Álgebra Conmutativa Computacional

F. J. Lobillo

2019/2020

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 $A \cap \mathbb{N}^n_l$. $\square$

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 $\alpha \in \mathbb{N}^n_l$ 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 $\exp(f) \in \mathbb{N}^n_l$, al ser el orden de eliminación, $\operatorname{supp}(f) \subseteq \mathbb{N}^n_l$, 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 $\exp(f) \in \mathbb{N}^n_l$. En consecuencia

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

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, $\exp(G) \cap \mathbb{N}^n_l$ genera $\exp(I) \cap \mathbb{N}^n_l$, y dado que

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

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

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

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

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

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

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

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

el morfismo de anillos que evalúa la t en 0 descrito en el Lema 4.7 donde $A = \mathbb{F}[x_1, \dots, x_n]$. Por una parte, $\phi_0(f) = f$ porque $f \in \mathbb{F}[x_1, \dots, x_n]$. 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 $g_1, \dots, g_t \in \mathbb{F}[x_1, \dots, x_n]$, luego $f \in J$. Evaluando en $t = 1$ obtenemos análogamente que $f \in I$, por lo que $f \in I \cap J$ y $H \cap \mathbb{F}[x_1, \dots, x_n] \subseteq I \cap J$. □

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $f_1, \dots, f_n \in \mathbb{F}[t_1, \dots, t_r]$ y sea*

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

Sea $I = \langle x_1 - f_1, \dots, x_n - f_n \rangle \subseteq \mathbb{F}[t_1, \dots, t_r, x_1, \dots, x_n]$ y sea $J = I \cap \mathbb{F}[x_1, \dots, x_n]$ 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 2.25 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 $\operatorname{lt}(x_i - f_i) = x_i$ 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. $\square$

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

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

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

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

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

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

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 2.25 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

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

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

$$q^N h = p_1(q_1 x_1 - f_1) + \dots + p_n(q_n x_n - f_n) + \rho.$$

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

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

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

$$q^N y^N h = p_1 y^N (q_1 x_1 - f_1) + \dots + p_n y^N (q_n x_n - f_n).$$

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 $h \in \langle q_1x_1 - f_1, \ldots, q_nx_n - f_n, 1 - qy\rangle = I$. 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

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

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* $f_1, \dots, f_n \in \mathbb{F}_q[t_1, \dots, t_r]$ *y sea*

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

Sea $I = \langle x_1 - f_1, \dots, x_n - f_n, x_1^q - x_1, \dots, x_n^q - x_n \rangle$*, un ideal en* $\mathbb{F}_q[t_1, \dots, t_r, x_1, \dots, x_n]$*, y sea* $J = I \cap \mathbb{F}_q[x_1, \dots, x_n]$ *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. $\square$

Ejercicios sobre Eliminación e Implicitación

Ejercicio 4.1. Dada la variedad afín definida por las ecuaciones

$$\begin{aligned} x^2 + 2y^2 &= 3 \\ x^2 + xy + y^2 &= 3 \end{aligned}$$

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

$$\begin{aligned} x^2 + y^2 + z^2 &= 4 \\ x^2 + 2y^2 &= 5 \\ xz &= 1 \end{aligned}$$

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

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

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 paramétricamente 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 $W = \mathbf{V}(q_1, \dots, q_n) \subseteq \mathbb{F}$, y

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

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

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 $\mathbb{C}$?.

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.