ECUACIONES POLINOMIALES Y ALGORITMOS

Práctica 4 $*$ 2do. Cuatrimestre 2004

Ordenes monomiales y Algoritmo de División en $\mathbf{K}[X_1,\dots,X_n]$

1.– Una base $\{X^\alpha,\ \alpha \in A \subset \mathbb{N}_0{}^n\}$ de un ideal monomial I se llama *minimal* si para todo $X^\alpha, X^\beta \in A,\ X^\alpha \mid X^\beta \Longrightarrow \alpha = \beta$.
Mostrar que todo ideal monomial tiene una base minimal, y que ésta es única.

2.– Sean $f, g \in \mathbf{K}[X_1,\dots,X_n]$ polinomios no nulos, y $<$ un orden monomial fijado. $M(f)$ nota el monomio de cabeza de f para el orden $<$. Mostrar que :
(i) $M(fg) = M(f)M(g)$
(ii) Si $f + g \neq 0$, entonces $M(f+g) \le \max\{M(f), M(g)\}$
(iii) Si $M(f) \neq M(g)$, entonces $M(f+g) = \max\{M(f), M(g)\}$
(iv) Dar ejemplos donde $M(f+g) < \max\{M(f), M(g)\}$
(v) Sean $f_1, f_2, g_1, g_2 \in \mathbf{K}[X_1,\dots,X_n]$. ¿ Vale necesariamente que $M(f_1g_1 + f_2g_2)$ es igual a $M(f_1g_1)$ ó a $M(f_2g_2)$?

3.– Probar que el orden en $\mathbf{K}[X,Y]$ definido por $X^\alpha Y^\beta < X^{\alpha'} Y^{\beta'} \iff \alpha + \pi\beta < \alpha' + \pi\beta'$ es un orden monomial (donde $\pi = 3.14...$). Ordenar según este orden todos los monomios de grado ≤ 4.

4.– Ordenes Producto
Sean $<_1$ y $<_2$ ordenes monomiales en $\mathbf{K}[X_1,\dots,X_n]$ y $\mathbf{K}[Y_1,\dots,Y_m]$ respectivamente. Si representamos por $X^\alpha Y^\beta$ los monomios de $\mathbf{K}[X_1,\dots,X_n,Y_1,\dots,Y_m]$, se define en $\mathbf{K}[X_1,\dots,X_n,Y_1,\dots,Y_m]$ el siguiente orden $<$:

$$X^\alpha Y^\beta < X^{\alpha'} Y^{\beta'} \quad \Longleftrightarrow \quad X^\alpha < X^{\alpha'} \quad \text{ó} \quad X^\alpha = X^{\alpha'} \text{ e } \ Y^\beta < Y^{\beta'}$$

Probar que $<$ es un orden monomial (se llama orden producto y tiene importantes aplicaciones).

5.– Ordenes con pesos
Sean $<$ un orden monomial en $\mathbf{K}[X_1,\dots,X_n]$ y $u := (u_1,\dots,u_n) \in \mathbb{Z}^n_{\ge 0}$. Se define en $\mathbf{K}[X_1,\dots,X_n]$ el orden $<_u$ siguiente :

$$X^\alpha <_u X^\beta \quad \Longleftrightarrow \quad u\cdot\alpha < u\cdot\beta \quad \text{ó} \quad u\cdot\alpha = u\cdot\beta \ \text{ y } \ X^\alpha < X^\beta$$

(donde $\cdot$ denota el producto escalar común de vectores).
(i) Mostrar que $<_u$ es un orden monomial (que se llama el orden con peso determinado por u y $<$).
(ii) Determinar el peso u de manera de obtener como $<_u$ el orden lexicográfico graduado a partir del orden lexicográfico puro $<$.

6.– Ordenes con pesos independientes
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 $\mathbf{K}[X_1,\dots,X_n]$ el orden $<_u$ siguiente :

$$X^\alpha <_u X^\beta \quad \Longleftrightarrow \quad u\cdot\alpha < u\cdot\beta$$

(donde $\cdot$ denota el producto escalar común de vectores).
Mostrar que $<_u$ es un orden monomial (que se llama orden con pesos independientes). ¿ Dónde se usa la independencia lineal de los u_i?
Mostrar que $u = (1,\sqrt{2})$ y $u = (1,\sqrt{2},\sqrt{3})$ dan dos ordenes con pesos independientes en $\mathbf{K}[X,Y]$ y $\mathbf{K}[X,Y,Z]$ respectivamente.

7.– Sea $I = < X^6, X^2Y^3, XY^7 > \subset \mathbf{K}[X,Y]$.

(i) Dibujar en el plano el conjunto de vectores (m,n) que son exponentes de monomios X^mY^n que aparecen en los elementos de I.

(ii) Si se aplica el algoritmo de división para $f \in \mathbf{K}[X,Y]$, independientemente del orden monomial usado, ¿ qué monomios pueden aparecen en el resto ?

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

(i) 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 diagonal ("deglex") con $X > Y$.

(ii) Repetir inversando los elementos del conjunto F.

9.– Sean $f = X^3 - X^2Y - X^2Z + X$, $f_1 = X^2Y - Z$ y $f_2 = XY - 1$.

(i) Usando el orden diagonal 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).
(¿ En qué etapa aparece la diferencia entre los dos restos ?)

(ii) Sea $r := r_1 - r_2$. ¿ Pertenece r al ideal $< f_1, f_2 > \subset \mathbb{Q}[X,Y,Z]$? En caso afirmativo, hallar $a_1, a_2 \in \mathbb{Q}[X,Y,Z]$ tales que $r = a_1f_1 + a_2f_2$.

(iii) Calcular los cocientes y el resto de la división de f por (f_1, f_2). ¿ Se podía esperar ese resultado ?

(iv) Exhibir otro polinomio $g \in < f_1, f_2 >$ tal que su división por (f_1, f_2) da un resto no nulo.

(v) ¿ Resuelve el algoritmo de división el problema de la pertenencia de un polinomio f al ideal $< f_1, f_2 >$?

10.– Sean $f_1 = X$, $f_2 = Y - X$ y $f_3 = 1 - YZ$ y $I = < f_1, f_2, f_3 >$.

(i) Probar que $V(I) := \{ (x,y,z) \in \mathbb{C}^3 \text{ tq } f(x,y,z) = 0 \ \forall f \in I \}$ es vacío.

(ii) 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.

(iii) Mostrar que sin embargo $1 \in I$ exhibiendo a_1, a_2, a_3 tales que $1 = a_1f_1 + a_2f_2 + a_3f_3$.

11.– Sea $I = < Y - X^2, Z - X^3 > \subset \mathbb{C}[X,Y,Z]$

(i) 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 (elegir para ello un orden conveniente y aplicar el algoritmo de división).

(ii) Mostrar que en este caso $f \in I$ si y solo si el resto hallado para el orden de (i) es nulo. ¿ Qué hay de diferente aquí que en el caso de los dos ejercicios anteriores ?