Álgebra Conmutativa Computacional

F. J. Lobillo

2019/2020

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. $A[x_1,\dots,x_n] \cong A[x_1]\cdots[x_n]$.

2.2 Órdenes admisibles

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

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

Por supuesto este orden puede extenderse al orden producto en $\mathbb{N}^n$. El orden producto no es un orden total. Denotemos por $\le_\prod$ 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 $\exp(f) = \max_{\leq}(\operatorname{supp}(f))$,

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

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

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

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* $\operatorname{lc}(f) = -\operatorname{lc}(g)$.

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

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

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

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* $\operatorname{lc}(f)\operatorname{lc}(g) = 0$.

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,

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

Sean $(a_1, \ldots, a_{n-1}) \in \mathbb{F}^{n-1}$. 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 $\varphi_c(a_1,\dots,a_{n-1}) = \varphi(a_1,\dots,a_{n-1},c)$. Por hipótesis de inducción existe un polinomio $f_c \in \mathbb{F}[x_1,\dots,x_{n-1}]$ tal que $\varphi_c(a_1,\dots,a_{n-1}) = f_c(a_1,\dots,a_{n-1})$ para cada $(a_1,\dots,a_{n-1}) \in \mathbb{F}^{n-1}$. Sea

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

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

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

lo que demuestra el resultado. □

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

Proposición 2.18. *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 2.19. 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 2.20. *$\varnothing$ 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 2.21. $\mathbf{V}(F) = \mathbf{V}(\langle F \rangle)$.

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

Tenemos la construcción inversa.

Proposición 2.22. *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 $(a_1, \ldots, a_n) \in A$,

$$\begin{aligned} (gf)(a_1, \ldots, a_n) &= g(a_1, \ldots, a_n) f(a_1, \ldots, a_n) \\ &= g(a_1, \ldots, a_n) 0 = 0, \end{aligned}$$

por lo que $gf \in \mathbf{I}(A)$. □

Definición 2.23. Se define el ideal asociado a $A \subseteq \mathbb{F}^n$ como $\mathbf{I}(A)$.

Proposición 2.24. *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. Si* $F \subseteq \mathbb{F}[x_1, \ldots, x_n]$, $\langle F \rangle \subseteq \mathbf{I}(\mathbf{V}(F))$, *pudiendo ser la inclusión estricta.*

Demostración. Se propone como ejercicio. □

Corolario 2.25. *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 2.26. 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 2.27. $\sim$ *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 2.28. *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 2.29. $((R \times R \setminus \{0\}) / \sim, +, \cdot)$ *es un cuerpo.*

Demostración. Ejercicio. □

Definición 2.30. $(R \times R \setminus \{0\}) / \sim$ 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 2.31. 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

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

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 2.24.

Ejercicio 2.5. Demuestra la Proposición 2.29.

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 $\mathbb{R}^2$

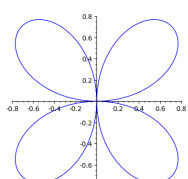
1. $\mathbf{V}(x^2 + 4y^2 + 2x - 16y + 1)$,
2. $\mathbf{V}(x^2 - y^2)$,
3. $\mathbf{V}(2x + y - 1, 3x - y + 2)$.

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.

Bibliografía

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

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