ECUACIONES POLINOMIALES Y ALGORITMOS 2 - 2003

Práctica 0 (Para alumnos que no cursaron ECPyA I)

1.

(i) Probar que $\mathbb{K}[X_1,\ldots,X_n]$ tiene una estructura de $\mathbb{K}-$ espacio vectorial y exhibir una base.

(ii) Un polinomio de grado d en 1 variable tiene a lo sumo $d+1$ coeficientes no nulos, o monomios. ¿ Cuántos coeficientes puede tener un polinomio de grado d en 2 variables ?

(iii) ¿ Cuántos coeficientes no nulos puede tener un polinomio homogéneo de grado d en n variables ?

(iv) ¿ Cuántos coeficientes no nulos puede tener un polinomio cualquiera de grado d en n variables ?

(v) ¿ Cuál es la dimensión de $\mathbb{K}[X_1,\ldots,X_n]_{\leq d} = \{\, f \in \mathbb{K}[X_1,\ldots,X_n]$ tal que $f=0$ ó $\operatorname{gr} f \leq d\}$ como $\mathbb{K}-$espacio vectorial?

(v) Probar que para todo $d,\, n \in \mathbb{N}$, $\binom{d+n}{n} \leq e\, d^n$ y si $d,\, n \geq 3$, $\binom{d+n}{n} \leq d^n$.

(vi) Buscar la fórmula de Stirling y deducir que $\binom{d+n}{n}$ se comporta asintóticamente como d^n. En consecuencia, no existe ningún polinomio $p(d,n)$ tal que $\binom{d+n}{n} \leq p(d,n),\ \forall\ d,n \in \mathbb{N}$.

2.

(i) Probar que el ideal $< X > \subset \mathbb{K}[X]$ es un $\mathbb{K}-$subespacio vectorial de $\mathbb{K}[X]$ de dimensión infinita.

(ii) Sean $f_1, f_2 \in \mathbb{K}[X_1,\ldots,X_n]$ cualesquiera. Probar que existen infinitos pares de polinomios $g_1, g_2 \in \mathbb{K}[X_1,\ldots,X_n]$ tales que $g_1 f_1 + g_2 f_2 = 0$.

(iii) Sea $I = < f_1,\ldots,f_s > \subset \mathbb{K}[X_1,\ldots,X_n]$ y $f \in I$. Probar que existen infinitas maneras de escribir $f = h_1 f_1 + \ldots + h_s f_s$ con $h_1,\ldots,h_s \in \mathbb{K}[X_1,\ldots,X_n]$.

(iv) Sea $I \subset \mathbb{K}[x_1,x_2,\ldots,x_n]$ un ideal. Probar que $rad(I) := \{f \in \mathbb{K}[x_1,x_2,\ldots,x_n] : \text{existe}\, N \in \mathbb{N}\, \text{tal que}\, f^N \in I\}$ es también un ideal (llamado el *radical* de I).

3.

(i) Supongamos $n=1$ y sean $f_1,\ldots,f_r \in K[x]$. Denotemos por f el máximo común divisor mónico de $f_1,\ldots,f_r$. Probar que $< f_1,\ldots,f_r > = < f >$.

(ii) Para todo n, vale que $\mathbb{K}[x_1,x_2,\ldots,x_n]$ es un *domino de factorización única* y sigue existiendo máximo común divisor (definido salvo constante) de dos polinomios dados. Dar un ejemplo de f_1, f_2 en dos variables cuyo máximo común divisor sea 1 (que sean coprimos) pero tales que f_1 y f_2 tengan ceros comunes.

(iii) Mostrar que si $n > 1$, entonces $\mathbb{K}[x_1,x_2,\ldots,x_n]$ no todo ideal se puede generar con un solo elemento.

4.

El objetivo de este ejercicio es demostrar que todas las curvas con parametrizaciones polinomiales $(f(t),g(t)) \subset \mathbb{K}^2$ están contenidas en variedades algebraicas propias:

(i) Mostrar que si $f,g \in \mathbb{K}[t]$ son polinomios de grado menor o igual que n, entonces para todo $m \in \mathbb{N}$ suficientemente grande, el conjunto de polinomios $\{f(t)^e.g(t)^{e'}, e \geq 0, e' \geq 0, e+e' \leq m\}$ es linealmente dependiente en $\mathbb{K}[t]$.

(ii) Deducir que si $C = \{(f(t),g(t)), t \in \mathbb{K}\}$ es una parametrización polinomial de la curva, entonces existe $f \in \mathbb{K}[x,y], f \neq 0$, tal que $C \subset V(f)$.

(iii) Lo anterior se puede generalizar fácilmente a cualquier curva $C \subset \mathbb{K}^3$ con parametrización polinomial. Por ejemplo, encontrar $f \in \mathbb{K}[x,y,z]$ no nulo tal que $V := \{(t^5,t^2,t^3) : t \in \mathbb{K}\} \subset V(f)$. Más aún, probar que V es una variedad afín, es decir, describir V como los ceros comunes de un conjunto finito de polinomios.

5.

(i) Probar que si un polinomio $f \in \mathbb{C}[X_1,\ldots,X_n]$ se anula sobre todos los puntos de $\mathbb{Z}^n$ (los puntos a coordenadas enteras), entonces f es el polinomio nulo.

(ii) Probar que pasa lo mismo si f se anula en el conjunto :

$$\{\, (x_1,\ldots,x_n) \in \mathbb{Z}^n \ \text{ tq } \ 0 \leq x_i \leq \operatorname{gr} f,\ 1 \leq i \leq n \,\}$$

(iii) ¿ Es $\mathbb{Z}^n$ una subvariedad algebraica de $\mathbb{C}^n$?

6. Probar las siguientes igualdades de ideales en $\mathbb{Q}[X,Y]$:
(i) $< X+Y, X-Y > = < X, Y >$
(ii) $< aX+bY, cX+dY > = < X, Y >$ si $ad-bc \neq 0,\ a,b,c,d \in \mathbb{Q}$
(iii) $< X+XY, Y+XY, X^2, Y^2 > = < X, Y >$
(iv) $< 2X^2+3Y^2-11, X^2-Y^2-3 > = < X^2-4, Y^2-1 >$

7. Probar que el orden en $\mathbb{K}[X,Y]$ 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.

8. Sean $f = X^3 - X^2Y - X^2Z + X$, $f_1 = X^2Y - Z$ y $f_2 = XY - 1$.
(i) Usando el orden deglex 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 $r = a_1 f_1 + a_2 f_2$.
(iii) Calcular los cocientes y el resto de la división de r por (f_1, f_2). ¿ Se podía esperar ese resultado ?
(iv) Probar que $g_1 = Y*Z-1, g_2 = X-Z$ es una base de Groebner de $I = < f_1, f_2 >$ para el orden lex con $X > Y > Z$. Hallar el resto de la division de f por g_1, g_2.

9. 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) Mostrar que $1 \in I$ exhibiendo a_1, a_2, a_3 tales que $1 = a_1 f_1 + a_2 f_2 + a_3 f_3$.

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

$$X^\alpha Y^\beta < X^{\alpha'} Y^{\beta'} \quad \iff \quad X^\alpha < X^{\alpha'} \quad \text{o} \quad X^\alpha = X^{\alpha'} \text{ e } Y^\beta < Y^{\beta'}$$

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

11) 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.
(iii) Encontrar un orden monomial para el cual los generadores dados de I no sean una base de Gröbner.

13) Sean $f, g \in \mathbb{K}[X_1,\dots,X_n]$ 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 $p, q \in \mathbb{K}[X_1,\dots,X_n]$ 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 $f_1, \dots, f_s \in \mathbb{K}[X_1,\dots,X_n]$ son tales que sus monomios de cabeza son coprimos dos a dos, entonces son una base de Gröbner del ideal que generan para $<$.