

Llicenciatura de Matemàtiques FME
Examen parcial d'Àlgebra Computacional
16 d'abril de 2008

Problema 1. Siguin $f, g \in K[X, Y]$. Demostreu que f i g són relativament primers a l'anell $K[X, Y]$ si, i només si, ho són com a elements dels dos anells $K(X)[Y]$ i $K(Y)[X]$.

Doneu un exemple amb $(f, g) = 1$ a $K(X)[Y]$ però $(f, g) \neq 1$ a $K[X, Y]$.

SOLUCIÓ: Recordi's que: tots tres anells $K[X, Y], K(X)[Y], K(Y)[X]$ són factorials (i, per tant, dos elements no nuls sempre tenen màxim comú divisor); els dos últims són Euclidiàns (i, per tant, hi ha identitat de Bézout) però és primer NO ho és (per tant si $d = (f, g)$ a $K[X, Y]$ la identitat $fF(X, Y) + gG(X, Y) = d$ pot no tenir solució; per exemple no en té si $f = X, g = Y$); les unitats (invertibles) d'aquests anells són: $K[X, Y]^* = K^*$ (polinomis constants no nuls), $K(X)[Y]^* = K(X)^*$ i $K(Y)[X]^* = K(Y)^*$ (quocients de polinomis en una variable no nuls); dir que dos elements d'un anell no són relativament primers equival a dir que tenen un divisor comú que no és una unitat de l'anell.

Suposi's que $(f, g) \neq 1$ a l'anell $K[X, Y]$. Això equival a dir que existeix un polinomi no constant $d(X, Y) \in K[X, Y]$ que els divideix tots dos. Aquest polinomi d ha de ser no constant en alguna de les dues variables (potser en totes dues). Si és no constant en la variable X , aleshores és un factor comú no invertible dels dos polinomis f i g a l'anell $K(Y)[X]$, i per tant $(f, g) \neq 1$ en aquest anell. Anàlogament, si és no constant en la variable Y aleshores $(f, g) \neq 1$ a $K(X)[Y]$.

Suposi's que $(f, g) \neq 1$ a l'anell $K(X)[Y]$. Això equival a dir que existeix un polinomi $d \in K(X)[Y]$ no constant en la variable Y que els divideix tots dos. Sigui $dq_1 = f$ i $dq_2 = g$ amb $q_1, q_2 \in K(X)[Y]$. Els elements $d, q_1, q_2 \in K(X)[Y]$ són polinomis en la variable Y amb coeficients que són funcions racionals en la variable X . Sigui $m(X) \in K[X]$ el mínim comú múltiple dels coeficients d'aquests tres polinomis. Aleshores els productes $m(X)d, m(X)q_1$ i $m(X)q_2$ són polinomis en les variables X, Y i es tenen identitats

$$(m(X)d)(m(X)q_1) = m(X)^2 f(X, Y), \quad (m(X)d)(m(X)q_2) = m(X)^2 g(X, Y)$$

a l'anell de polinomis $K[X, Y]$. El polinomi $m(X)d \in K[X, Y]$ és no constant en la variable Y , ja que d ho és. Sigui $p(X, Y) \mid (m(X)d)$ un factor primer d'aquest polinomi a l'anell $K[X, Y]$ que sigui no constant en Y (n'hi ha d'haver algun ja que si tots els seus factors primers tinguessin grau zero en Y aleshores $m(X)d$ seria constant en Y). Aleshores $p(X, Y)$ divideix $m(X)^2 f(X, Y)$ a l'anell $K[X, Y]$ i, com que no pot dividir $m(X)$, ja que és no constant en Y , ha de dividir $f(X, Y)$. Raonant anàlogament amb g es veu que $p(X, Y)$ també divideix $g(X, Y)$, i per tant $(f, g) \neq 1$ a l'anell $K[X, Y]$.

De la mateixa manera es demostra que si $(f, g) \neq 1$ a $K(Y)[X]$ aleshores tots dos polinomis tenen un divisor comú no constant a l'anell $K[X, Y]$.

Qualsevol parell de polinomis de la forma $u(X)f(Y), u(X)g(Y)$ amb $(f, g) = 1$ a $K[Y]$ i $\deg u > 0$ són relativament primers a $K(X)[Y]$ però no ho són a $K[X, Y]$.

Problema 2. Sigui A un anell Noetherià. Sigui $I = \langle S \rangle \subseteq A$ l'ideal generat per un subconjunt $S \subseteq A$ (no necessàriament finit). Demostreu que existeix un subconjunt $S_0 \subseteq S$ finit tal que $I = \langle S_0 \rangle$.

SOLUCIÓ: Recordant les diferents caracteritzacions dels anells Noetherians, (1) tot ideal és finitament generat; (2) tota cadena ascendent d'ideals estaciona; (3) tot conjunt no buit d'ideals té algun element maximal, es donen diferents possibilitats per a demostrar-ho:

1) El teorema de la base de Hilbert assegura que I és finitament generat. Siguin $a_1, \dots, a_n \in I$ un conjunt finit de generadors. Com que el conjunt S genera l'ideal I cada a_i és una combinació lineal a coeficients a l'anell A de (un nombre finit de) elements de S . Sigui S_0 la reunió dels conjunts finits d'elements de S que apareixen en aquestes n combinacions lineals. Aleshores S_0 és un subconjunt de S que és finit i genera l'ideal I .

2) Si S és buit genera l'ideal zero i el subconjunt finit S ja el genera. Suposi's S no buit. Sigui $s_1 \in S$ qualsevol. Si $\langle s_1 \rangle = I$ ja està; en cas contrari no pot ser $S \subseteq \langle s_1 \rangle$ i existeix un element $s_2 \in S$ tal que $s_2 \notin \langle s_1 \rangle$. Si $\langle s_1, s_2 \rangle = I$ ja està; en cas contrari existeix un element $s_3 \in S \setminus \langle s_1, s_2 \rangle$. D'aquesta manera en un nombre finit de passos s'arribarà a tenir $\langle s_1, s_2, \dots, s_n \rangle = I$ ja que en cas contrari es podria construir una cadena estrictament creixent (no estacionària) infinita

$$\langle s_1 \rangle \subset \langle s_1, s_2 \rangle \subset \langle s_1, s_2, s_3 \rangle \dots$$

en contradicció amb la hipòtesi de que A és Noetherià.

3) Sigui $\mathcal{I} = \{\langle T \rangle : T \subseteq S, |T| < \infty\}$ el conjunt dels ideals de A generats per subconjunts finits de S . És no buit ja que conté per exemple l'ideal zero, generat pel conjunt buit, que és un subconjunt finit de qualsevol conjunt. Sigui $J = \langle T_0 \rangle \in \mathcal{I}$ un ideal maximal. Aleshores $J = I$ i per tant I està generat pel subconjunt finit $T_0 \subseteq S$. En efecte, en cas contrari no pot ser que $S \subseteq J$ i per tant existeix un element $s \in S \setminus J$. Aleshores $J \subset J + \langle s \rangle = \langle T_0 \cup \{s\} \rangle \in \mathcal{I}$ és un element del conjunt estrictament més gran que J , el qual contradia la seva maximalitat.

Problema 3. Sigui $V = \mathbb{V}(Z^3 - X^5, Y^3 - X^2) \subseteq \mathbb{C}^3$. Sigui $W \subseteq \mathbb{C}^3$ la varietat definida per la parametrització polinòmica $F(T) = (T^3, T^2, T^5)$. Demostreu que es té $W \subset V$ i que la inclusió és estricta.

INDICACIÓ: Comproveu que $V = \mathbb{V}(Z^3 - X^3Y^3, Y^3 - X^2)$ i descomponeu el primer polinomi d'aquest nou sistema d'equacions en un producte.

SOLUCIÓ: Recordi's que, per definició, W és la clausura de Zariski del conjunt $F(\mathbb{C}) = \{F(z) : z \in \mathbb{C}\}$. Cada punt $(z, z^2, z^3) \in F(\mathbb{C})$ pertany a V ja que les seves coordenades satisfan les dues equacions que defineixen V . Per tant, $W = \overline{F(\mathbb{C})} \subseteq V$, ja que la clausura de Zariski és la intersecció de totes les varietats que contenen el conjunt, i per tant està continguda en tota varietat que contingui $F(\mathbb{C})$.

Per veure que la inclusió es estricta es segueix la indicació. Per comprovar que

$$\mathbb{V}(Z^3 - X^5, Y^3 - X^2) = \mathbb{V}(Z^3 - X^3Y^3, Y^3 - X^2)$$

n'hi ha prou a veure que els dos polinomis de cada costat generen el mateix ideal I , ja que aleshores la varietat és $\mathbb{V}(I)$, que no depèn dels polinomis. En efecte, es té

$$Z^3 - X^3Y^3 = (1)(Z^3 - X^5) + (-X^3)(Y^3 - X^2) \Rightarrow \langle Z^3 - X^3Y^3, Y^3 - X^2 \rangle \subseteq \langle Z^3 - X^5, Y^3 - X^2 \rangle$$

i la inclusió contrària és conseqüència de la igualtat

$$Z^3 - X^5 = (1)(Z^3 - X^3Y^3) + (X^3)(Y^3 - X^2).$$

Així, la varietat V és també el conjunt de zeros d'aquests altres dos polinomis. Es té la descomposició en producte de primers a $\mathbb{C}[X, Y]$ següent

$$Z^3 - X^3Y^3 = (Z - XY)(Z - \rho XY)(Z - \rho^2 XY), \quad \rho = \frac{-1 + \sqrt{-3}}{2} = e^{2\pi i/3}.$$

de la qual es dedueix que

$$V = \mathbb{V}(Z^3 - X^3Y^3, Y^3 - X^2) = \mathbb{V}(Z - XY, Y^3 - X^2) \cup \mathbb{V}(Z - \rho XY, Y^3 - X^2) \cup \mathbb{V}(Z - \rho^2 XY, Y^3 - X^2).$$

Les tres varietats V_i a la dreta d'aquesta descomposició no estan contingudes l'una en l'altra, ja que per exemple, els tres punts $(1, 1, 1)$, $(1, 1, \rho)$, $(1, 1, \rho^2) \in V$ pertanyen cadascun a una i només una d'aquestes varietats (es pot veure, tot i que per aquest problema no cal, que aquesta descomposició és de fet la descomposició irredundant de V com a reunió de varietats simples).

És clar que $F(\mathbb{C}) \subseteq V_1 = \mathbb{V}(Z - XY, Y^3 - X^2)$. Per tant, $W \subseteq V_1 \neq V$.