicio 4.5. Sea $\mathbb{F}$ un cuerpo de característica cero. Calcula la variedad cuyas ecuaciones paramétricas vienen dadas por

$$\begin{aligned} x &= t, \\ y &= t^2, \\ z &= t^3. \end{aligned}$$

Describe el subconjunto de $\mathbb{F}^3$ formado por la unión de las rectas tangentes a los puntos de la variedad anterior mediante ecuaciones paramétricas y calcula la menor variedad que las contiene.

Ejercicio 4.6. Calcula la menor variedad que contiene al subconjunto de $\mathbb{C}^3$ definido por

$$\begin{aligned} x &= uv, \\ y &= uv^2, \\ z &= u^2. \end{aligned}$$

Comprueba que hay puntos en la variedad que no están en la imagen de las ecuaciones paramétricas.

Ejercicio 4.7. El *paraguas de Whitney* es la superficie definida para-

métricamente por

$$\begin{aligned} x &= uv, \\ y &= v, \\ z &= u^2. \end{aligned}$$

Encuentra la menor variedad que contiene al paraguas de Whitney. Estudia si el paraguas de Whitney coincide con su variedad o está estrictamente contenido. Comprueba que los parámetros u, v no están determinados por x, y, z, es decir, hay puntos correspondientes a más de una pareja de valores de los parámetros.

Ejercicio 4.8. Sea $\mathbb{F}$ un cuerpo infinito. Sea $W = \mathbf{V}(q_1, \ldots, q_n) \subseteq \mathbb{F}$, y

$$\begin{aligned} \phi : \mathbb{F} \setminus W &\to \mathbb{F}^n \\ a &\mapsto \left(\tfrac{f_1(a)}{q_1(a)}, \ldots, \tfrac{f_n(a)}{q_n(a)} \right) \end{aligned}$$

donde $f_i(t)$ y $q_i(t)$ son primos relativos para cada $1 \leq i \leq n$. Sea $I = \langle q_1 x_1 - f_1, \ldots, q_n x_n - f_n \rangle \subseteq \mathbb{F}[t, x_1, \ldots, x_n]$. Demuestra que $\mathbf{V}(I_1)$ es la menor variedad afín que contiene a $\operatorname{im}(\phi)$.

Ejercicio 4.9. *Folium de Descartes*. Encuentra la menor variedad asociada a las ecuaciones paramétricas

$$\begin{aligned} x &= \frac{3t}{1+t^3}, \\ y &= \frac{3t^2}{1+t^3}. \end{aligned}$$

¿Existen puntos en la variedad no parametrizables sobre $\mathbb{R}$ o $\mathbb{C}$?.

Capítulo 5

Variedades Irreducibles y Descomposición

5.1 Teorema de los ceros de Hilbert

Dado $a \in \mathbb{F}$ y $f \in \mathbb{F}[X]$, denotamos por $\bar{f} = f(x_1, \ldots, x_{n-1}, a) \in \mathbb{F}[x_1, \ldots, x_{n-1}]$. Si $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ es un ideal, denotamos también

$$I_{x_n=a} = \{\bar{f} \mid f \in I\}.$$

Lema 5.1. *Si $\mathbb{F}$ es algebraicamente cerrado y $I \subsetneq \mathbb{F}[x_1, \ldots, x_n]$, existe $a \in \mathbb{F}$ tal que $I_{x_n=a} \subsetneq \mathbb{F}[x_1, \ldots, x_{n-1}]$.*

Demostración. La demostración se divide en dos casos.

Caso 1. $I \cap \mathbb{F}[x_n] \neq \{0\}$. Sea $f \in I \cap \mathbb{F}[x_n]$ no nulo. f no puede ser constante porque $1 \notin I$, y no perdemos generalidad en suponer que es mónico. Como $\mathbb{F}$ es algebraicamente cerrado,

$$f = \prod_{i=1}^{r} (x_n - b_i)^{m_i},$$

con $b_1, \ldots, b_r \in \mathbb{F}$. Supongamos que para todo $1 \leq i \leq r$, $I_{x_n=b_1} = \mathbb{F}[x_1, \ldots, x_{n-1}]$. Existe entonces, para cada $1 \leq i \leq r$, un $g_i \in I$ tal que $g_i(x_1, \ldots, x_{n-1}, b_i) = 1$. Esto implica que

$$\begin{aligned} 1 &= g_i(x_1, \ldots, x_{n-1}, b_i) \\ &= g_i(x_1, \ldots, x_{n-1}, x_n - (x_n - b_i)) = g_i - h_i(x_n - b_i) \end{aligned}$$

para ciertos $h_i \in \mathbb{F}[x_1, \ldots, x_n]$. Tenemos, por consiguiente

$$1 = \prod_{i=1}^{r} (g_i - h_i(x_n - b_i))^{m_i} = h \prod_{i=1}^{r} (x_n - b_i)_i^m + g,$$

donde $h = \prod_{i=1}^{r} h_i^{m_i}$ y $g \in I$. Como $\prod_{i=1}^{r} (x_n - b_i)^{m_i} = f \in I$, concluimos que $1 \in I$, lo que es imposible porque I es un ideal propio. Debe, por tanto, existir una raíz b_i tal que $I_{x_n=b_i} \neq \mathbb{F}[x_1, \ldots, x_{n-1}]$, lo que demuestra el lema en el caso 1.

Caso 2. $I \cap \mathbb{F}[x_n] = \{0\}$. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para I con respecto al orden LEX. Podemos expresar

$$g_i = c_i(x_n) X^{\alpha(i)} + \sum_{\beta < \alpha(i)} c_\beta X^\beta$$

donde $c_i(x_n) \in \mathbb{F}[x_n] \setminus \{0\}$ y $\alpha(i)_n = 0$. Como $\mathbb{F}$ es algebraicamente cerrado, es infinito, por lo que existe $a \in \mathbb{F}$ tal que $c_i(a) \neq 0$ para cada $1 \leq i \leq r$. Es fácil comprobar que

$$I_{x_n=a} = \langle \overline{g_1}, \ldots, \overline{g_t} \rangle$$

y que $\exp(\overline{g_i}) = \alpha(i)$. Además $\alpha(i) \neq 0$ ya que en caso contrario $g_i = c_i \in I \cap \mathbb{F}[x_n] = \{0\}$, lo que es imposible. Veamos que $\{\overline{g_1}, \ldots, \overline{g_t}\}$ es una base de Gröbner para $I_{x_n=a}$. Sean $g_i, g_j \in G$ y $\gamma = \operatorname{lcm}(\alpha(i), \alpha(j))$. Sea

$$S = c_j(x_n)X^{\gamma-\alpha(i)}g_i - c_i(x_n)X^{\gamma-\alpha(j)}g_j.$$

Tenemos que $\exp(S) < \gamma$. Como $S \in I$, $S = \sum_{l=1}^{t} h_l g_l$ con $\exp(h_l g_l) \leq \exp(S)$. Evaluando en $x_n = a$,

$$c_j(a)X^{\gamma-\alpha(i)}\overline{g_i} - c_i(a)X^{\gamma-\alpha(j)}\overline{g_j} = \sum_{l=1}^{t} \overline{h_l}\,\overline{g_l}.$$

Como $\exp(\overline{g_i}) = \alpha(i)$, tenemos que $\overline{S}$ es un múltiplo constante del S-polinomio $S(\overline{g_i}, \overline{g_j})$. Además,

$$\gamma > \exp(S) \geq \exp(h_l g_l), \quad 1 \leq l \leq t,$$

por lo que

$$\gamma > \exp(\overline{h_l}\,\overline{g_l}), \quad 1 \leq l \leq t.$$

Por el Teorema 3.4, $\operatorname{rem}(S(\overline{g_i}, \overline{g_j}), \{\overline{g_1}, \ldots, \overline{g_t}\}) = 0$, lo que implica que $\{\overline{g_1}, \ldots, \overline{g_t}\}$ es una base de Gröbner para $I_{x_n=a}$. Como $\alpha(i) \neq 0$ para cada $1 \leq i \leq t$, tenemos que $1 \notin I_{x_n=a}$, lo que demuestra el caso 2 y el lema. □

Teorema 5.2 (Nullstellensatz débil)**.** *Sea $\mathbb{F}$ un cuerpo algebraicamente cerrado. Sea $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ un ideal tal que $\mathbf{V}(I) = \varnothing$. Entonces $I = \mathbb{F}[x_1, \ldots, x_n]$.*

Demostración. Es un sencillo argumento inductivo obtenido a partir del Lema 5.1. □

Teorema 5.3 (Nullstellensatz)**.** *Sea* $\mathbb{F}$ *un cuerpo algebraicamente cerrado. Sea* $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ *un ideal. Entonces* $f \in \mathbf{I}(\mathbf{V}(I))$ *si y solo si* $f^m \in I$ *para algún* $m \in \mathbb{N}$.

Demostración. Es sencillo comprobar que si $f^m \in I$, entonces $f \in \mathbf{I}(\mathbf{V}(I))$. Supongamos por tanto que $f \in \mathbf{I}(\mathbf{V}(I))$. Sea

$$J = \langle I \rangle + \langle yf - 1 \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n, y]$$

y sea $(a_1, \ldots, a_n, a_{n+1}) \in \mathbb{F}^{n+1}$. Si $(a_1, \ldots, a_n) \in \mathbf{V}(I)$, tenemos que $f(a_1, \ldots, a_n) = 0$, por lo que

$$1 - a_{n+1} f(a_1, \ldots, a_n) = 1 \neq 0,$$

es decir, $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(J)$. Por otra parte, si $(a_1, \ldots, a_n) \notin \mathbf{V}(I)$, tenemos que $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(I) \supseteq \mathbf{V}(J)$ viendo $I \subseteq \mathbb{F}[x_1, \ldots, x_n, y]$. En cualquier caso $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(J)$, por lo que $\mathbf{V}(J) = \varnothing$. Por el Teorem 5.2,

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf)$$

para ciertos $p_i, q \in \mathbb{F}[x_1, \ldots, x_n, y]$ y $f_i \in I$ con $1 \leq i \leq s$. Sea $y = \frac{1}{f}$. Tenemos que

$$1 = \sum_{i=1}^{s} p_i \left(x_1, \ldots, x_n, \tfrac{1}{f}\right) f_i.$$

Multiplicando ambos lados de la igualdad por f^m con m suficientemente grande para que se eliminen todos los denominadores, tenemos que

$$f^m = \sum_{i=1}^{s} h_i f_i$$

para ciertos $h_i \in \mathbb{F}[x_1, \ldots, x_n]$ con $1 \leq i \leq s$. En conclusión $f^m \in I$, como queríamos. □

5.2

Radical de un ideal

Sea I un ideal de un anillo conmutativo R. Se define el radical de I como el conjunto

$$\sqrt{I} = \{f \in R \mid f^m \in I \text{para algún } m \in \mathbb{N}\}$$

.

Proposición 5.4. *$\sqrt{I}$ es un ideal de R que contiene a I.*

Demostración. Es inmediato que $I \subseteq \sqrt{I}$. Sean $f, g \in \sqrt{I}$ y sean m, l tales que $f^m, g^l \in I$. Dado que

$$\begin{aligned}(f+g)^{m+l} &= \textstyle\sum_{k=0}^{m} \binom{m+l}{k} f^k g^{m+l-k} + \sum_{k=m+1}^{m+l} \binom{m+l}{k} f^k g^{m+l-k} \\ &= g^l \textstyle\sum_{k=0}^{m} \binom{m+l}{k} f^k g^{m-k} \\ &\quad + f^m \textstyle\sum_{k=m+1}^{m+l} \binom{m+l}{k} f^{k-m} g^{m+l-k} \\ &\in I,\end{aligned}$$

tenemos que $f + g \in \sqrt{I}$. Por otra parte,

$$(hf)^m = h^m f^m \in I$$

para cualquier $h \in R$. Por tanto $\sqrt{I}$ es un ideal. □

Decimos que un ideal es radical si $I = \sqrt{I}$. Observemos que I es radical si y solo si

$$f^m \in I \text{ para algún } m \in \mathbb{N} \Rightarrow f \in I.$$

Lema 5.5. *Sea* $A \subseteq \mathbb{F}^n$. *Entonces* $\mathbf{I}(A)$ *es un ideal radical.*

Demostración. Supongamos que $f^m \in \mathbf{I}(A)$. Entonces para cualquier $a \in A$, $f(a)^m = 0$, lo que implica que $f(a) = 0$ para cualquier $a \in A$. En consecuencia $f \in \mathbf{I}(A)$. □

Teorema 5.6 (Nullstellensatz fuerte)**.** *Sea* $\mathbb{F}$ *algebraicamente cerrado. Si* $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ *es un ideal,*

$$\sqrt{I} = \mathbf{I}(\mathbf{V}(I)).$$

Demostración. Si $f \in \sqrt{I}$, tenemos que $f^m \in I \subseteq \mathbf{I}(\mathbf{V}(I))$. Por el Lema 5.5, $f \in \mathbf{I}(\mathbf{V}(I))$.
Por otra parte, si $f \in \mathbf{I}(\mathbf{V}(I))$, por el Teorema 5.3 $f^m \in I$ para algún $m \in \mathbb{N}$, es decir, $f \in \sqrt{I}$. □

Teorema 5.7. *Sea* $\mathbb{F}$ *un cuerpo.*

(A) Las aplicaciones

$$\textit{variedades afines} \xrightarrow{\mathbf{I}} \textit{ideales}$$

y

$$\textit{ideales} \xrightarrow{\mathbf{V}} \textit{variedades afines}$$

invierten la inclusión.

(B) Para cada variedad V, $\mathbf{V}(\mathbf{I}(V)) = V$, *por lo que* $\mathbf{I}$ *es inyectiva.*

(C) $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$ *para cualquier ideal* I.

(D) Si $\mathbb{F}$ *es algebraicamente cerrado, las aplicaciones*

$$\textit{variedades afines} \xrightarrow{\mathbf{I}} \textit{ideales radicales}$$

y

$$\textit{ideales radicales} \xrightarrow{\mathbf{V}} \textit{variedades afines}$$

son biyecciones inversa una de otra que invierten la inclusión.

Demostración. Ejercicio. □

Proposición 5.8. *Sea* $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$. *Sea* $f \in \mathbb{F}[x_1, \ldots, x_n]$ *y sea* $J = \langle I \rangle + \langle 1 - fy \rangle \subseteq \mathbb{F}[x_1, \ldots x_n, y]$. *Tenemos que* $f \in \sqrt{I}$ *si y solo si* $J = \mathbb{F}[x_1, \ldots x_n, y]$.

Demostración. Un argumento análogo al empleado en la demostración del Teorema 5.3 demuestra que si $J = \mathbb{F}[x_1, \ldots x_n, y]$, tenemos que $f^m \in I$ para algún $m \in \mathbb{N}$, por lo que $f \in \sqrt{I}$.
Para ver la implicación contraria, supongamos que $f^m \in I \subseteq J$. Como $1 - fy \in J$, tenemos que

$$\begin{aligned} 1 &= y^m f^m + (1 - (yf)^m) \\ &= y^m f^m + (1 + yf + \cdots + (yf)^{m-1})(1 - yf) \in J, \end{aligned}$$

por lo que $J = \mathbb{F}[x_1, \dots x_n, y]$. □

Proposición 5.9. $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Demostración. Si $f \in \sqrt{I \cap J}$, $f^m \in I \cap J \subseteq I$, por lo que $f \in \sqrt{I}$. Análogamente $f \in \sqrt{J}$ y tenemos la inclusión $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$. Si $f \in \sqrt{I} \cap \sqrt{J}$, existen m, l tales que $f^m \in I$ y $f^l \in J$. En consecuencia $f^{m+l} = f^m f^l \in I \cap J$, por lo que $f \in \sqrt{I \cap J}$. □

5.3 Cocientes de ideales y saturación

Sea I un ideal en un anillo conmutativo R y sea $F \subseteq R$ no vacío. Se define el cociente como

$$I : F = \{f \in R \mid fg \in I \ \forall g \in F\}$$

Proposición 5.10. $I : F$ *es un ideal que contiene a* I.

Demostración. Es inmediato observar que si $f \in I$, entonces $fg \in I$ para todo $g \in F$, por lo que $f \in I : J$. Sean $f_1, f_2 \in I : J$. Entonces para todo $g \in F$, $f_1 g, f_2 g \in I$, lo que implica que

$$(f_1 + f_2)g = f_1 g + f_2 g \in I,$$

para todo $g \in F$. Esto demuestra que $f_1 + f_2 \in I : F$. Por otra parte, sea $f \in I : F$, $h \in R$ y $g \in F$. Como $fg \in I$, tenemos que $hfg \in I$. Al ser $g \in F$ un elemento arbitrario, tenemos que $hf \in I : F$, lo que demuestra que $I : F$ es un ideal. □

Proposición 5.11. $I : F = I : \langle F \rangle$.

Demostración. Como $F \subseteq \langle F \rangle$, tenemos que $I : F \supseteq I : \langle F \rangle$. Sea $f \in I : F$ y sea $g = \sum_{i=1}^{s} h_i f_i \in \langle F \rangle$ para ciertos $f_1, \ldots, f_s \in F$. Como $ff_i \in I$, para cada $1 \leq i \leq s$, tenemos que

$$fg = \sum_{i=1}^{s} h_i f f_i \in I,$$

lo que implica que $f \in I : \langle F \rangle$ al ser g un elemento arbitrario de $\langle F \rangle$. □

La saturación se define de manera similar. Sea I un ideal en un anillo conmutativo R y sea $F \subseteq R$ no vacío. La saturación de I respecto de F se define como

$$I : F^{\infty} = \{f \in R \mid \forall g \in F, \exists n \in \mathbb{N}, fg^n \in I\}$$

Proposición 5.12. $I : F^{\infty} = I : \langle F \rangle^{\infty}$.

Demostración. Como $F \subseteq \langle F \rangle$, tenemos que $I : F^{\infty} \supseteq I : \langle F \rangle^{\infty}$. Sea $f \in I : F^{\infty}$ y sea $g = \sum_{i=1}^{s} h_i g_i \in \langle F \rangle$ para ciertos $g_1, \ldots, g_s \in F$. Existe $n \in \mathbb{N}$ tal que $fg_i^n \in I$ para todo $1 \leq i \leq s$. Por el Teorema multinomial

$$g^{sn} = \sum_{k_1+\cdots+k_s=sn} \binom{sn}{k_1,\ldots,k_s} \prod_{i=1}^{s} (h_i g_i)^{k_i},$$

por lo que

$$fg^{sn} = \sum_{k_1+\cdots+k_s=sn} \binom{sn}{k_1,\ldots,k_s} \prod_{i=1}^{s} h_i^{k_i} f g_i^{k_i} \in I,$$

ya que $k_1 + \cdots + k_s = sn$ implica que existe un $1 \leq i \leq s$ tal que $k_i \geq n$. Dado que g es un elemento arbitrario de $\langle F \rangle$, tenemos que $f \in I : \langle F \rangle^{\infty}$. □

En vista de las Proposiciones 5.11 y 5.12 no perdemos generalidad si nos restringimos a calculas cocientes y saturaciones de ideales.

Proposición 5.13. *Sean* I, J *ideales de* R. *Se verifican las siguientes afirmaciones:*

(A) $I : J^\infty$ *es un ideal.*

(B) $I \subseteq I : J^m \subseteq I : J^\infty$ *para todo* $m \in \mathbb{N}$.

(C) Si R *es Noetheriano, existe* $N \in \mathbb{N}$ *tal que* $I : J^\infty = I : J^n$ *para todo* $n \geq N$.

(D) Si J *es finitamente generado,* $\sqrt{I : J^\infty} = \sqrt{I} : J$.

Demostración. El apartado (A) es análogo a la parte correspondiente de la Proposición 5.10, y se deja como ejercicio.
Si $f \in I : J^m$ y $g \in J$, tenemos que $g^m \in J^m$, por lo que $fg^m \in I$, lo que implica que $f \in I : J^\infty$, es decir $I : J^m \subseteq I : J^\infty$. Observemos que $J_1 \subseteq J_2$ implica que $I : J_1 \subseteq I : J_2$, por lo que $I : J^m \subseteq I : J^{m+1}$, y en particular $I : J \subseteq I : J^m$ para cualquier $m \geq 1$. El apartado (B) es, por tanto, consecuencia de la Proposición 5.10.
La cadena descendente

$$J \supseteq J^2 \supseteq \cdots \supseteq J^n \supseteq \cdots$$

produce una cadena ascendente

$$I : J \subseteq I : J^2 \subseteq \cdots \subseteq I : J^n \subseteq \cdots .$$

Si R es Noetheriano, la cadena anterior debe estabilizar, es decir, existe $N \in \mathbb{N}$ tal que $I : J^N = I : J^n$ para todo $n \geq N$. Para demostrar

(C) veamos que $I : J^N = I : J^\infty$. Sea $f \in I : J^N$ y $g \in J$. Ya hemos visto que $I : J^N \subseteq I : J^\infty$, por lo que nos queda comprobar la inclusión contraria. Como $J = \langle g_1, \ldots, g_s \rangle$, por la Proposición 5.12 $I : J^\infty = I : \{g_1, \ldots, g_s\}^\infty$. Sea $f \in I : \{g_1, \ldots, g_s\}^\infty$, existe $M \geq N$ tal que $fg_i^M \in I$ para cualquier $1 \leq i \leq s$, por lo que $f \in I : \langle g_1^M, \ldots, g_s^M \rangle$. Es un ejercicio demostrar que

$$J^{sM} \subseteq \langle g_1^M, \ldots, g_s^M \rangle,$$

por lo que

$$I : \langle g_1^M, \ldots, g_s^M \rangle \subseteq I : J^{sM} = I : J^N.$$

En consecuencia $f \in I : J^N$, lo que demuestra (C).
El apartado (D) también lo demostramos por doble inclusión. Supongamos que $f \in \sqrt{I : J^\infty}$. Existe $m \in \mathbb{N}$ tal que $f^m \in I : J^\infty$. Dado $g \in J$, existe $M \in \mathbb{N}$ tal que $f^m g^M \in I$, lo que implica que $(fg)^{\max\{m,M\}} \in I$, es decir, $fg \in \sqrt{I}$. Como g es un elemento arbitrario de J, tenemos que $f \in \sqrt{I} : J$, lo que demuestra que $\sqrt{I : J^\infty} \subseteq \sqrt{I} : J$. Recíprocamente, sea $f \in \sqrt{I} : J$ y sea $J = \langle g_1, \ldots, g_s \rangle$. Existe $M \in \mathbb{N}$ tal que $f^M g_i^M = (fg_i)^M \in I$ para cada $1 \leq i \leq s$, lo que implica que

$$f^M \in I : \langle g_1^M, \ldots, g_s^M \rangle \subseteq I : J^{sM}$$

de igual forma a la demostración del apartado (C). Como por (B)

$$I : J^{sM} \subseteq I : J^\infty,$$

tenemos que $f \in \sqrt{I : J^\infty}$, lo que demuestra la inclusión $\sqrt{I} : J \subseteq \sqrt{I : J^\infty}$ y el resultado. □

Proposición 5.14. *Sean* $I, J_1, \ldots, J_r$ *ideales en un anillo conmutativo* R. *Entonces*

$$I : \left(\sum_{i=1}^{r} J_i\right) = \bigcap_{i=1}^{r} (I : J_i)$$

y

$$I : \left(\sum_{i=1}^{r} J_i\right)^{\infty} = \bigcap_{i=1}^{r} (I : J_i^{\infty})$$

Demostración. Ejercicio □

Corolario 5.15. *Sea* I *un ideal de* R *y* $g_1, \ldots, g_s \in R$. *Entonces*

$$I : \{g_1, \ldots, g_s\} = \bigcap_{i=1}^{s} (I : g_i)$$

y

$$I : \{g_1, \ldots, g_s\}^{\infty} = \bigcap_{i=1}^{s} (I : g_i^{\infty}) .$$

Teorema 5.16. *Sea* I *un ideal de* $\mathbb{F}[x_1, \ldots, x_n]$ *y sea* $g \in \mathbb{F}[x_1, \ldots, x_n]$.

(A) Si $I \cap \langle g \rangle = \langle h_1, \ldots, h_s \rangle$, *entonces* $I : g = \langle h_1/g, \ldots, h_s/g \rangle$.

(B) Sea $\tilde{I} = \langle I \rangle + \langle 1 - yg \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n, y]$. *Entonces*

$$I : g^{\infty} = \tilde{I} \cap \mathbb{F}[x_1, \ldots, x_n].$$

Demostración. Si $f \in \langle h_1/g, \ldots, h_s/g \rangle$, tenemos que $f = \sum_{i=1}^{s} a_i(h_i/g)$, por lo que

$$fg = \sum_{i=1}^{s} a_i h_i \in I \cap \langle g \rangle \subseteq I,$$

por lo que $f \in I : g$. Recíprocamente, si $fg \in I$, dado que $fg \in \langle g \rangle$, tenemos que $fg = \sum_{i=1}^{r} a_i h_i$, por lo que $f = \sum_{i=1}^{r} a_i(h_i/g)$, por lo que $I : g \subseteq \langle h_1/g, \ldots, h_s/g \rangle$. Con esto tenemos (A).
El apartado (B) se deja como ejercicio. □

5.4

Variedades irreducibles

Definición 5.17. Una variedad afín $V \subseteq \mathbb{F}^n$ se dice irreducible si $V = V_1 \cup V_2$ con V_1, V_2 variedades afines implica que $V = V_1$ o $V = V_2$.

Definición 5.18. Un ideal $I \subseteq R$ en un anillo conmutativo se dice primo si $fg \in I$ implica $f \in I$ o $g \in I$.

Proposición 5.19. *Un ideal $I \subseteq R$ es primo si y solo si R/I es un dominio.*

Demostración. Ejercicio. □

Proposición 5.20. *Una variedad afín $V \subseteq \mathbb{F}^n$ es irreducible si y solo si $\mathbf{I}(V)$ es un ideal primo.*

Demostración. Supongamos que V es irreducible y sean f, g tales que $fg \in \mathbf{I}(V)$. Sean $V_1 = V \cap \mathbf{V}(f)$ y $V_2 = V \cap \mathbf{V}(g)$. Dado $a \in V$, como $(fg)(a) = 0$ tenemos que $a \in \mathbf{V}(f)$ o $a \in \mathbf{V}(g)$, por lo que deducimos que $V = V_1 \cup V_2$. Dado que V es irreducible, tenemos que $V = V_1$ o $V = V_2$. Si $V = V_1 = V \cap \mathbf{V}(f)$, tenemos que $V \subseteq \mathbf{V}(f)$, lo que implica que $f \in \mathbf{I}(V)$. Si $V = V_2$ concluimos que $g \in \mathbf{I}(V)$, lo que implica que $\mathbf{I}(V)$ es primo.
Recíprocamente, supongamos que $\mathbf{I}(V)$ es primo y supongamos que $V = V_1 \cup V_2$. Supongamos que $V \neq V_1$. Como $V_2 \subseteq V$, tenemos que $\mathbf{I}(V) \subseteq \mathbf{I}(V_2)$. Sea $f \in \mathbf{I}(V_2)$. Dado que $V_1 \subsetneq V$, tenemos que $\mathbf{I}(V) \subsetneq \mathbf{I}(V_1)$, por lo que existe $g \in \mathbf{I}(V_1) \setminus \mathbf{I}(V)$. Dado $a \in V = V_1 \cup V_2$, si $a \in V_1$ tenemos que $g(a) = 0$, y si $a \in V_2$ concluimos que $f(a) = 0$. En ambos casos $(fg)(a) = f(a)g(a) = 0$,

por lo que $fg \in \mathbf{I}(V)$. Como $\mathbf{I}(V)$ es primo y $g \notin \mathbf{I}(V)$ tenemos que $f \in \mathbf{I}(V)$, lo que implica que $\mathbf{I}(V) = \mathbf{I}(V_2)$. En consecuencia $V = V_2$ y V es irreducible. □

Corolario 5.21. *Si $\mathbb{F}$ es algebraicamente cerrado, $\mathbf{I}()$ y $\mathbf{V}()$ proporcionan biyecciones entre variedades irreducibles e ideales primos.*

Proposición 5.22. *Si $\mathbb{F}$ es un cuerpo infinito, toda variedad definida por parametrizaciones racionales es irreducible.*

Demostración. Sea V la menor variedad conteniendo a la imagen de la aplicación

$$\begin{aligned} \phi : \mathbb{F}^r \setminus W &\to \mathbb{F}^n \\ (a_1, \ldots, a_r) &\mapsto \left(\tfrac{f_1(a_1,\ldots,a_r)}{q_1(a_1,\ldots,a_r)}, \ldots, \tfrac{f_n(a_1,\ldots,a_r)}{q_n(a_1,\ldots,a_r)} \right), \end{aligned}$$

donde $f_1, \ldots, f_n, q_1, \ldots, q_n \in \mathbb{F}[t_1, \ldots, t_r]$ y $W = \mathbf{V}(q_1 \cdots q_n)$. Dado que $\mathbf{I}(V) = \mathbf{I}(\mathrm{im}(\phi))$, tenemos que

$$\mathbf{I}(V) = \{h \in \mathbb{F}[X] \mid (h \circ \phi)(a) = 0 \; \forall a \in \mathbb{F}^r \setminus W\}.$$

Si $a \in \mathbb{F}^r \setminus W$, tenemos que

$$(h \circ \phi)(a) = 0 \iff ((q_1 \cdots q_n)^N (h \circ \phi))(a) = 0.$$

Sea N el grado total de h. Es un ejercicio comprobar que

$$(q_1 \cdots q_n)^N (h \circ \phi) \in \mathbb{F}[t_1, \ldots, t_r].$$

Como $\mathbb{F}$ es infinito, concluimos que

$$h \in \mathbf{I}(V) \iff (q_1 \cdots q_n)^N (h \circ \phi) = 0 \in \mathbb{F}[t_1, \ldots, t_r].$$

Supongamos que $fg \in \mathbf{I}(V)$, y sean M y N los grados totales de f y g respectivamente. Como el grado total de fg es $M + N$, tenemos que

$$(q_1 \cdots q_n)^M (f \circ \phi)(q_1 \cdots q_n)^N (g \circ \phi) = \\ (q_1 \cdots q_n)^{M+N} (f \circ \phi)(g \circ \phi) = 0.$$

Como $\mathbb{F}[t_1, \ldots, t_r]$ es un dominio y $(q_1 \cdots q_n)^M (f \circ \phi)$, $(q_1 \cdots q_n)^N (g \circ \phi)$ son polinomios, tenemos que uno de ellos debe ser cero, es decir, $f \in \mathbf{I}(V)$ o $g \in \mathbf{I}(V)$. Con esto demostramos que $\mathbf{I}(V)$ es un ideal primo, lo que implica por la Proposición 5.20 que V es irreducible. □

Definición 5.23. Un ideal $I \subseteq R$ se dice maximal si $I \neq R$, y para cualquier otro ideal J tal que $I \subseteq J \subseteq R$, se tiene que $J = I$ o $J = R$.

Proposición 5.24. *$M \subseteq R$ es maximal si y sólo si R/M es un cuerpo.*

Demostración. Ejercicio. □

Corolario 5.25. *Todo ideal maximal es primo.*

Demostración. Consecuencia inmediata del hecho de que todo cuerpo es un dominio. □

Proposición 5.26. *Dados $a_1, \ldots, a_n \in \mathbb{F}$, el ideal*

$$\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$$

es maximal.

Demostración. Ejercicio. □

Teorema 5.27. *Si $\mathbb{F}$ es algebraicamente cerrado, $I \subseteq \mathbb{F}[X]$ es maximal si y solo si*

$$I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$$

para ciertos $a_1, \ldots, a_n \in \mathbb{F}$.

Demostración. Dado que $I \neq \mathbb{F}[X]$, $\mathbf{V}(I) \neq \varnothing$ por el Teorema 5.2, es decir, existe $(a_1, \ldots, a_n) \in \mathbf{V}(I)$. Como para cualquier $f \in I$, tenemos que $f(a_1, \ldots, a_n) = 0$, tenemos que $f \in \mathbf{I}(\{(a_1, \ldots, a_n)\})$. Por tanto

$$I \subseteq \mathbf{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle,$$

donde la última igualdad es un ejercicio. Por la Proposición 5.26, tenemos que $I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. □

Corolario 5.28. *Si $\mathbb{F}$ es algebraicamente cerrado, existe una biyección entre los puntos de $\mathbb{F}^n$ y los ideales maximales de $\mathbb{F}[x_1, \ldots, x_n]$.*

5.5 Descomposición de variedades

Proposición 5.29. *Las variedades afines satisfacen la condición de cadena descendente.*

Demostración. Supongamos que tenemos una cadena de variedades afines en $\mathbb{F}^n$

$$V_1 \supseteq V_2 \supseteq \cdots \supseteq V_m \supseteq V_{m+1} \supseteq \cdots.$$

Esta cadena induce la cadena siguiente de ideales en $\mathbb{F}[x_1, \ldots, x_n]$

$$\mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \subseteq \cdots \subseteq \mathbf{I}(V_m) \subseteq \mathbf{I}(V_{m+1}) \subseteq \cdots.$$

Como $\mathbb{F}[x_1, \ldots, x_n]$ es Noetheriano, existe m_0 tal que, $\mathbf{I}(V_{m_0}) = \mathbf{I}(V_m)$ para todo $m \geq m_0$, lo que implica que $V_{m_0} = V_m$ para todo $m \geq m_0$. □

Teorema 5.30. *Toda variedad $V \subseteq \mathbb{F}^n$ se descompone como una unión finita $V = V_1 \cup \cdots \cup V_m$ de variedades irreducibles.*

Demostración. Si V no puede ponerse como unión finita de variedades irreducibles tenemos $V = V_1 \cup V_1'$ con $V \supsetneq V_1$, $V \subsetneq V_1'$ y V_1 tampoco puede ponerse como unión finita de variedades irreducibles. Por el mismo argumento $V_1 = V_2 \cup V_2'$ con $V_1 \supsetneq V_2$, $V_1 \supsetneq V_2'$ y V_2 una variedad que no puede ponerse como unión finita de variedades irreducibles. Reiterando la construcción llegamos a una cadena infinita

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq \cdots$$

de variedades afines, lo que no puede existir por la Proposición 5.29. □

Definición 5.31. Sea $V \subseteq \mathbb{F}^n$ una variedad afín. Una descomposición

$$V = V_1 \cup \cdots \cup V_m$$

como unión de variedades irreducibles se dice minimal si $V_i \nsubseteq V_j$ cuando $i \neq j$.

Teorema 5.32. *Toda variedad afín $V \subseteq \mathbb{F}^n$ tiene una descomposición minimal, que es única salvo el orden.*

Demostración. El Teorema 5.30 garantiza una descomposición

$$V = V_1 \cup \cdots \cup V_m$$

como unión de variedades irreducibles. Si existen $i \neq j$ tales que $V_i \subseteq V_j$, tenemos que

$$V = V_1 \cup \cdots \cup V_{i-1} \cup V_{i+1} \cup \cdots \cup V_m$$

es también una descomposición en variedades irreducibles. Reiterando la operación llegamos a una descomposición minimal.
Para ver la unicidad, supongamos que tenemos otra descomposición minimal $V = V'_1 \cup \cdots \cup V'_l$. Tenemos que

$$V_i = V_i \cap V = (V_i \cap V'_1) \cup \cdots \cup (V_i \cap V'_l).$$

Por la irreducibilidad de V_i, existe j tal que $V_i = V_i \cap V'_j$, es decir, $V_i \subseteq V'_j$. Argumentando de forma análoga, $V'_j \subseteq V_k$ para cierto k, por lo que

$$V_i \subseteq V'_j \subseteq V_k.$$

Por la minimalidad de la descomposición tenemos que $i = k$ y $V_i = V'_j$. Esto implica que $m \leq l$ y

$$\{V_1, \ldots, V_m\} \subseteq \{V'_1, \ldots, V'_l\}.$$

Invistiendo los papeles de las descomposiciones tenemos que $l \leq m$ y

$$\{V'_1, \ldots, V'_l\} \subseteq \{V_1, \ldots, V_m\}.$$

lo que da la unicidad de la descomposición minimal. □

5.6 Descomposición primaria de ideales

Definición 5.33. Un ideal $I \subseteq R$ se dice primario si $fg \in I$ implica que $f \in I$ o que $g^m \in I$ para cierto $m \geq 0$.

Lema 5.34. *Si* I *es primario,* $\sqrt{I}$ *es primo, en cuyo caso* $\sqrt{I}$ *es el menor ideal primo que contiene a* I.

Demostración. Ejercicio. □

Si I es primario y $P = \sqrt{I}$, se dice que I es P-primario.
Digamos que $I \subseteq R$ es irreducible si $I = I_1 \cap I_2$ implica que $I = I_1$ o $I = I_2$.

Lema 5.35. *Todo ideal irreducible es primario.*

Demostración. Supongamos que I es irreducible y que $fg \in I$. Por la Proposición 5.13, existe N tal que $I : g^\infty = I : g^N$. Es un ejercicio comprobar que $I = (I + \langle g^N \rangle) \cap (I + \langle f \rangle)$. Como I es irreducible, tenemos que $I = (I + \langle g^N \rangle)$ o $I = (I + \langle f \rangle)$, lo que implica que $f \in I$ o $g^N \in I$. □

Teorema 5.36. *Todo ideal de un anillo conmutativo Noetheriano* R *puede ponerse como intersección finita de ideales primarios.*

Demostración. Digamos que $I \subseteq R$ es irreducible si $I = I_1 \cap I_2$ implica que $I = I_1$ o $I = I_2$. De forma análoga al Teorema 5.30 pero empleando la condición de cadena ascendente, podemos demostrar que todo ideal puede escribirse como una intersección finita de ideales irreducibles. El Teorema es por tanto consecuencia del Lema 5.35. □

Definición 5.37. Una descomposición primaria de un ideal I es una expresión $I = \bigcap_{i=1}^{m} Q_i$ donde Q_i es primario para todo $1 \leq i \leq m$. La descomposición se dice minimal si $\sqrt{Q_i} \neq \sqrt{Q_j}$ para $i \neq j$ y $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$.

Lema 5.38. *Si* I, J *son primarios tales que* $\sqrt{I} = \sqrt{J}$*, entonces* $I \cap J$ *es primario.*

Demostración. Ejercicio. □

Teorema 5.39 (Lasker-Noether)**.** *Todo ideal* $I \subseteq R$ *en un anillo conmutativo Noetheriano tiene una descomposición primaria minimal.*

Demostración. La existencia de la descomposición primaria $I = \bigcap_{i=1}^{m} Q_i$ es consecuencia del Teorema 5.36. Supongamos que existen $i \neq j$ tales que $\sqrt{Q_i} = \sqrt{Q_j}$. Por el Lema 5.38, $Q_{ij} = Q_i \cap Q_j$ es un ideal primario, por lo que podemos cambiar Q_i y Q_j por Q_{ij} en la descomposición primaria. Reiterando el procedimiento eventualmente llegamos a una descomposición primaria en la que cada radical es distinto. Llamamos nuevamente $I = \bigcap_{i=1}^{m} Q_i$ a dicha descomposición. Si existe i tal que $Q_i \supseteq \bigcap_{j \neq i} Q_j$, tenemos que $I = \bigcap_{j \neq i} Q_j$, una nueva descomposición primaria. Reiterando nuevamente la construcción, llegamos a una descomposición primaria minimal. □

Teorema 5.40 (Lasker-Noether)**.** *Sea* $I = \bigcap_{i=1}^{m} Q_i$ *una descomposición primaria minimal de un ideal propio* I *en un anillo conmutativo Noetheriano* R*. Sea* $P_i = \sqrt{Q_i}$ *para cada* $1 \leq i \leq m$*. Entonces* $\{P_i \mid 1 \leq i \leq m\}$ *son los ideales primos propios que aparecen en el conjunto* $\{\sqrt{I : f} \mid f \in R\}$.

Demostración. Como $I = \bigcap_{i=1}^{m} Q_i$, tenemos que $I : f = \bigcap_{i=1}^{m} (Q_i : f)$. Por tanto

$$\sqrt{I : f} = \bigcap_{i=1}^{m} \sqrt{Q_i : f} = \bigcap_{\substack{i=1 \\ Q_i \not\supseteq f}}^{m} \sqrt{Q_i : f} = \bigcap_{\substack{i=1 \\ Q_i \not\supseteq f}}^{m} P_i$$

(ver ejercicios). Si $\sqrt{I : f}$ es primo propio, entonces $\sqrt{I : f} = P_i$ para algún i por ser los primos irreducibles (ver ejercicios). Por otra parte, si $f \in \bigcap j \neq i Q_j \setminus Q_i$, tenemos que

$$\sqrt{I : f} = \bigcap_{\substack{j=1 \\ Q_j \not\ni f}}^{m} \sqrt{Q_j : f} = \sqrt{Q_i : f} = P_i,$$

lo que demuestra el teorema. □

Ejercicios sobre Variedades Irreducibles y Descomposición

Ejercicio 5.1. Encuentra $f \in \mathbf{I}(\mathbf{V}(I)) \setminus I$, donde $I = \langle x^2+y^2-1, y-1\rangle$.

Ejercicio 5.2. Demuestra que $\mathbf{V}(y-x^2, z-x^3) = \mathbf{V}((y-x^2)^2+(z-x^3)^2) \subseteq \mathbb{R}^3$.

Ejercicio 5.3. ¿Es posible encontrar dos ideales en $\mathbb{R}[x,y]$ que definan la misma variedad tales que ninguno esté incluido en el otro? Responde a la misma pregunta para $\mathbb{R}[x]$.

Ejercicio 5.4. Sea $\mathbb{F}$ un cuerpo.

1. Dado $g = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{F}[x]$ con $a_0 \neq 0$, se define la homogenización de g como

   $$g^h = a_0x^n + a_1x^{n-1}y + \cdots + a_{n-1}xy^{n-1} + a_ny^n$$

   Demuestra que g tiene una raíz en $\mathbb{F}$ si y solo si existe $(a,b) \in \mathbb{F}^2 \setminus \{(0,0)\}$ tal que $g^h(a,b) = 0$.

2. Si $\mathbb{F}$ no es algebraicamente cerrado, demuestra que existe $f \in \mathbb{F}[x,y]$ tal que $\mathbf{V}(f) = \{(0,0)\}$.

3. Si $\mathbb{F}$ no es algebraicamente cerrado, demuestra que para cualquier $l > 0$ existe $f \in \mathbb{F}[x_1,\ldots,x_l]$ tal que $\mathbf{V}(f) = \{(0,\ldots,0)\}$.

4. Si $\mathbb{F}$ no es algebraicamente cerrado y $W = \mathbf{V}(g_1,\ldots,g_s)$ demuestra que existe $h \in \mathbb{F}[X]$ tal que $W = \mathbf{V}(h)$.

Ejercicio 5.5. Demuestra que $I : J^\infty$ es un ideal para cualesquiera ideales I, J en un anillo conmutativo R.

Ejercicio 5.6. Dado I ideal en un anillo conmutativo R,

1. Demuestra que $\sqrt{I}$ es un ideal radical.
2. Demuestra que I es radical si y solo si $\sqrt{I} = I$.
3. Demuestra que $\sqrt{\sqrt{I}} = \sqrt{I}$.

Ejercicio 5.7. Demuestra que un ideal es propio si y solo si su radical también es propio.

Ejercicio 5.8. Si $\sqrt{I} = \langle f_1, f_2 \rangle$ con $f_i^{m_i} \in I$, demuestra que $f^{m_1+m_2-1} \in I$ para cualquier $f \in \sqrt{I}$.

Ejercicio 5.9. Si I es un ideal en un anillo Noetheriano R, demuestra que existe $m \in \mathbb{N}$ tal que $f^m \in I$ para cualquier $f \in \sqrt{I}$.

Ejercicio 5.10. Determina si los siguientes polinomios pertenecen a los radicales indicados. En caso de respuesta afirmativa, encuentra la menor potencia que mete al polinomio en el ideal.

$$¿x + y \in \sqrt{\langle x^3, y^3, xy(x+y) \rangle}?,$$

$$¿x^2 + 3xz \in \sqrt{\langle x + z, x^2y, x - z^2 \rangle}?$$

Ejercicio 5.11. Sea R un DFU. Dados $f, g \in R$, se define (f, g) como el mayor (respecto de la divisibilidad) divisor común de f y g. Demuestra que existe (f, g). Demuestra que $h = (f, g)$ si y solo si $\langle h \rangle$ es el menor ideal principal que contiene a $\langle f, g \rangle$.

Ejercicio 5.12. Si $I = \langle f_1, \ldots, f_s \rangle$, demuestra que $I^{sn} \subseteq \langle f_1^n, \ldots, f_s^n \rangle$.

Ejercicio 5.13. Sean $I, J_1, \ldots, J_r$ ideales en un anillo conmutativo R. Demuestra que

$$I : \left(\sum_{i=1}^{r} J_i\right) = \bigcap_{i=1}^{r} (I : J_i)$$

y

$$I : \left(\sum_{i=1}^{r} J_i\right)^{\infty} = \bigcap_{i=1}^{r} (I : J_i^{\infty}).$$

Ejercicio 5.14. Demuestra que $\left(\bigcap_{i=1}^{m} I_i\right) : F = \bigcap_{i=1}^{m} (I_i : F)$.

Ejercicio 5.15. Sea I un ideal de $\mathbb{F}[x_1, \ldots, x_n]$ y sea $g \in \mathbb{F}[x_1, \ldots, x_n]$. Sea $\tilde{I} = \langle I \rangle + \langle 1 - yg \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n, y]$. Demuestra que

$$I : g^{\infty} = \tilde{I} \cap \mathbb{F}[x_1, \ldots, x_n].$$

Ejercicio 5.16. Sean

$$f = (x + y)^2(x - y)(x + z^2)$$

y

$$g = (x + z^2)^3(x - y)(z + y).$$

Calcula $\langle f \rangle : \langle g \rangle$ considerando los polinomios con coeficientes en $\mathbb{Q}$ y en $\mathbb{Z}_2$.

Ejercicio 5.17. Sean I, J ideales de un anillo conmutativo R. Si I es radical, demuestra que $I : J$ es radical y $I : J = I : \sqrt{J} = I : J^{\infty}$.

Ejercicio 5.18. Sean $V, W \subseteq \mathbb{F}^n$ variedades afines. Demuestra que

$$\mathbf{I}(V) : \mathbf{I}(W) = \mathbf{I}(V \setminus W).$$

Ejercicio 5.19. Demuestra que $I : J^\infty = I : J^N$ si y solo si $I : J^N = I : J^{N+1}$.

Ejercicio 5.20. Demuestra que

1. $IJ \subseteq K$ si y solo si $I \subseteq K : J$,
2. $(I : J) : K = I : (JK)$,

para cualesquiera ideales $I, J, K \subseteq R$.

Ejercicio 5.21. Demuestra que todo ideal primo es radical.

Ejercicio 5.22. Sean $f_1, \ldots, f_n, q_1, \ldots, q_n \in \mathbb{F}[t_1, \ldots, t_r]$, $W = \mathbf{V}(q_1 \cdots q_n)$ y

$$\begin{aligned} \phi : \mathbb{F}^r \setminus W &\to \mathbb{F}^n \\ (a_1, \ldots, a_r) &\mapsto \left(\tfrac{f_1(a_1,\ldots,a_r)}{q_1(a_1,\ldots,a_r)}, \ldots, \tfrac{f_n(a_1,\ldots,a_r)}{q_n(a_1,\ldots,a_r)} \right). \end{aligned}$$

Dado $h \in \mathbb{F}[x_1, \ldots, x_n]$, demuestra que

$$(q_1 \cdots q_n)^N (h \circ \phi) \in \mathbb{F}[t_1, \ldots, t_r],$$

donde N es el grado total de h.

Ejercicio 5.23. Demuestra que

$$\langle x_1 - a_1, \ldots, x_n - a_n \rangle \in \mathbb{F}[x_1, \ldots, x_n]$$

es un ideal maximal para cualesquiera $a_1, \ldots, a_n \in \mathbb{F}$.

Ejercicio 5.24. Demuestra que $\mathbf{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.

Ejercicio 5.25. Demuestra que si I es primario, $\sqrt{I}$ es primo, en cuyo caso $\sqrt{I}$ es el menor ideal primo que contiene a I.

Ejercicio 5.26. Demuestra que en un anillo Noetheriano, todo ideal puede ser descrito como una intersección finita de ideales irreducibles.

Ejercicio 5.27. Demuestra que si $fg \in I$ e $I : g^\infty = I : g^N$, se tiene que $I = (I + \langle g^N \rangle) \cap (I + \langle f \rangle)$.

Ejercicio 5.28. Demuestra que si I, J son ideales primarios tales que $\sqrt{I} = \sqrt{J}$, entonces $I \cap J$ es primario.

Ejercicio 5.29. Si $P \subseteq R$ es ideal primo, demuestra que $f \in P \iff P : f = R$, y $f \notin P \iff P : f = P$.

Ejercicio 5.30. Sea $I \subseteq R$ un ideal primario con $P = \sqrt{I}$, y sea $f \in R$. Demuestra que

1. si $f \in I$, entonces $I : f = R$,
2. si $f \notin I$, entonces $I : f$ es P-primario,
3. si $f \notin P$, entonces $I : f = I$.

Ejercicio 5.31. Si P es un ideal primo tal que $P \supseteq \bigcap_{i=1}^m I_i$, entonces existe i tal que $P \supseteq I_i$. Si $P = \bigcap_{i=1}^m I_i$, demuestra que $P = I_i$ para algún i.

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 $\sigma \in T(E)$. 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 $E = \{\alpha^1, \ldots, \alpha^s\} + \mathbb{N}^n$,

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

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

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

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* $E = \{\alpha^1, \ldots, \alpha^t\} + \mathbb{N}^n$*, 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 $\sigma = \{1, \ldots, n\} \setminus \operatorname{top}_m(\alpha)$. 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 $\operatorname{supp}(\alpha) = \operatorname{top}_m(\alpha) = \{1, \ldots, n\} \setminus \sigma$. Como $\sigma \in T(E)$, para todo $k \in \{1, \ldots, t\}$, $\sigma \cap \operatorname{supp}(\alpha^k) \neq \varnothing$, 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 $\{1, \psi, \ldots, \psi^{n-1}\}$. Por otra parte, $\psi^n \in \langle I \rangle_{R[\psi]}$, 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

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

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

Si $I \neq 0$ *entonces* $\delta < n$*.*

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 $d = \dim(\exp(I))$ y sea r el mayor número de elementos algebraicamente independientes en R/I. Sea $\sigma \in T(\exp(I))$ tal que $d = n - \#\sigma$ y sea $\{x_{i_1}, \ldots, x_{i_d}\} = \{x_i \,;\, i \notin \sigma\}$. Vamos a comprobar que $\{x_{i_1} + I, \ldots, x_{i_d} + I\}$ es un conjunto de elementos algebraicamente independiente. Para ello sea $f \in \mathbb{F}[x_{i_1}, \ldots, x_{i_d}] \cap I$. 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

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

tenemos que $x_{i_1} + I, \ldots, x_{i_d} + I$ son algebraicamente independientes y como consecuencia $d \leq r$.

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 $\dim(\exp(I)) = d \geq r$. □

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 $\psi \in \langle P \rangle_S \cap C$, 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

Definición 6.31. Dada $A = \mathbb{F}[x_1, \ldots, x_n]/J$, se dice que $\mathbb{F}[y_1, \ldots, y_d] \subseteq A$ es una normalización de Noether si $y_1, \ldots, y_d$ son algebraicamente independientes sobre $\mathbb{F}$ y A es finitamente generado sobre $\mathbb{F}[y_1, \ldots, y_d]$.

Teorema 6.32. *Si* $\mathbb{F}[y_1, \ldots, y_d] \subseteq A$ *es una normalización de Noether con* $A = \mathbb{F}[x_1, \ldots, x_n]/J$, *entonces* $\dim(A) = d$.

Demostración. Por la Proposición 6.15 y el Corolario 6.30 tenemos que $\dim(A) = \dim(\mathbb{F}[y_1, \ldots, y_d]) \geq d$, donde la última desigualdad es consecuencia de uno de los ejercicios. Veamos, por inducción en d, que toda cadena de ideales primos

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_m$$

en $\mathbb{F}[y_1, \ldots, y_d]$ satisface $m \leq d$. Si $d = 0$ no hay nada que demostrar. Supongamos que $d > 0$ y que $m > 0$. Por el Lemma 6.22 existe una normalización de Noether $\mathbb{F}[t_1, \ldots, t_d] \subseteq \mathbb{F}[y_1, \ldots, y_d]$ tal que $P_1 \cap \mathbb{F}[t_1, \ldots, t_d] = \langle t_{\delta+1}, \ldots, t_d \rangle$. Como $P_1 \neq 0$, tenemos que $\delta < d$.

Por tanto $\mathbb{F}[t_1, \ldots, t_\delta] \subseteq \mathbb{F}[y_1, \ldots, y_d]/P_1$ es una normalización de Noether. Por hipótesis de inducción, la cadena

$$0 = P_1/P_1 \subsetneq P_2/P_1 \subsetneq \cdots \subsetneq P_m/P_1$$

debe satisfacer que $m - 1 \leq \delta$, por lo que $m \leq \delta + 1 \leq d$, lo que termina la demostración. □

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.