

# ECUACIONES POLINOMIALES Y ALGORITMOS

SEGUNDO CUATRIMESTRE 2011– PRÁCTICA 2

## Ideales, Ordenes monomiales y Algoritmo de División en $K[X_1, \dots, X_n] =: K[\mathbf{X}]$

### (1) Ordenes con pesos independientes

- (a) Probar que el orden en  $K[X, Y]$  definido por  $X^\alpha Y^\beta < X^{\alpha'} Y^{\beta'} \iff \alpha + \pi\beta < \alpha' + \pi\beta'$  es un orden monomial (donde  $\pi = 3.14\dots$ ). Ordenar según este orden todos los monomios de grado  $\leq 4$ .
- (b) En general, sea  $u := (u_1, \dots, u_n)$  un vector de  $\mathbb{R}^n$  tq  $u_1, \dots, u_n$  son positivos y linealmente independientes sobre  $\mathbb{Q}$ . Se define en  $K[\mathbf{X}]$  el orden  $<_u$  siguiente :

$$\mathbf{X}^\alpha <_u \mathbf{X}^\beta \iff u \cdot \alpha < u \cdot \beta$$

(donde  $\cdot$  denota el producto escalar común de vectores).

- (c) Mostrar que  $<_u$  es un orden monomial (que se llama orden con pesos independientes).  
 $\dot{\iota}$  Dónde se usa la independencia lineal de los  $u_i$ ?
- (d) Mostrar que  $u = (1, \sqrt{2}, \sqrt{3})$  da un orden con pesos independientes en  $K[X, Y, Z]$ .

### (2) Sea $I = \langle X^6, X^2Y^3, XY^7 \rangle \subset K[X, Y]$ .

- Dibujar en el plano el conjunto de vectores  $(m, n)$  que son exponentes de monomios  $X^m Y^n$  que aparecen en los elementos de  $I$ .
- Si se aplica el algoritmo de división para  $f \in K[X, Y]$ , independientemente del orden monomial usado,  $\dot{\iota}$  qué monomios pueden aparecer en el resto ?

### (3) Sean $u = (1, 1, 0, 0), v = (0, 0, 1, 1, 1)$ y definamos el siguiente orden $<_{2,3}$ en $K[X_1, X_2, X_3, X_4, X_5]$ .

Denotemos por  $<_3$  el orden graduado reverso lexicográfico en  $K[X_3, X_4, X_5]$ . Decimos que  $X^\beta <_{2,3} X^\alpha$  si  $\langle u, \alpha \rangle > \langle u, \beta \rangle$ , o en caso en que  $\langle u, \alpha \rangle = \langle u, \beta \rangle$ , vale que  $\alpha_1 > \beta_1$ ; si además vale que  $\alpha_1 > \beta_1$  entonces  $\langle v, \alpha \rangle > \langle v, \beta \rangle$ ; si resulta que  $\langle v, \alpha \rangle = \langle v, \beta \rangle$ , entonces vale que  $X_3^{\alpha_3} X_4^{\alpha_4} X_5^{\alpha_5} <_3 X_3^{\beta_3} X_4^{\beta_4} X_5^{\beta_5}$ .

- (a) Probar que  $<_{2,3}$  es un orden monomial
- (b) Probar que si  $\alpha$  es cualquier exponente no nulo con  $\alpha_3 = \alpha_4 = \alpha_5 = 0$  y  $\beta$  es cualquier exponente que verifica que  $\beta_1 = \beta_2 = 0$ , entonces  $\beta <_{2,3} \alpha$ .
- (c) Ordenar con este orden todos los monomios en  $K[X_1, X_2, X_3, X_4, X_5]$  de grado menor o igual que 2.

### (4) Sean $f = X^7 + X^3Y^2 - Y + 1$ y $F = (XY^2 - X, X - Y^3)$ .

- Calcular el resto y los cocientes de la división del polinomio  $f$  por el conjunto ordenado  $F$  para el orden lexicográfico  $X > Y$  y para el orden graduado lexicográfico (también llamado diagonal o deglex) con  $X > Y$ .
- Repetir permutando los elementos del conjunto  $F$ .  $\dot{\iota}$  Qué se observa ?

### (5) Sean $f = X^3 - X^2Y - X^2Z + X, f_1 = X^2Y - Z$ y $f_2 = XY - 1$ .

- Usando el orden graduado lexicográfico con  $X > Y > Z$  calcular :
  - el resto  $r_1$  de  $f$  por  $(f_1, f_2)$ .
  - el resto  $r_2$  de  $f$  por  $(f_2, f_1)$ .
- Sea  $r := r_1 - r_2$ .  $\dot{\iota}$  Pertenece  $r$  al ideal  $\langle f_1, f_2 \rangle \subset \mathbb{Q}[X, Y, Z]$ ? En caso afirmativo, hallar  $a_1, a_2 \in \mathbb{Q}[X, Y, Z]$  tales que  $r = a_1 f_1 + a_2 f_2$ .

- Explicitar (sin hacer cuentas) los cocientes y el resto de la división de  $r$  por  $(f_1, f_2)$ .
- (6) Sean  $f_1 = X$ ,  $f_2 = Y - X$  y  $f_3 = 1 - YZ$  y  $I = \langle f_1, f_2, f_3 \rangle$ .
- Probar que  $\{(x, y, z) \in \mathbb{C}^3 \text{ tal que } f(x, y, z) = 0 \forall f \in I\}$  es vacío.
  - Probar que para cualquier orden monomial que se considere y para cualquier orden de los polinomios  $f_1, f_2, f_3$ , el resto de la división del polinomio 1 por los generadores de  $I$  es no nulo.
  - Mostrar que sin embargo  $1 \in I$  exhibiendo  $a_1, a_2, a_3$  tales que  $1 = a_1f_1 + a_2f_2 + a_3f_3$ .
- (7) Sea  $I = \langle Y - X^2, Z - X^3 \rangle \subset \mathbb{C}[X, Y, Z]$
- Mostrar que todo  $f \in \mathbb{C}[X, Y, Z]$  puede escribirse en la forma :
 
$$f = a_1(X, Y, Z)(Y - X^2) + a_2(X, Y, Z)(Z - X^3) + r(X)$$
 donde  $r(X) \in \mathbb{C}[X]$  es un polinomio puro en  $X$ .
    - ¿ Corresponde esto a efectuar la división de Hironaka para alg'ún orden adecuado ?
    - Mostrar que en este caso  $f \in I$  si y solo si  $r = 0$ . ¿ Qué hay de diferente aquí que en el caso de los dos ejercicios anteriores ?
- (8) Justificar (sin hacer cuentas) por qué los polinomios dados en los ejercicios (4), (5), y (6) no son una base de Gröbner del ideal que generan para los órdenes considerados, mientras que los del ejercicio 11 sí lo son para el orden lexicográfico  $X < Y < Z$ . ¿ Y para un orden diagonal ?
- (9) Sea  $I \subset K[\mathbf{X}]$  un ideal y  $G$  una base de Gröbner de  $I$  para  $<$ , y sean  $f, g \in K[\mathbf{X}]$ . Se nota por  $r_G(f)$  el resto de dividir a  $f$  por la base de Gröbner  $G$  para algún algoritmo de división fijo.
- Probar que  $r_G(f) = r_G(g) \iff f - g \in I$ .
  - Deducir que  $r_G(f + g) = r_G(f) + r_G(g)$  y que  $r_G(fg) = r_G(r_G(f)r_G(g))$ .
- (10) Sean  $G$  y  $G'$  dos bases de Gröbner de un ideal  $I \subset K[\mathbf{X}]$  para un orden monomial fijado. Mostrar que si  $f \in K[\mathbf{X}]$ , entonces  $r_G(f) = r_{G'}(f)$ . Es decir, una vez fijado el orden monomial, el resto es independiente de la base de Gröbner considerada.
- (11) Mostrar que un conjunto finito de generadores de un ideal monomial es siempre una base de Gröbner del ideal.
- (12) Sean  $f_1, \dots, f_s \in K[X]$  (una variable, es decir  $n = 1$ ). Determinar una base de Gröbner de  $\langle f_1, \dots, f_s \rangle$ .
- (13) Sea  $I \subset K[\mathbf{X}]$  un ideal principal. Mostrar que cualquier subconjunto finito de  $I$  que contenga un generador de  $I$  es una base de Gröbner de  $I$ .
- (14) Sea  $A \in \mathbb{R}^{4 \times 7}$  la siguiente matriz :
- $$A = \begin{bmatrix} 1 & 2 & 3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$
- Sea  $I \subset \mathbb{R}[X_1, X_2, \dots, X_7]$  el ideal generado por las formas lineales  $\{f_1, f_2, f_3, f_4\}$  que se deducen de las filas de  $A$  (es decir,  $f_i = a_{i1}X_1 + \dots + a_{i7}X_7$  ( $1 \leq i \leq 7$ ) si  $A = (a_{ij})$ ). Probar que  $\{f_1, f_2, f_3, f_4\}$  es una base de Gröbner de  $I$  para algún orden monomial.

- Generalizar a matrices  $A \in \mathbb{R}^{n \times m}$  en forma triangulada.
  - ¿Cuál es el proceso de triangulación que corresponde a producir una base de Gröbner reducida (para el orden lexicográfico puro  $X_1 > \cdots > X_n$ ) del ideal de  $K[\mathbf{X}]$  generado por los polinomios lineales determinados por las filas de  $A$  ?
- (15) ¿ Es  $G = \{X^4Y^2 - Z^5, X^3Y^3 - 1, X^2Y^4 - 2Z\}$  una base de Gröbner del ideal que genera con respecto al orden diagonal con  $X > Y > Z$  ?