ECUACIONES POLINOMIALES Y ALGORITMOS

Primer Cuatrimestre 2018– Práctica 6

Resultante, Teorema de extensión y el Nullstellensatz

(**1**) Dados $f = X^5 - 3X^4 - 2X^3 + 3X^2 + 7X + 6$ y $g = X^4 + X^2 + 1$, calcular $\mathrm{Res}\,(f,g)$ y decidir si f, g tienen un factor en común en $\mathbb{Q}[X]$. ¿Y en $\mathbb{Z}[X]$?

(**2**) Sea $f = aX^2 + bX + c = a(X - \alpha)(X - \beta) \in K[X]$ con $a \neq 0$.

- Verificar que el *Discriminante* $\Delta := b^2 - 4ac$ también es igual a $a^2(\alpha - \beta)^2$, y por lo tanto reencontrar "f tiene una raíz doble $\iff \Delta = 0$".
- Justificar la afirmación "$\mathrm{Res}\,(f, f') = 0 \iff \Delta = 0$". Calcular $\mathrm{Res}\,(f, f')$ y comparar con Δ.

(**3**) Sea $f = X^3 + pX + q = (X - \alpha)(X - \beta)(X - \gamma) \in K[X]$.
Se define el *Discriminante* de f (caso f mónico) como $\Delta(f) := (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$, que satisface: $\Delta(f) = 0$ si y sólo si f tiene una raíz múltiple.

- Verificar que $\Delta(f) = -4p^3 - 27q^2$.
- Calcular $\mathrm{Res}\,(f, f')$ y comparar con $\Delta(f)$.

(**4**) Sea $f = a_0X^n + \cdots + a_n = a_0(X - \alpha_1)\ldots(X - \alpha_n) \in K[X]$, con $a_0 \neq 0,\ n \geq 2$.
Se define el *Discriminante* de f (caso general) como:

$$\Delta(f) := a_0^{2n-2}\prod_{i<j}(\alpha_i - \alpha_j)^2.$$

Probar que $\mathrm{Res}\,(f, f') = a_0^{n-1}\prod_i f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} a_0\, \Delta(f)$.
(Sug: Verificar que $f' = a_0 \sum_i (X - \alpha_1)\cdots(X - \alpha_{i-1})(X - \alpha_{i+1})\cdots(X - \alpha_n)$.)

(**5**) Sean $f = 2X^2 + 3X + 1$ y $g = 7X^2 + X + 3$

- Usar el algoritmo de Euclides para calcular $\mathrm{mcd}(f; g)$, y hallar $r, s \in \mathbb{Q}[X]$ tales que $1 = rf + sg$.
- Limpiando denominadores, relacionarlo con $\mathrm{Res}\,(f, g)$.

(**6**) Sean $f = a_nX^n + \cdots + a_0$ y $g = b_mX^m + \cdots + b_0$. En el curso para definir la resultante $\mathrm{Res}\,(f, g)$ como el determinante de la matriz de Sylvester, se supuso que n ó $m \geq 1$ y $a_n \neq 0,\ b_m \neq 0$. Comparar el determinante de la matriz de Sylvester de tamaño $n + m$ con la verdadera resultante cuando $a_n = 0$ (pero $b_m \neq 0$), o sea cuando uno no conoce a priori el grado exacto del polinomio f, pudiendo ser éste incluso constante.
¿Qué pasa si a_n y b_m son cero?

(**7**) Sean $f = XY - 1$ y $g = X^2 + Y^2 - 4$.

- Mirando a f y g en $(\mathbb{Q}[Y])[X]$, calcular $\mathrm{Res}_X(f, g)$.
¿Tienen f y g un factor en común en $\mathbb{Q}[X, Y]$? ¿Y en $(\mathbb{Q}(Y))[X]$?
- ¿Existe un polinomio puro en Y en $\langle f, g\rangle$?
- ¿Existen $r, s \in \mathbb{Q}[X, Y]$ tales que $1 = rf + sg$? ¿ Y en $(\mathbb{Q}(Y))[X]$?
- Describir $\mathbf{V}_{\mathbb{C}}(f, g)$.

(**8**) Sea $I = \langle Y - X^2, Z - X^3\rangle \subset \mathbb{R}[X, Y, Z]$. Verificar que $\mathbf{V}_{\mathbb{R}}(I) = \mathbf{V}_{\mathbb{R}}((Y - X^2)^2 + (Z - X^3)^2)$, y generalizar probando que toda variedad de $\mathbb{R}^n$ puede ser definida por medio de un solo polinomio.

(9) Sea el sistema de ecuaciones dado por:

$$\begin{cases} X^5 & + & 1/X^5 & = & Y \\ X & + & 1/X & = & Y \end{cases}$$

- Determinar un ideal $I \subset \mathbb{C}[X, Y, Z]$ que "ayude" para resolver este sistema, y encontrar sistemas de generadores de los ideales de eliminación $I \cap \mathbb{C}[Y, Z]$ e $I \cap \mathbb{C}[Z]$.
- Aplicar el teorema de extensión para decidir cuáles $c \in \mathbf{V}_{\mathbb{C}}(I \cap \mathbb{C}[Z])$ se extienden a $(a, b, c) \in \mathbf{V}_{\mathbb{C}}(I)$.
- ¿Cuáles soluciones $(b, c) \in \mathbf{V}_{\mathbb{C}}(I \cap \mathbb{C}[Y, Z])$ se extienden a soluciones $(a, b, c) \in \mathbf{V}_{\mathbb{C}}(I)$? ¿Por qué no se contradice el teorema de extensión?
- Resolver completamente el sistema original.

(10) Sean $f = X(Y - Z) + Y - 1$, $g = X(Y - Z) + Z - 1$ e $I = \langle f, g\rangle \subset \mathbb{C}[X, Y, Z]$.

- Hallar a mano todas las soluciones del sistema $\{ f = 0, g = 0 \}$.
- Describir $I_1 = I \cap \mathbb{C}[Y, Z]$. ¿Se extiende todo $(b, c) \in \mathbf{V}_{\mathbb{C}}(I_1)$ a $(a, b, c) \in \mathbf{V}_{\mathbb{C}}(I)$?
- Determinar otros generadores de I donde para todo $(b, c) \in \mathbf{V}_{\mathbb{C}}(I_1)$, existe $a \in \mathbb{C}$ tal que $(a, b, c) \in \mathbf{V}_{\mathbb{C}}(I)$.

(11) El *Paraguas de Whitney* es la superficie $\mathcal{W}$ dada paramétricamente, con parámetros U, V, por:

$$\begin{cases} X & = & UV \\ Y & = & V \\ Z & = & U^2 \end{cases}$$

- Hacerse una idea de lo que representa en $\mathbb{R}^3$. (Si sabe puede usar alguna software para dibujarlo en $\mathbb{R}^3$.)
- Hallar ecuaciones en X, Y, Z tales que la variedad V definida por ellas contenga a $\mathcal{W}$.
- Mostrar que (si eligió bien las ecuaciones), en $\mathbb{C}^3$ se tiene $V_{\mathbb{C}} = \mathcal{W}_{\mathbb{C}}$, pero en $\mathbb{R}^3$, $\mathcal{W}_{\mathbb{R}} \subset V_{\mathbb{R}}$, sin que valga la igualdad. ¿Qué puntos de $V_{\mathbb{R}}$ no pertenecen a $\mathcal{W}_{\mathbb{R}}$?
- Mostrar que los parámetros U, V no están siempre univocamente determinados por X, Y, Z. ¿En qué puntos falla la unicidad y qué tienen que ver con el dibujo?

(12) Sean $f_1 = YX^3 + X^2$, $f_2 = Y^3X^2 + Y^2$ y $f_3 = YX^4 + X^2 + Y^2$, e $I = \langle f_1, f_2, f_3\rangle \subset \mathbb{C}[X, Y]$.

- Hallar $I_1 := I \cap \mathbb{C}[Y]$.
- Si h_i son los coeficientes principales de los generadores f_i de I como polinomios en X, calcular $\mathbf{V}_{\mathbb{C}}(I_1)$ y $\mathbf{V}_{\mathbb{C}}(I_1) \cap \mathbf{V}_{\mathbb{C}}(h_1, h_2, h_3)$ y compararlos.
- Sea $J = \langle f_1, f_2, f_3, h_1, h_2, h_3\rangle$. Probar que $I \neq J$ pero $\mathbf{V}_{\mathbb{C}}(I) = \mathbf{V}_{\mathbb{C}}(J)$ y $\mathbf{V}_{\mathbb{C}}(I_1) = \mathbf{V}_{\mathbb{C}}(J_1)$ donde $J_1 := J \cap \mathbb{C}[Y]$.
- Considerar los polinomios $g_1 = f_1 - h_1X^3$, $g_2 = f_2 - h_2X^2$, $g_3 = f_3 - h_3X^4$, y probar que $J = \langle g_1, g_2, g_3, h_1, h_2, h_3\rangle$. Repetir lo anterior para J_1. ¿Hay algo distinto?
- Verificar que si $I = \langle f_1, \dots, f_s\rangle \subset \mathbb{C}[X_1, \dots, X_n]$, vale siempre:

  $$\mathbf{V}_{\mathbb{C}}(I_1) = \Pi_1(\mathbf{V}_{\mathbb{C}}(I)) \cup (\mathbf{V}_{\mathbb{C}}(h_1, \dots, h_s) \cap \mathbf{V}_{\mathbb{C}}(I_1)),$$

  donde h_i definidos como arriba y $\Pi_1 : \mathbb{C}^2 \to \mathbb{C}, (x, y) \mapsto y$. A veces $\mathbf{V}_{\mathbb{C}}(h_1, \dots, h_s) \cap \mathbf{V}_{\mathbb{C}}(I_1)$ coincide con $\mathbf{V}_{\mathbb{C}}(I_1)$ pero a veces está estrictamente incluído.
  (Se puede probar que en $\mathbb{C}$ siempre se pueden cambiar las ecuaciones que definen $\mathbf{V}_{\mathbb{C}}(I)$ de manera que $\mathbf{V}_{\mathbb{C}}(h_1, \dots, h_s) \cap \mathbf{V}_{\mathbb{C}}(I_1)$ esté estrictamente contenido en $\mathbf{V}_{\mathbb{C}}(I_1)$.)

(13) Sea $I = \langle X^2 + Y^2 + Z^2 + 2, 3X^2 + 4Y^2 + 4Z^2 + 5\rangle \subset K[X, Y, Z]$. Sea $I_1 := I \cap K[Y, Z]$ y $\Pi_1 : K^3 \to K^2,\ (x, y, z) \mapsto (y, z)$.

- Probar que en $\mathbb{C}$ vale: $\mathbf{V}_{\mathbb{C}}(I_1) = \Pi_1(\mathbf{V}_{\mathbb{C}}(I))$

- Calcular en $\mathbb{R}$: $\mathbf{V}_{\mathbb{R}}(I)$ y $\mathbf{V}_{\mathbb{R}}(I_1)$, y mostrar que en $\mathbb{R}$ no hay modo de hallar nuevas ecuaciones para definir $\mathbf{V}_{\mathbb{R}}(I)$ de manera que se cumpla la última afirmación del ejercicio anterior.

(**14**) Sea $I = \langle X^2 + Y^2 + Z^2 - 1, X^2 + Z^2 - Y, X - Z \rangle \subset \mathbb{C}[X, Y, Z]$.

- Describir $\mathbf{V}_{\mathbb{C}}(I)$.
- ¿Es I un ideal radical?

(**15**) **La flor de 4 pétalos**
Esta es la curva de $\mathbb{R}^2$ definida por la ecuación polar $r = \operatorname{sen}(2\theta)$.

- Usando $r^2 = x^2 + y^2$, $x = r\cos(\theta)$ e $y = r\operatorname{sen}(\theta)$, probar que la flor de 4 pétalos está contenida en la variedad $\mathbf{V}_{\mathbb{R}}((X^2 + Y^2)^3 - 4X^2Y^2)$.
- Justificar cuidadosamente que $\mathbf{V}_{\mathbb{R}}((X^2 + Y^2)^3 - 4X^2Y^2)$ está contenido en la flor de 4 pétalos. (Hay que tener cuidado pues r puede ser negativo en $r = \operatorname{sen}(2\theta)$).
- ¿Se anula el polinomio $X^7 - X^6Y + 3X^5Y^2 - 3X^4Y^3 - 3X^2Y^3 + Y^6X - Y^7 - 4X^3Y^2 + 4X^2Y^2$ sobre los puntos de la flor? (Cuidado con la justificación si se usa el teorema de los ceros de Hilbert)

(**16**) ¿Tiene el sistema:

$$\begin{cases} XZ + Y^2Z + 5X^3 + 8Y = 0 \\ XY - 2X^2 + 3Y^5 - Z^2 = 0 \\ Z^3 + X^3 + Y^4 - XYZ = 0 \end{cases}$$

soluciones comunes en $\mathbb{C}^3$?
Si las tiene, ¿cuántas? ¿finitas o infinitas? ¿cómo describirlas?

(**17**) Probar que en $\mathbb{R}$, $\mathbf{V}_{\mathbb{R}}(X^2 + Y^2)$ es finito y sin embargo, $\langle X^2 + Y^2 \rangle \cap \mathbb{R}[X] = (0)$ y $\langle X^2 + Y^2 \rangle \cap \mathbb{R}[Y] = (0)$. ¿Dónde falla el razonamiento hecho para $\mathbb{C}$?