ECUACIONES POLINOMIALES Y ALGORITMOS

Práctica 5 $*$ 1er. Cuatrimestre 2002

Bases de Gröbner y primeras aplicaciones

1.– Justificar por qué los polinomios dados en los ejercicios 8, 9 y 10 de la Práctica 4 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 ?

2.– Probar que si $G = \{g_1, \ldots, g_t\}$, $g_i \in \mathbb{K}[X_1, \ldots, X_n]$ es una base de Gröbner (para un orden monomial fijo $<$) del ideal que genera, entonces el resto de la división de $f \in \mathbb{K}[X_1, \ldots, X_n]$ por los polinomios de G es independiente del ordenamiento de los polinomios g_i.

3.– Sea $I \subset \mathbb{K}[X_1, \ldots, X_n]$ un ideal y G una base de Gröbner de I para $<$, y sean $f, g \in \mathbb{K}[X_1, \ldots, X_n]$.
(i) Probar que $r_G(f) = r_G(g) \iff f - g \in I$.
(ii) Deducir que $r_G(f + g) = r_G(f) + r_G(g)$ y que $r_G(fg) = r_G(r_G(f)r_G(g))$.

4.– Sean G y G' dos bases de Gröbner de un ideal $I \subset \mathbb{K}[X_1, \ldots, X_n]$ para un orden monomial fijado. Mostrar que si $f \in \mathbb{K}[X_1, \ldots, X_n]$, entonces $r_G(f) = r_{G'}(f)$ (donde $r_G(f)$ nota el resto de dividir a f por la base de Gröbner G). Es decir, una vez fijado el orden monomial, el resto es independiente de la base de Gröbner considerada.

5.– Mostrar que un conjunto finito de generadores de un ideal monomial es siempre una base de Gröbner del ideal.

6.– Sean $f_1, \ldots, f_s \in \mathbb{K}[X]$ (una variable). Determinar una base de Gröbner de $< f_1, \ldots, f_s >$.

7.– Sea $I \subset \mathbb{K}[X_1, \ldots, X_n]$ un ideal principal (i.e $I =< f >$ para algún polinomio f). Mostrar que cualquier subconjunto finito de I que contenga un generador de I es una base de Gröbner de I.

8.– Sea $A \in \mathbb{R}^{4\times 7}$ la siguiente matriz :

$$A = \begin{pmatrix} 1 & 2 & 3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(i) Sea $I \subset \mathbb{R}[X_1, X_2, \ldots, X_7]$ 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, $f_i = a_{i1}X_1 + \cdots + a_{i7}X_7$ $(1 \leq i \leq 7)$ 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.
(ii) Generalizar a matrices $A \in \mathbb{R}^{n\times m}$ en forma triangulada.

9.– Sea $A = (a_{ij}) \in \mathbb{K}^{s\times n}$ una matriz, y sean $f_i = a_{i1}X_1 + \cdots + a_{in}X_n$ los polinomios lineales de $\mathbb{K}[X_1, \ldots, X_n]$ determinados por las filas de A. Sea $B = (b_{ij})$ la matriz triangular reducida que se obtiene a partir de A por triangulación de Gauss-Jordan, donde además los primeros elementos no nulos de cada fila son iguales a 1. Mostrar que los polinomios lineales que se deducen de las filas no nulas de B forman una base de Gröbner de $< f_1, \ldots, f_s >$ para el orden lexicográfico $X_1 > X_2 > \cdots > X_n$.

10.– Sea $I =< X + Z, Y - Z >\subset \mathbb{C}[X, Y, Z]$.
(i) Probar que los generadores dados son una base de Gröbner de I para el orden lexicográfico $X > Y > Z$.

(ii) Dividiendo XY por los generadores, ordenados de las dos maneras posibles, mostrar que si bien el resto es el mismo (como tiene que ser), los cocientes no lo son.

En lo que sigue $S(f,g)$ denota el polinomio de menor grado que se obtiene cancelando los término de cabeza de f y g, es decir

$$S(f,g) = \frac{[M(f) : M(g)]}{L(f)} f - \frac{[M(f) : M(g)]}{L(g)} g$$

(donde $[\,:\,]$ nota el mínimo común múltiplo.)

11.– ¿ 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 $X > Y > Z$?

12.– ¿ Depende $S(f,g)$ del orden monomial que se considera ? Ejemplificar.

13.– Sean $f, g \in \mathbb{K}[X_1, \ldots, X_n]$, y X^α, X^β monomios. Hallar un monomio X^γ tal que $S(X^\alpha f, X^\beta g) = X^\gamma S(f,g)$.

14.– Sean $f, g \in \mathbb{K}[X_1, \ldots, X_n]$ y $<$ un orden monomial dado tales que $M(f)$ y $M(g)$ son coprimos.
(i) Probar que $M(S(f,g))$ es o bien un múltiplo de $M(f)$ o bien un múltiplo de $M(g)$.
(ii) Probar que existen $p, q \in \mathbb{K}[X_1, \ldots, X_n]$ tales que $S(f,g) = p\,f + q\,g$ con $M(S(f,g)) = \max\{\, M(p\,f), M(q\,g)\,\}$.
(iii) Concluir que $\{\, f, g\,\}$ forman una base de Gröbner del ideal que generan para $<$, y, más aún, que si $f_1, \ldots, f_s \in \mathbb{K}[X_1, \ldots, X_n]$ son tales que sus monomios de cabeza son coprimos dos a dos, entonces son una base de Gröbner del ideal que generan para $<$.

15.– Hallar bases de Gröbner y bases de Gröbner reducidas para los órdenes lexicográfico puro $X > Y$ y diagonal con $X > Y$ de los siguientes ideales de $\mathbb{K}[X,Y]$:

$$I =< X^2Y - 1, XY^2 - X > \quad \text{y} \quad J =< X^2 + Y, X^4 + 2X^2Y + Y^3 + 3 >$$

y deducir si se puede alguna característica de $V(I)$ ó $V(J)$.

16.– Sean $f, g \in \mathbb{K}[X]$ (una variable). Determinar la base de Gröbner reducida de $< f, g >$.

17.– Determinar si $XY^3 - Z^2 + Y^5 - Z^3 \in < -X^3 + Y, X^2Y - Z >$ y si $X^3Z - 2Y^2 \in < XZ - Y, XY + 2Z^2, Y - Z >$.

18.– Usando órdenes lexicográficos puros, determinar exactamente los puntos complejos de las variedades $V(X^2+Y^2+Z^2-1, X^2+Y^2+Z^2-2X, 2X-3Y-Z)$ y $V(X^2Y-Z^3, 2XY-4Z-1, Z-Y^2, X^3-4YZ)$.

19.– Sea $I =< X^{n+1} - YZ^{n+1}W, XY^{n-1} - Z^n, X^nZ - Y^nW > \subset \mathbb{C}[X,Y,Z,W]$ y el orden monomial "grevlex" (orden graduado lexicográfico reverso) con $X > Y > Z > W$. Un matemático italiano, T.Mora, mostró alrededor de 1980 que la base de Gröbner reducida de I contiene al polinomio $Z^{n^2+1} - Y^{n^2}W$. Mostrar que es cierto para $n = 3, 4$ y 5.

20.– Calcular usando el orden lexicográfico puro y el orden "grevlex" con $X > Y > Z$ bases de Gröbner de los ideales $< X^5 + Y^4 + Z^3 - 1, X^3 + Y^2 + Z^2 - 1 >$, $< X^5 + Y^4 + Z^3 - 1, X^3 + Y^3 + Z^2 - 1 >$, y comparar los tamaños.
¿ Qué se observa ? ¿ Pudo la máquina terminar todas los cómputos para "lex" ?

21.– Comprobar que para el ideal del ejercicio 18 con $n = 3$, se obtiene la misma base de Gröbner usando el orden lexicográfico puro y el "grevlex".
La experiencia muestra que si bien el orden "grevlex" no siempre funciona mejor que el "lex", en general es una buena idea usar el primero cuando sirve para lo que uno quiere.

22.– Calcular la base de Gröbner reducida de los ideales $< X^3, Y^3 - X, Z^3 - Y, 1 - ZW^2 >$ y $< X^3, Y^3 - X, Z^3 - Y, W^3 - Z, 1 - WT^2 >$ para algún orden. ¿ Tardó mucho ?

23.– Considerar el ideal $I =< X_1^2 - X_1, \ldots, X_n^2 - X_n, Y - X_1 - \cdots - X_n > \in \mathbb{C}[X_1, \ldots, X_n, Y]$.

(i) Describir $V(I)$ y la proyección de $V(I)$ sobre el eje Y, es decir el conjunto :

$$\pi(V(I)) = \{\, y \in \mathbb{C} : \exists\, x_1, \ldots, x_n \in \mathbb{C} \text{ tq } (x_1, \ldots, x_n, y) \in V(I) \,\}.$$

Determinar un polinomio puro en Y que se anula en los puntos de $\pi(V(I))$. ¿ Qué grado tiene ?

(ii) Los generadores de I son una base de Gröbner de I para el orden lexicográfico $Y > X_1 > \cdots > X_n$ (¿ Por qué ?) pero no para el orden lexicográfico $X_1 > \cdots > X_n > Y$. Calcular una base de Gröbner de I para este último orden para $n = 3$, $n = 4$, $n = 5$, $n = 6$, ... ¿ Se obtiene algún polinomio puro en Y en la base de Gröbner ? ¿ Qué tiene que ver con $\pi(V(I))$?

(iii) ¿ Se observa alguna dificultad a medida que va creciendo n ?

24.– Considerar el ideal $I =< X_1^2 - X_1, \ldots, X_n^2 - X_n, Y - X_1 - 2X_2 - \cdots - 2^{n-1}X_n > \in \mathbb{C}[X_1, \ldots, X_n, Y]$.

(i) Describir $V(I)$ y la proyección de $V(I)$ sobre el eje Y, es decir el conjunto :

$$\pi(V(I)) = \{\, y \in \mathbb{C} : \exists\, x_1, \ldots, x_n \in \mathbb{C} \text{ tq } (x_1, \ldots, x_n, y) \in V(I) \,\}.$$

Determinar un polinomio puro en Y que se anula en los puntos de $\pi(V(I))$. ¿ Qué grado tiene ?

(ii) Los generadores de I son una base de Gröbner de I para el orden lexicográfico $Y > X_1 > \cdots > X_n$ (¿ Por qué ?) pero no para el orden lexicográfico $X_1 > \cdots > X_n > Y$. Calcular una base de Gröbner de I para este último orden para $n = 3$, $n = 4$, $n = 5$, $n = 6$, ... ¿ Se obtiene algún polinomio puro en Y en la base de Gröbner ? ¿ Qué tiene que ver con $\pi(V(I))$?

(iii) ¿ Se observa alguna dificultad a medida que va creciendo n ?