NOTAS SOBRE EL TEOREMA DE BÉZOUT PARA CURVAS PLANAS.

FERNANDO CUKIERMAN

Índice

1. Introducción.

Nos proponemos demostrar los dos Teoremas siguientes.

1. **Teorema.** *(Teorema de Bézout en el plano afín) Sea k un cuerpo algebraicamente cerrado. Sean $f, g \in k[x, y]$ polinomios de grados respectivos d, e, sin factores comunes. Denotemos $X = \mathcal{C}(f) \cap \mathcal{C}(g)$ el conjunto de ceros comunes de f y g en k^2. Entonces X es un conjunto finito y*

$$\sum_{p \in X} (f, g; p) \leq de. \tag{1.1}$$

Además, vale la igualdad en 1.1 si y sólo si f y g no tienen direcciones asintóticas en común.

2. **Teorema.** *(Teorema de Bézout en el plano proyectivo) Sea k un cuerpo algebraicamente cerrado. Sean $F, G \in k[x_0, x_1, x_2]$ polinomios homogéneos de grados respectivos d, e, sin factores comunes. Denotemos $X = \mathcal{C}(F) \cap \mathcal{C}(G)$ el conjunto de ceros comunes de F y G en $\mathbb{P}^2(k)$. Entonces X es un conjunto finito y*

$$\sum_{p \in X} (F, G; p) = de. \tag{1.2}$$

En estas notas daremos las definiciones involucradas y desarrollaremos las demostraciones de los Teoremas 1 y 2. Principalmente necesitaremos varias propiedades de la resultante y de la multiplicidad de intersección. La idea central de la demostración presente del Teorema 1 (ver Sección 6) se encuentra en la cadena de desigualdades 4.1. Por otra parte, el Teorema 2, como veremos, es consecuencia inmediata del Teorema 1.

Existen al menos cuatro definiciones (equivalentes) de la multiplicidad de intersección $(f, g; p)$ de dos polinomios $f, g \in k[x, y]$ en un punto $p \in k^2$:

a) La de *Macaulay y Fulton*, que nosotros también adoptamos; ver [9] y Definición 22.

b) El *orden de anulación de la resultante* (en un sistema de coordenadas apropiado), como en 2.2 y Teorema 23.

c) La obtenida vía los *desarrollos de Newton-Puiseux*, para lo cual se puede consultar [19], o también [2], [5], [6], [7], [13].

d) La basada en la noción de *residuo* de la forma diferencial $df/f \wedge dg/g$, también relacionada con el concepto de *grado* de una función; ver [14].

Todas estas definiciones están de cierta manera motivadas por el siguiente caso particular: si uno de los polinomios, digamos f, es no-singular en p, por el teorema de la función implícita existe una parametrización analítica $(x(t), y(t))$ de la curva $f = 0$ alrededor de p. Entonces la multiplicidad de intersección se puede calcular como el orden de anulación de $g(x(t), y(t))$ en $t = 0$.

En cuanto a los pros y contras de cada una de estas definiciones, b) es bastante intuitiva y elemental, pero su cálculo es dificultoso. La definición a) es posiblemente más abstracta, pero tiene buenas propiedades y un algoritmo sencillo de Fulton para su cálculo efectivo en ejemplos; ver Sección 8. Las definiciones c) y d) tienen interés conceptual y son más calculables que b). No utilizaremos c) ni d) en estas notas y referimos para su estudio a las referencias ya mencionadas.

Como consecuencia natural de las varias definiciones de la multiplicidad de intersección, existen varias demostraciones del Teorema de Bézout. La primera de ellas, clásica y bastante elemental, se basa en las propiedades de la resultante. En [19], pag. 60, el autor alude a las deficiencias de una demostración basada solamente en la definición b), y por este motivo combina el argumento clásico via resultantes con la definición c). En particular en [19] se demuestra la equivalencia entre b) y c). Por otra parte, la demostración de [9] utiliza solamente la definición a). Está basada en complejos de Koszul y polinomios de Hilbert. Es una demostración elegante y eficaz, aunque requiere un grado mayor de sofisticación algebraica. Nuestra presentación consiste en desarrollar la demostración clásica via resultantes, combinándola con la definición a) de la multiplicidad de intersección. Esto requiere demostrar la equivalencia entre a) y b), cosa que llevamos a cabo en Teorema 23 y Corolario 26. Allí en particular se aclara la necesidad en b) de un sistema de coordenadas apropiado. Al demostrar esta equivalencia vamos a relacionar la matriz de Sylvester con la matriz de Bézout para el cálculo de la resultante, ver Proposición 12.

2. Preliminares sobre polinomios y series formales.

2.1. Sea $f \in A[x_1, \ldots, x_n]$ un polinomio en n variables $x_1, \ldots, x_n$ con coeficientes en un anillo conmutativo A. Por definición, f es una combinación lineal de la forma

$$f(x_1, \ldots, x_n) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \; x^\alpha$$

donde $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ es un monomio con exponente α y los coeficientes $a_\alpha \in A$ son tales que el soporte de f

$$\mathrm{sop}(f) := \{\alpha / a_\alpha \neq 0\}$$

es un conjunto finito. Para cada $\alpha \in \mathbb{N}^n$ denotamos

$$|\alpha| = \sum_i \alpha_i.$$

Sea $f \in A[x_1, \ldots, x_n]$, $f \neq 0$. Definimos el grado de f como

$$\mathrm{gr}(f) = \max\{|\alpha| / \; \alpha \in \mathrm{sop}(f)\}.$$

Para cada $d \in \mathbb{N}$ denotamos

$$A[x_1, \ldots, x_n]_{\leq d} = \{f \in A[x_1, \ldots, x_n] / \; f = 0 \;\text{ o }\; \mathrm{gr}(f) \leq d\},$$

el conjunto de polinomios de grado $\leq d$, incluyendo el polinomio cero.

Si $f \in A[x_1, \ldots, x_n] - \{0\}$ denotamos

$$\mathcal{C}(f) = \{x \in A^n / \; f(x) = 0\},$$

el conjunto de ceros de f.

También vamos a considerar el anillo de series formales $A[[x_1, \ldots, x_n]]$ cuyo elemento típico se escribe $f(x_1, \ldots, x_n) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \; x^\alpha$ con $a_\alpha \in A$.

2.2. Un polinomio $f \in A[x_1, \ldots, x_n]$ se dice *homogéneo* de grado d si es combinación lineal de monomios de grado exactamente d:

$$f(x_1, \ldots, x_n) = \sum_{|\alpha| = d} a_\alpha x^\alpha.$$

El polinomio cero satisface esta condición y por lo tanto está incluído. Para todo f homogéneo de grado d se verifica que $f(\lambda x) = \lambda^d f(x)$ para todo $\lambda \in A$.

Denotamos

$$A[x_1, \ldots, x_n]_d$$

el conjunto de los polinomios homogéneos de grado d en $x_1, \ldots, x_n$.

Todo $f \in A[x_1, \ldots, x_n]_{\leq d}$ se escribe de manera única en la forma

$$f = \sum_{j=0}^{d} f_j,$$

donde f_j es homogéneo de grado j. El polinomio f_j se llama *componente homogénea de f de grado j*.

Tenemos entonces una descomposición en suma directa de A-módulos libres

$$A[x_1, \ldots, x_n]_{\leq d} = \oplus_{0 \leq j \leq d} A[x_1, \ldots, x_n]_j.$$

2.3. La expresión de f como suma de polinomios homogéneos se puede escribir, más precisamente,

$$f = \sum_{j=r}^{d} f_j$$

con $f_r \neq 0$ y $f_d \neq 0$. Aquí $d = \mathrm{gr}(f)$ es el grado de f. El entero r se denomina *multiplicidad* (o también, *orden de anulación*) de f y se denota

$$r = \mu(f). \tag{2.1}$$

La *forma inicial* de f es el polinomio homogéneo f_r con $r = \mu(f)$. El *cono tangente* de f está definido por

$$\mathrm{cono}(f) = \mathcal{C}(f_r).$$

Similarmente, f_d se denomina *forma final* de f.

2.4. Las nociones anteriores se pueden extender a cualquier punto p mediante una translación. Precisamente, para $p \in A^n$, la forma inicial de f en p es la forma inicial del polinomio f_p definido por

$$f_p(x) = f(x + p).$$

El cono tangente de f en p, denotado $\mathrm{cono}_p(f)$, es el conjunto de ceros de la forma inicial de f en p. Del mismo modo, la multiplicidad de f en p se define como

$$\mu_p(f) = \mu(f_p), \tag{2.2}$$

con $\mu(f_p)$ como en 2.1.

2.5. Sea $f = f(x, y)$ un polinomio de grado $\leq d$ en dos variables x, y, con coeficientes en el cuerpo k. El conjunto $\mathcal{C}(f) \subset k^2$ es denominado también *curva algebraica afín* definida por f. Se aplican en este caso las nociones anteriores referentes a conjuntos de ceros $\mathcal{C}(f) \subset k^n$. Una particularidad del caso $n = 2$ es que el cono tangente es una unión de rectas, como se deduce de la siguiente:

3. **Proposición.** *Sea $f_r = f_r(x, y) \in k[x, y]_r$ un polinomio homogéneo de grado r con coeficientes en un cuerpo k algebraicamente cerrado. Entonces f_r se factoriza como producto de formas lineales*

$$f_r = \prod_i L_i^{r_i}$$

donde $L_i(x, y) = a_i x + b_i y$, $r_i \in \mathbb{N}$, $\sum_i r_i = r$.

Demostración. Resulta de des-homogeneizar y homogeneizar f_r; dejamos los detalles como ejercicio. □

Las rectas (distintas) $\mathcal{C}(L_i) \subset k^2$ se denominan *rectas componentes del cono de f en el origen.* También se las denomina a veces *rectas tangentes de f en el origen.* El entero r_i se denomina multiplicidad de L_i. Si $r > 1$ y $r_i = 1$ para todo i, se dice que 0 es un punto singular ordinario de f.

4. **Proposición.** *Sea $f = f(x, y) \in k[x, y]$ un polinomio de grado d con coeficientes en un cuerpo k. Sea f_r la forma inicial de f (en el origen, por simplicidad) y supongamos que $f_r = g_s h_{r-s}$ donde $g_s, h_{r-s} \in k[x, y]$ son polinomios homogéneos, de grados s y $r - s$ respectivamente, sin factores comunes. Entonces existen $g, h \in k[[x, y]]$ (anillo de series formales) tales que g_s (resp. h_{r-s}) es la forma inicial de g (resp. h) y $f = gh$ en $k[[x, y]]$.*

Demostración. Buscamos $g = \sum_{j \geq s} g_j$ y $h = \sum_{j \geq r-s} h_j$ tales que $f = gh$, o sea,

$$f_j = \sum_{s \leq k \leq j-(r-s)} g_k \ h_{j-k}$$

para todo $j \geq r$. La hipótesis sobre g_s, h_{r-s} permite resolver recursivamente el sistema infinito de ecuaciones

$$g_s \ h_{j-s} + g_{j-(r-s)} \ h_{r-s} = f_j - \sum_{s<k<j-(r-s)} g_k \ h_{j-k}$$

para $j = r, r + 1, \ldots$, en virtud del siguiente Lema.

□

5. **Lema.** *Sean $g \in k[x, y]_n$ y $h \in k[x, y]_m$. Sea r un entero $\geq n + m$. Supongamos que g y h no tienen factores comunes. Entonces para todo $c \in k[x, y]_r$ existen $a \in k[x, y]_{r-n}$ y $b \in k[x, y]_{r-m}$ tales que $c = a \ g + b \ h$.*

Demostración. Consideramos la aplicación k-lineal

$$\varphi : k[x, y]_{r-n} \times k[x, y]_{r-m} \to k[x, y]_r$$

tal que $\varphi(a, b) = a \ g + b \ h$. Queremos ver que φ es sobreyectiva.

Comenzamos calculando la dimensión del núcleo $\ker(\varphi)$: si $\varphi(a, b) = 0$ tenemos $ag = -bh$. Como $k[x, y]$ es DFU y g y h no tienen factores comunes, resulta que existe $d \in k[x, y]$ tal que $a = hd$ y $b = -gd$. Es claro que d es homogéneo de grado $r - (m + n)$. Por lo tanto, $\ker(\varphi)$ es igual a la imagen de la aplicación lineal inyectiva $\psi : k[x, y]_{r-(m+n)} \to k[x, y]_{r-n} \times k[x, y]_{r-m}$ tal que $\psi(d) = (hd, -gd)$. Obtenemos que $\dim \ker(\varphi) = \dim k[x, y]_{r-(m+n)} = r - (m + n) + 1$.

Entonces, $\dim \operatorname{im}(\varphi) = \dim(k[x, y]_{r-n} \times k[x, y]_{r-m}) - \dim \ker(\varphi) = (r - n) + 1 + (r - m) + 1 - (r - (m + n) + 1) = r + 1 = \dim k[x, y]_r$, lo cual implica que φ es sobreyectiva.

□

6. **Observación.** *Hemos demostrado en el Lema 5 la exactitud de la sucesión de k-espacios vectoriales*

$$0 \to k[x, y]_{r-(m+n)} \to k[x, y]_{r-n} \times k[x, y]_{r-m} \to k[x, y]_r \to 0$$

conocida como componente de grado r del complejo de Koszul asociado a g, h.

2.6. El anillo de series formales $k[[x_1, \ldots, x_n]]$ es un dominio de factorización única (ver p. ej. [20]). Un $f \in k[x, y]$ irreducible puede ser reducible cuando es considerado como elemento de $k[[x, y]]$. En su factorización $f = \prod_i f_i$, las series formales irreducibles f_i que aparecen se denominan *ramas de f en* 0.

El proceso algebraico de pasar de $f \in k[x, y]$ a $f \in k[[x, y]]$ corresponde geométricamente a concentrar la atención en un entorno arbitrariamente chico de $0 \in \mathcal{C}(f)$ (localización).

2.7. Sea $p \in k^2$. Denotamos

$$\tau_p : k[x,y] \to k[[x,y]]$$

la composición de $k[x,y] \to k[x,y]$, definida por $f \mapsto f_p$ (ver 2.4), con la inclusión $k[x,y] \hookrightarrow k[[x,y]]$. De este modo τ_p es un morfismo de anillos inyectivo. Recordemos que los elementos inversibles de $k[[x,y]]$ son las series formales $h \in k[[x,y]]$ tales que $h(0,0) \neq 0$. Para $f \in k[x,y]$ resulta entonces que $f(p) \neq 0$ si y sólo si $\tau_p(f)$ es inversible.

En [9] y otras referencias se utiliza (de modo similar), en lugar de $k[[x,y]]$, el anillo local algebraico $k[x,y]_p$ que consiste de las fracciones racionales cuyo denominador no se anula en p, y en lugar de τ_p, el morfismo de anillos $k[x,y] \to k[x,y]_p$ tal que $f \mapsto f/1$.

3. Resultante.

En esta sección recordamos algunos resultados sobre resultantes, a ser utilizados en la demostración del Teorema de Bézout. Para un tratamiento mas detallado sugerimos las referencias [3], [18], [19], entre varias otras que tratan el tema.

3.1. Sea A un dominio de integridad y sean $f, g \in A[t]$ dos polinomios de grados d y e respectivamente.

Similarmente a lo hecho en el Lema 5 consideramos el morfismo de A-módulos

$$\varphi_{f,g} = \varphi : A[t]_{<e} \times A[t]_{<d} \to A[t]_{<(d+e)}$$

tal que $\varphi(a, b) = af + bg$, donde denotamos $A[t]_{<e}$ el conjunto de polinomios de grado $< e$; es un A-módulo libre de rango e, con base ordenada distinguida $B_e = \{1, t, t^2, \ldots, t^{e-1}\}$ constituída por los monomios de grado $< e$.

La matriz de $\varphi_{f,g}$ en las bases ordenadas

$$B_{e,d} := B_e \times \{0\} \ \cup \ \{0\} \times B_d = \{(1, 0), (t, 0), \ldots (t^{e-1}, 0), (0, 1), (0, t), \ldots (0, t^{d-1})\}$$

y B_{d+e} es la conocida matriz de Sylvester de f, g. El determinante de esta matriz es, por definición, la resultante $R_{d,e}(f, g)$.

7. **Proposición.** *Sea A un DFU y sean $f \in A[t]_{\leq d}$ y $g \in A[t]_{\leq e}$. Supongamos que* $\mathrm{gr}(f) = d$ *o* $\mathrm{gr}(g) = e$. *Entonces las siguientes afirmaciones son equivalentes:*

i) f y g tienen un factor común de grado positivo.

ii) Existen polinomios $a, b \in A[t]$ tales que $\mathrm{gr}(a) < e$, $\mathrm{gr}(b) < d$, $af + bg = 0$.

iii) $R_{d,e}(f, g) = 0$.

Demostración. Ejercicio. □

8. **Observación.** *Si $f \in A[t]_{\leq d}$ y $g \in A[t]_{\leq e}$ pero* $\mathrm{gr}(f) < d$ *y* $\mathrm{gr}(g) < e$ *entonces* $R_{d,e}(f, g) = 0$ *(la matriz de Sylvester tiene una fila nula) sin que f y g tengan necesariamente un factor común de grado positivo.*

9. **Proposición.** (Resultante conmuta con especialización) *Sea $\epsilon : A \to B$ un morfismo de anillos. Sean $f \in A[t]_{\leq d}$ y $g \in A[t]_{\leq e}$. Denotamos $\epsilon : A[t] \to B[t]$ la extensión natural que consiste de aplicar ϵ en cada coeficiente de un $h \in A[t]$. Entonces:*

$$R_{d,e}(\epsilon(f), \epsilon(g)) = \epsilon(R_{d,e}(f, g))$$

Demostración. La formación de la matriz de Sylvester y del determinante claramente conmutan con ϵ. □

3.2. Sea $f \in A[x,y]$ de grado d. Como antes, podemos escribir

$$f = \sum_{0 \leq i+j \leq d} a_{ij} x^i y^j = \sum_{0 \leq k \leq n} f_k$$

donde $f_k = \sum_{i+j=k} a_{ij} x^i y^j$ es la componente homogénea de grado k. Siendo d el grado de f, tenemos $f_d \neq 0$, o sea, $a_{i(d-i)} \neq 0$ para algún $i = 0, 1, \ldots, d$. Podemos reagrupar los monomios de f del modo siguiente:

$$f = \sum_{0 \leq j \leq d} (\sum_{0 \leq i \leq d} a_{ij} x^i) y^j = \sum_{0 \leq j \leq D} a_j y^j$$

donde $a_j = \sum_{0 \leq i \leq d} a_{ij} x^i \in A[x]$ y

$$D = \max\{j / a_j \neq 0\} = \max\{j / a_{ij} \neq 0 \text{ para algún } \ i\}$$

El entero D se denomina *grado de f en la variable y*; denotamos $D = \mathrm{gr}_y(f)$.

Mediante esta reescritura tenemos definida una identificación (o isomorfismo canónico)

$$A[x,y] = A[x][y]$$

Similarmente identificamos $A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n]$ para cualquier $n \geq 2$.

10. **Proposición.** (Grado de la resultante, caso homogéneo) *Sean F, $G \in k[x_0, x_1, \ldots, x_n]$ dos polinomios homogéneos de grados d y e, respectivamente. Utilizando la identificación $k[x_0, \ldots, x_n] = k[x_1, \ldots, x_{n-1}][x_0]$ de 3.2, sea $R = R_{x_0}(x_1, \ldots, x_n)$ la resultante de F y G con respecto a x_0. Entonces R es un elemento de $k[x_1, \ldots, x_n]$ homogéneo de grado de.*

Demostración. Ejercicio (o ver [19]). □

11. **Proposición.** (Grado de la resultante) *Sean $f, g \in k[x,y]$ dos polinomios de grados d y e respectivamente, sin factores comunes. Sea $R = R_y(f,g) \in k[x]$ la resultante de f y g con respecto a y. Entonces R es un elemento de $k[x]$ de grado $\leq de$. Además, $\mathrm{gr}(R) = de$ si y sólo si f y g no tienen direcciones asintóticas comunes (o sea, las formas finales f_d, g_e no tienen factores comunes; ver [4]).*

Demostración. Denotemos $f = \sum_{j \leq d} f_j$ y $g = \sum_{j \leq e} g_j$ las descomposiciones de f y g como suma de polinomios homogéneos. En particular, f_d y g_e son las formas finales de f y g. Sean $F, G \in k[x,y,z]$ las homogeneizaciones de f y g, vale decir, $F = \sum_{j \leq d} f_j z^{d-j}$ y $G = \sum_{j \leq e} g_j z^{d-j}$, de modo que F y G son homogéneos de grados d y e respectivamente, y tales que $f(x,y) = F(x,y,1)$ y $g(x,y) = G(x,y,1)$.

Utilizando la Proposición 9 tenemos que

$$R_y(f,g) = R_y(F,G)|_{z=1}$$

Por la Proposición 10, $R_y(F,G)) \in k[x,z]$ es homogéneo de grado de. Entonces $R_y(F,G))|_{z=1} \in k[x]$ tiene grado $\leq de$. Resulta entonces que $\mathrm{gr}(R) \leq de$, lo cual demuestra nuestra primera afirmación.

Para demostrar la segunda afirmación, observemos que $\mathrm{gr}(R) < de$ si y sólo si z divide a $R_y(F,G)$, vale decir, $R_y(F,G)|_{z=0} = 0$. Utilizando nuevamente la Proposición 9 resulta

$$R_y(F,G)|_{z=0} = R_y(F|_{z=0}, G|_{z=0}) = R_y(f_d, g_e).$$

Obtenemos entonces que $\mathrm{gr}(R) < de$ si y sólo si f_d y g_e tienen un factor común, o sea, f y g tienen una dirección asintótica común, como deseábamos demostrar.

$\square$

Hemos definido la resultante como el determinante de la matriz de Sylvester. La resultante también puede ser expresada como el determinante de otra matriz, denominada matriz de Bézout. El resultado preciso se encuentra en la siguiente Proposición y va a ser utilizado más adelante para comparar dos definiciones de la multiplicidad de intersección entre curvas.

12. **Proposición.** (Resultante de Bézout) *Sea A un dominio de integridad y sean $f, g \in A[t]$ dos polinomios de grados n y m respectivamente. Suponemos que el coeficiente principal $g_m \in A$ es inversible. Sea $\tilde{f} : A[t]/(g) \to A[t]/(g)$ el homomorfismo de A-módulos inducido por multiplicación por f, o sea, tal que $\tilde{f}(\overline{h}) = \overline{fh}$ para todo $h \in A[t]$. Entonces*

$$R(f, g) = g_m^n \ \det(\tilde{f}).$$

Demostración. Debido a que g_m es inversible, el A-módulo $A[t]/(g)$ es libre, con base

$$\bar{B}_m = \{\bar{1}, \bar{t}, \ldots, \bar{t}^{m-1}\}$$

La matriz $[\tilde{f}]_{\bar{B}_m}$ de $\tilde{f}$ en la base $\bar{B}_m$ se denomina *matriz de Bézout de f, g*. Es una matriz $m \times m$ cuyos coeficientes son elementos de A que dependen de los coeficientes de f y g. Se sugiere como ejercicio escribir explícitamente dicha matriz para los primeros valores de m, n.

Queremos demostrar que el determinante de la matriz $m \times m$ de Bézout coincide con el determinante de la matriz $(m + n) \times (m + n)$ de Sylvester, salvo el factor inversible g_m^n.

Consideremos el siguiente diagrama de A-módulos libres:

$$\begin{tikzcd}
0 \arrow[r] & A[t]_{<n} \arrow[r] \arrow[d, equal] & A[t]_{<m} \times A[t]_{<n} \arrow[r, "\pi_1"] \arrow[d, "\varphi_{f,g}"] & A[t]/(g) \arrow[r] \arrow[d, "\tilde{f}"] & 0 \\
0 \arrow[r] & A[t]_{<n} \arrow[r, ".g"] & A[t]_{<(m+n)} \arrow[r, "\pi"] & A[t]/(g) \arrow[r] & 0
\end{tikzcd}$$

donde π es proyección al cociente, π_1 es proyección en la primera coordenada seguida de proyección al cociente y $.g$ denota multiplicación por g. Es inmediato verificar que el diagrama es conmutativo y las filas son exactas.

Como en 3.1 denotemos las bases ordenadas $B = B_{m,n}$ y $B' = B_{m+n}$, de modo que $[\varphi_{f,g}]_{BB'}$ es la matriz de Sylvester de f, g.

Consideramos el siguiente conjunto ordenado de elementos de $A[t]_{<(m+n)}$:

$$B'' = \{1, t, t^2, \ldots, t^{m-1}\} \cup \{g, tg, t^2 g, \ldots, t^{n-1} g\}$$

Afirmamos que B'' es base de $A[t]_{<(m+n)}$. En efecto, denotemos $[B''B']$ la matriz cuyas columnas son las coordenadas de los elementos de B'' en la base B'. Es fácil ver que dicha matriz tiene la estructura en bloques:

$$[B''B'] = \begin{bmatrix} I_m & * \\ 0 & T \end{bmatrix}$$

donde I_m es la matriz identidad $m \times m$ y T es triangular de $n \times n$, con g_m a lo largo de la diagonal. Obtenemos entonces que

$$\det[B''B'] = g_m^n.$$

Por nuestra hipótesis sobre g_m resulta que $\det[B''B']$ es inversible, y por lo tanto B'' es base. Observemos además que $[B''B'] = [\mathrm{id}]_{B''B'}$ es la matriz de cambio de base.

A continuación, afirmamos que la matriz de $\varphi = \varphi_{f,g}$ en las bases B, B'' tiene estructura en bloques:

$$[\varphi]_{BB''} = \left[\begin{array}{cc} [\tilde{f}] & 0 \\ * & I_n \end{array} \right]$$

donde $[\tilde{f}] = [\tilde{f}]_{\bar{B}_m}$ es la matriz de Bézout. En efecto, tenemos

$$\varphi(t^i, t^j) = t^i f + t^j g,\ 0 \leq i < m,\ 0 \leq j < m.$$

Aplicando el algoritmo de división podemos escribir $t^i f = a_i g + b_i$ donde $a_i, b_i \in A[t]$ y $\mathrm{gr}(b_i) < m$ para $0 \leq i < m$. De las definiciones resulta entonces que la i-ésima columna de $[\tilde{f}]$ es el vector de coeficientes de b_i y que $[\varphi]_{BB''}$ tiene la forma en bloques propuesta.

Finalmente, tomando determinante en la igualdad $[\varphi]_{BB'} = [\mathrm{id}]_{B''B'}\, [\varphi]_{BB''}$ obtenemos la fórmula enunciada. $\square$

13. **Observación.** *Para un tratamiento alternativo de la Proposición 12 se puede consultar* [3]*, teniendo en cuenta que el determinante de la matriz de Bézout es, por definición, la* Norma *de la clase de f en el álgebra $A[t]/(g)$. Para una generalización interesante de la Proposición 12 ver* [17]*, Lemma 15.28.8. Un estudio profundo de varias expresiones matriciales de resultantes se puede encontrar en* [12].

4. Teorema de Bézout en el plano afín, comienzo de la Demostración.

4.1. Manteniendo la notación de 3.2, para $f \in A[x,y]$ es claro que $\mathrm{gr}_y(f) = D \leq \mathrm{gr}(f) = d$. Además, vale $\mathrm{gr}_y(f) = \mathrm{gr}(f)$ si y sólo si $f_d(0,1) = a_{0d} \neq 0$, o sea, f contiene el monomio y^d.

Observemos también que $a_j = \sum_{0 \leq i \leq d-j} a_{ij} x^i$ y por lo tanto $\mathrm{gr}(a_j) \leq d - j$. En particular, $a_d = a_{0d} \in A$ es una constante. Entonces, $\mathrm{gr}_y(f) = \mathrm{gr}(f)$ si y sólo si $f = \sum_{0 \leq j \leq d} a_j y^j$ con $a_d \in A$, $a_d \neq 0$.

En caso que $\mathrm{gr}_y(f) = \mathrm{gr}(f)$ diremos que f *satisface la condición de Noether.*

Geométricamente esta condición significa que f no tiene asíntotas verticales (ver [4]).

14. **Proposición.** *Sea k un cuerpo y sean $f, g \in k[x,y]$, de grados d, e respectivamente. Denotamos $R_y(f,g) \in k[x]$ la resultante $R_{D,E}$ de f, g considerados como elementos de $k[x][y]$ de grados D, E en y, respectivamente. Entonces, f, g tienen un factor común $h \in k[x,y]$ de grado positivo en y si y sólo si $R_y(f,g) = 0$.*

Demostración. Es consecuencia directa de las propiedades generales de la resultante. □

15. **Proposición.** *Sea k un cuerpo y sean $f, g \in k[x,y]$ de grados d, e respectivamente, sin factores comunes. Sea $X = \mathcal{C}(f) \cap \mathcal{C}(g) \subset k^2$ el conjunto de ceros comunes de f y g. Denotamos $\pi : k^2 \to k$ la proyección definida por $\pi(x,y) = x$ y $R = R_y(f,g)$. Entonces:*

a) $R \in k[x]$ es un polinomio no-nulo.

b) $\pi(X) \subset \mathcal{C}(R)$, o sea, las primeras coordenadas de los ceros comunes de f y g son ceros de R.

c) X es un conjunto finito.

Demostración. a) Como suponemos que f y g no tienen factor común, en particular no tienen factor común de grado positivo en y. Por la Proposición 14 resulta $R \neq 0$.

b) Sea $a \in \pi(X)$. Sea entonces $b \in k$ tal que $p = (a,b) \in X$. Consideremos el morfismo de k-álgebras $\epsilon : k[x] \to k$ tal que $\epsilon(x) = a$. Resulta entonces que $\epsilon(f)(y) = f(a,y)$ y $\epsilon(g)(y) = g(a,y)$ tienen la raíz común b. Por lo tanto, $0 = R_y(\epsilon(f), \epsilon(g)) = \epsilon(R_y(f,g)) = \epsilon(R)$, o sea, $R(a) = 0$.

c) Por a) y b), la restricción de π a X

$$\pi|_X : X \to \mathcal{C}(R)$$

tiene imagen contenida en el conjunto finito $\mathcal{C}(R)$. Basta entonces con ver que $\pi|_X^{-1}(a)$, que denotaremos X_a, es finito para todo $a \in \mathcal{C}(R)$. El conjunto X_a, que consiste de todos los puntos de X con primera coordenada a, está en biyección con el conjunto de ceros comunes de $\epsilon(f), \epsilon(g) \in k[y]$. Si este conjunto fuese infinito, tendríamos $\epsilon(f) = \epsilon(g) = 0$ y entonces $x - a$ sería un factor común de f y g en $k[x,y]$.

□

16. **Observación.** *Con la notación de la Demostración de c), tenemos la siguiente fórmula para el cardinal $|X|$:*

$$|X| = \sum_{a \in \mathcal{C}(R)} |X_a|$$

17. **Proposición.** *Sea k un cuerpo algebraicamente cerrado. Con la notación de Proposición 15, escribamos $f = \sum_{0\leq j\leq D} a_j y^j$, $g = \sum_{0\leq j\leq E} b_j y^j$ como en 3.2. Entonces:*

$$\mathcal{C}(R) = \pi(X) \cup (\mathcal{C}(a_D) \cap \mathcal{C}(b_E))$$

Demostración. Sea $a \in k$ tal que $R(a) = 0$ y $a_D(a) \neq 0$ o $b_E(a) \neq 0$. Sea ϵ como en Proposición 15. Por la Proposición 9 tenemos que $R(\epsilon(f), \epsilon(g)) = 0$. Como $\epsilon(f)$, $\epsilon(g)$ satisfacen la hipótesis de Proposición 7, resulta que tienen un factor común en $k[y]$ de grado positivo. Debido a que k es algebraicamente cerrado, dicho factor tiene grado uno. Por lo tanto, $\epsilon(f)$, $\epsilon(g)$ tienen una raíz común $b \in k$, de lo cual resulta que $(a, b) \in X$ y por lo tanto $a \in \pi(X)$.

La recíproca resulta de Proposición 15 y Observación 8. □

18. **Corolario.** *Supongamos además que $\mathcal{C}(a_D) \cap \mathcal{C}(b_E) = \emptyset$, cosa que ocurre por ejemplo si f o g satisface la condición de Noether 4.1. Entonces:*

$$\mathcal{C}(R) = \pi(X)$$

4.2. Recordemos la acción del grupo general lineal en el anillo de polinomios.

Sea $\sigma : k^n \to k^n$ una función lineal, escrita en coordenadas:

$$\sigma(x_1, \ldots, x_n) = (\sum_j \sigma_{1j} x_j, \ldots, \sum_j \sigma_{nj} x_j)$$

con $\sigma_{ij} \in k$. Para $f \in k[x_1, \ldots, x_n]$ denotamos $f^\sigma \in k[x_1, \ldots, x_n]$ el polinomio definido por

$$f^\sigma(x_1, \ldots, x_n) = f(\sum_j \sigma_{1j} x_j, \ldots, \sum_j \sigma_{nj} x_j).$$

Sea $\mathrm{GL}_n(k)$ el grupo de transformaciones lineales $k^n \to k^n$ inversibles. Entonces la aplicación

$$k[x_1, \ldots, x_n] \times \mathrm{GL}_n(k) \to k[x_1, \ldots, x_n]$$

tal que $(f, \sigma) \mapsto f^\sigma$ es una acción (a derecha) del grupo $\mathrm{GL}_n(k)$ en la k-álgebra $k[x_1, \ldots, x_n]$.

Para cada $\sigma \in \mathrm{GL}_n(k)$, la aplicación $\sigma^* : k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]$ tal que $\sigma^*(f) = f^\sigma$, es un isomorfismo de k-álgebras. Los subespacios $k[x_1, \ldots, x_n]_d$ y $k[x_1, \ldots, x_n]_{\leq d}$ son estables. Si f_j denota la componente homogénea de grado j de f, vale que $(f^\sigma)_j = (f_j)^\sigma$. Por lo tanto, f^σ y f tienen el mismo grado y la misma multiplicidad.

En cuanto a los conjuntos de ceros, se verifica que

$$\mathcal{C}(f^\sigma) = \sigma^{-1}(\mathcal{C}(f)).$$

19. **Proposición.** *Sea k un cuerpo infinito y sea $f \in k[x, y]$ de grado d. Entonces existe $\sigma \in GL_2(k)$ tal que f^σ satisface la condición de Noether 4.1.*

Demostración. Sabemos 4.1 que f satisface la condición de Noether si y sólo si $f_d(0, 1) \neq 0$. Sea $\sigma : k^2 \to k^2$ lineal inversible. Entonces f^σ tiene grado d y su forma final es $(f_d)^\sigma$. Por lo tanto, $(f^\sigma)_d(0, 1) = f_d(\sigma(0, 1))$. Elijamos un $(a, b) \in k^2$ tal que $f_d(a, b) \neq 0$. Un tal (a, b) existe porque $f_d \neq 0$ y k es infinito. Entonces cualquier σ tal que $\sigma(0, 1) = (a, b)$ satisface lo requerido. □

20. **Ejercicio.** *Demostrar similarmente que para cualquier $r \in \mathbb{N}$ y $f_1, \dots, f_r \in k[x, y]$ no nulos existe $\sigma \in GL_2(k)$ tal que f_i^σ satisface la condición de Noether para todo i.*

Podemos mejorar el resultado de la Proposición 15 c), del modo siguiente:

21. **Proposición.** *Sea k un cuerpo y sean $f, g \in k[x, y]$ de grados d, e respectivamente, sin factores comunes. Sea $X = \mathcal{C}(f) \cap \mathcal{C}(g) \subset k^2$ el conjunto de ceros comunes de f y g. Entonces $|X| \leq de$.*

Demostración. Sabemos por la Proposición 15 que X es finito. Denotemos $X = \{p_1, \dots, p_r\}$ con $p_i = (a_i, b_i) \in k^2$. Sea $\overline{p_i p_j}$ la recta que une p_i con p_j para cada $i \neq j$ y sea $h_{ij} \in k[x, y]$ el polinomio de grado uno ecuación de $\overline{p_i p_j}$.

Sin pérdida de generalidad, podemos suponer que se satisfacen las siguientes condiciones:

i) f y g satisfacen la condición de Noether.

ii) Ninguna de las rectas $\overline{p_i p_j}$ es vertical (o sea, los h_{ij} satisfacen la condición de Noether).

En efecto, por el Ejercicio 20, existe $\sigma \in \mathrm{GL}_2(k)$ tal que f^σ, g^σ y los h_{ij}^σ satisfacen la condición de Noether. Y por 4.2 tenemos $\sigma^{-1}(\mathcal{C}(f) \cap \mathcal{C}(g)) = \mathcal{C}(f^\sigma) \cap \mathcal{C}(g^\sigma)$.

La condición ii) equivale a decir que todos los elementos de X tienen diferente primera coordenada, o sea, con notación de 15 vale $|X_a| = 1$ para todo $a \in \mathcal{C}(R)$, o también que

$$\pi : X \to \mathcal{C}(R)$$

es inyectiva. Resulta entonces de la Observación 16 que

$$|X| \leq |\mathcal{C}(R)| \leq \mathrm{gr}(R) \leq de. \tag{4.1}$$

como se deseaba demostrar. □

5. Multiplicidad de intersección y orden de anulación de la resultante.

En esta Sección definiremos la multiplicidad de intersección de dos curvas planas en un punto, siguiendo [9]. También, relacionaremos dicha multiplicidad con el orden de anulación de la resultante. Las propiedades generales de la multiplicidad de intersección serán desarrolladas en la Sección 8.

22. **Definición.** *Sean $f, g \in k[x, y]$. Definimos la multiplicidad de intersección $(f, g; 0) \in \mathbb{N} \cup \{\infty\}$ de f y g en el punto $0 = (0, 0)$ como*

$$(f, g; 0) = \dim_k k[[x, y]]/(f, g)$$

donde (f, g) denota el ideal generado por $\{f, g\}$ en el anillo $k[[x, y]]$.

Si $p = (a, b) \in k^2$, definimos $(f, g; p) = (f_p, g_p; 0)$, donde $f_p(x, y) = f(x + a, y + b)$.

A continuación establecemos la relación que existe entre el orden de anulación de la resultante y la multiplicidad de intersección. El Teorema siguiente se basa en [10] (1.6) y [11] (App. A).

23. **Teorema.** (Resultante y multiplicidad de intersección) *Sean $f, g \in k[x, y] = k[x][y]$, de grados respectivos d, e, sin factores comunes. Mantenemos las notaciones de 3.2, 21. En particular, $R = R_y(f, g) \in k[x]$ es la resultante de f, g respecto a la variable y, y $\pi : X \to k$ denota la primera proyección. Sea $a \in k$ y supongamos que a no es cero común de a_D, b_E. Entonces (ver 2.2)*

$$\mu_a(R) = \sum_{p \in \pi^{-1}(a)} (f, g; p).$$

Demostración. Fijado $a \in k$ denotemos $\pi^{-1}(a) = \{p_1, \ldots, p_n\}$ con $p_i = (a, b_i)$. Tenemos

$$\sum_{p \in \pi^{-1}(a)} (f, g; p) = \sum_{i=1}^{n} (f, g; p_i) = \sum_{i=1}^{n} \dim_k k[[x, y]]/(f_{p_i}, g_{p_i})$$

donde $f_{p_i} = f(x + a, y + b_i), g_{p_i} = g(x + a, y + b_i)$. Denotamos similarmente $f_a(x, y) = f(x + a, y), g_a(x, y) = g(x + a, y)$. Tenemos un morfismo de anillos

$$\tau : k[[x]][y]/(f_a, g_a) \to \prod_{1=1}^{n} k[[x, y]]/(f_{p_i}, g_{p_i})$$

definido por $\tau(h) = (h_{p_1}, \ldots, h_{p_n})$ (ver 2.7). Dejamos como ejercicio para el lector demostrar que τ es un isomorfismo, usando el Teorema chino del resto (ver p. ej. [9]). Por lo tanto,

$$\sum_{i=1}^{n} \dim_k k[[x, y]]/(f_{p_i}, g_{p_i}) = \dim_k k[[x]][y]/(f_a, g_a),$$

con lo cual sólo necesitamos demostrar que

$$\dim_k k[[x]][y]/(f_a, g_a) = \mu_a(R) = \mu(R_a). \tag{5.1}$$

Consideremos $k[[x]][y]/(f_a)$ como módulo (libre, de rango $D = \mathrm{gr}_y(f)$) sobre el anillo $A = k[[x]]$. Sea

$$\psi : k[[x]][y]/(f_a) \to k[[x]][y]/(f_a)$$

el morfismo inducido por multiplicacion por g_a. Entonces, $k[[x]][y]/(f_a, g_a) = \mathrm{coker}(\psi)$. Debido a la Proposición 12, $R_a = \det(\psi)$ y entonces $\mu(R_a) = \dim_k A/(\det(\psi))$. Por lo tanto, 5.1 es consecuencia del Lema siguiente. ∎

24. **Lema.** *Sea $A = k[[x]]$ y sea $\psi : A^n \to A^n$ un endomorfismo de un A-módulo libre de rango finito. Entonces*

$$\dim_k \operatorname{coker}(\psi) = \dim_k \operatorname{coker}(\det(\psi))$$

Demostración. El endomorfismo ψ es de la forma $\psi(m) = M.m$ para $m \in A^n$, donde $M \in A^{n\times n}$. Como se sabe de la teoría de divisores elementales, debido a que A es un anillo principal existen $P, Q \in A^{n\times n}$ inversibles tal que PMQ es una matriz diagonal. Nos reducimos entonces al caso en que M es una matriz diagonal, con diagonal $(a_1, \dots, a_n)$, $a_i \in A$. Podemos suponer $a_i \neq 0$ para todo i, ya que en caso contrario ambos miembros de la igualdad enunciada son infinito. Tenemos $a_i = x^{e_i} u_i$ donde $u_i \in A$ es una unidad y $e_i \in \mathbb{N}$. Entonces,

$$\dim_k \operatorname{coker}(\psi) = \dim_k \oplus_i A/(a_i) = \sum_i e_i = \dim_k A/(\det M) = \dim_k \operatorname{coker}(\det(\psi)).$$

□

25. **Observación.** *El Lema anterior es válido reemplazando $k[[x]]$ por anillos A más generales, utilizando la noción de* longitud *de un A-módulo en lugar de* $\dim_k$. *Si A es principal, esencialmente la misma demostración anterior es válida. Para A más general se puede consultar* [10] *p. 7 y* [11] *(A2.6).*

26. **Corolario.** *En las condiciones del Teorema 23, supongamos además que $\pi^{-1}(a)$ consiste de un sólo punto p. Entonces*

$$\mu_a(R) = (f, g; p).$$

27. **Corolario.** *La multiplicidad de intersección $\mu_a(R)$ calculada con la resultante, no depende del sistema de coordenadas en posición general. Más precisamente: dados $f, g \in k[x, y]$ (sin factores comunes) y $p \in X = \mathcal{C}(f) \cap \mathcal{C}(g)$ existe (ver 19) $\sigma : k^2 \to k^2$ isomorfismo lineal tal que $\pi^{-1}(a) = \{p\}$, denotando $\sigma = (\sigma_1, \sigma_2)$ con $\sigma_i : k^2 \to k$, $\pi = \sigma_1|X$ y $a = \pi(p)$. Decimos que σ está en posición general. Por el Corolario 26 vale que $\mu_a(R) = (f, g; p)$. En particular, el valor de $\mu_a(R)$ no depende de σ, si σ está en posición general.*

6. Teorema de Bézout en el plano afín, fin de la Demostración.

Estamos en condiciones de completar la demostración del Teorema 1.

Demostración. La idea es analizar la cadena de desigualdades 4.1.

Suponemos como en la demostración de la Proposición anterior que se satisfacen las condiciones de Noether i). Consideremos los puntos de intersección contados con multiplicidad:

$$\sum_{p\in X}(f,g;p) = \sum_{a\in\pi(X)}\sum_{p\in\pi^{-1}(a)}(f,g;p) = \sum_{a\in\mathcal{C}(R)}\mu_a(R) = \mathrm{gr}(R)$$

ya que por el Teorema 23 tenemos $\sum_{p\in\pi^{-1}(a)}(f,g;p) = \mu_a(R)$ para todo $a \in k$.

Además, por la Proposición 11 sabemos que $\mathrm{gr}(R) \leq de$, y que vale la igualdad si y sólo si f y g no tienen direcciones asintóticas en común, lo cual completa la demostración del Teorema 1.

□

7. Teorema de Bézout en el plano proyectivo.

Referimos a [4] para la definición y primeras propiedades de los espacios proyectivos.

7.1. Curvas en el plano proyectivo. En esta sección consideramos curvas algebraicas de grado d en el plano proyectivo $\mathbb{P}^2(k)$, o sea, conjuntos de la forma

$$\mathcal{C}(F) = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(k) : \ F(x_0, x_1, x_2) = 0\}$$

donde $F \in k[x_0, x_1, x_2]_d$ es un polinomio no-nulo en las variables x_0, x_1, x_2, homogéneo de grado d.

28. **Definición.** *(Multiplicidad de intersección para curvas proyectivas) Sean F, G dos polinomios homogéneos en x_0, x_1, x_2 sin factores comunes, de grados d y e respectivamente. Definimos*

$$(F, G; p) = (F_*, G_*; p_*)$$

donde F_* y G_* denotan la deshomogeneización respecto de la variable x_i para algun $i = 0, 1, 2$ tal que $p_i \neq 0$.

29. **Proposición.** *$(F, G; p)$ no depende de la variable utilizada para deshomogeneizar.*

Demostración. Resulta inmediatamente de la propiedad de invariancia, combinada con Proposición (7.4.2) de [4]. □

Estamos ahora en condiciones de demostrar el Teorema 2.

Demostración. Veamos primero que X es finito. Sean $f = F_*, g = G_* \in k[x, y]$ las deshomogeneizaciones respecto a la variable x_0, de modo que $f(x, y) = F(1, x, y)$ y $g(x, y) = G(1, x, y)$. Entonces f, g no tienen factores comunes, y por lo tanto tienen finitos ceros en común. Estos son los ceros comunes de F y G donde $x_0 \neq 0$. Además, F y G tienen finitos ceros en común donde $x_0 = 0$ (recta del infinito), ya que en caso contrario tendrían a x_0 como factor común.

Siendo entonces que X es finito, podemos elegir una recta $L \subset \mathbb{P}^2(k)$ tal que $X \cap L = \emptyset$. Mediante un cambio lineal de coordenadas podemos suponer $L = \mathcal{C}(x_0)$ (seguimos denotando F y G a los nuevos polinomios). Entonces, con la notación del párrafo anterior, $f = F_*, g = G_*$ no tienen direcciones asintóticas en común y en virtud del Teorema 1 tenemos

$$\sum_{p \in X} (F, G; p) = \sum_{p \in X - L} (F_*, G_*; p) = de.$$

□

Para aplicaciones del Teorema de Bézout referimos por ejemplo a [9] y [19].

8. Propiedades de la multiplicidad de intersección.

A continuación revisamos las propiedades de la multiplicidad de intersección de [9], incluyendo algunas demostraciones alternativas y comentarios.

30. **Teorema.** *La multiplicidad de intersección 22 satisface las siguientes propiedades:*

a) $(f, g; p) = \infty$ *si y sólo si* f *y* g *tienen un factor común* h *tal que* $h(p) = 0$.

b) $(f, g; p) = 0$ *si y sólo si* $p \notin \mathcal{C}(f) \cap \mathcal{C}(g)$

c) (Invariancia) Si $\sigma : k[[x, y]] \to k[[x, y]]$ *es un isomorfismo de* k*-álgebras entonces*

$$(\sigma(f), \sigma(g); \sigma(p)) = (f, g; p)$$

para $f, g \in k[x, y]$ *tales que* $\sigma(f), \sigma(g) \in k[x, y]$. *Si* $p = (a, b) \in k^2$, $\sigma(p)$ *denota el punto* $(\sigma(x - a)(0, 0), \sigma(y - b)(0, 0)) \in k^2$.

d) (Conmutatividad) $(g, f; p) = (f, g; p)$

e) (Aditividad) $(f, g_1.g_2; p) = (f, g_1; p) + (f, g_2; p)$

f) $(f, g; p) = (f, g + a.f; p)$ *para todo* $a \in k[x, y]$.

g) Vale la desigualdad

$$(f, g; p) \geq \mu_p(f)\ \mu_p(g).$$

Además, vale la igualdad si y sólo si las formas iniciales de f *y* g *no tienen factores comunes.*

En particular, $(f, g; p) = 1$ *si y sólo si* f *y* g *son no-singulares en* p *y sus rectas tangentes en* p *son distintas.*

Demostración. Las propiedades c), d), f) son consecuencias inmediatas de las definiciones.

b) Sin pérdida de generalidad podemos suponer $p = (0, 0)$.

La condición $(f, g; 0) = 0$ significa que vale la igualdad de ideales $(f, g) = (1)$, o sea, que existe una combinación lineal $af + bg = 1$ con $a, b \in k[[x, y]]$.

Si $0 \in \mathcal{C}(f) \cap \mathcal{C}(g)$, especializando $(x, y) = (0, 0)$ obtenemos la contradicción $0 = 1$.

Recíprocamente, supongamos $0 \notin \mathcal{C}(f) \cap \mathcal{C}(g)$, de modo que $f(0, 0) \neq 0$ o $g(0, 0) \neq 0$. Por lo tanto, f es una unidad o g es una unidad, con lo cual $(f, g) = (1)$, como queríamos demostrar.

a) Supongamos que f, g tienen un factor común $h \in k[x, y]$ tal que $h(0, 0) = 0$. Como $(f, g) \subset (h)$, tenemos una sobreyección $k[[x, y]]/(f, g) \to k[[x, y]]/(h)$. Basta entonces con demostrar que $\dim_k k[[x, y]]/(h) = \infty$. Como tenemos una inyección $k[x, y]/(h) \to k[[x, y]]/(h)$, basta con ver que $\dim_k k[x, y]/(h) = \infty$. Si esta dimensión fuese finita entonces los conjuntos $\{\bar{x}^n, n \in \mathbb{N}\}$ y $\{\bar{y}^m, m \in \mathbb{N}\}$ serían linealmende dependientes ($\bar{x}$, $\bar{y}$ denota clase de congruencia módulo h). Esto significa que existen polinomios $p \in k[x]$ y $q \in k[y]$ divisibles por h en $k[x, y]$. Resulta entonces que h es constante, lo cual es una contradicción.

Recíprocamente, supongamos que f y g no tienen un factor común h tal que $h(0, 0) = 0$. Queremos ver que $\dim_k k[[x, y]]/(f, g) < \infty$. Podemos suponer que f y g no tienen ningún factor común:

si tienen un factor común h entonces sabemos que $h(0,0) \neq 0$, con lo cual $h \in k[[x,y]]$ es una unidad, y podemos descartar h sin modificar el ideal $(f,g) \subset k[[x,y]]$. Sea $R = R_y(f,g) \in k[x]$ la resultante respecto a la variable y, que es no-nula debido a que f,g no tienen factor común. Entonces podemos escribir $R = ux^m \in k[[x]]$ donde $u \in k[[x]]$ es inversible y $m \in \mathbb{N}$. Por otra parte sabemos por las propiedades generales de la resultante que $R = Af + Bg$ para ciertos $A, B \in k[x,y]$. Resulta entonces que x^m pertenece al ideal $(f,g) \subset k[[x,y]]$. Repitiendo el argumento con la resultante $R_x(f,g)$ obtenemos similarmente que $y^n \in (f,g)$ para cierto $n \in \mathbb{N}$. Entonces tenemos $(x^m, y^n) \subset (f,g)$ y por lo tanto un epimorfismo $k[[x,y]]/(x^m,y^n) \to k[[x,y]]/(f,g)$. Como $\dim_k k[[x,y]]/(x^m,y^n) < \infty$ (ejercicio) resulta $\dim_k k[[x,y]]/(f,g) < \infty$, como deseábamos demostrar.

e) Consideramos la sucesión de aplicaciones k-lineales

$$0 \to k[[x,y]]/(f,g_1) \to k[[x,y]]/(f,g_1.g_2) \to k[[x,y]]/(f,g_2) \to 0$$

donde la primera función es inducida por multiplicación por g_2, y la segunda es la proyección canónica. Se verifica sin dificultad (lo dejamos como ejercicio) que esta sucesión es exacta, lo cual implica la aditividad enunciada.

g) Aquí referimos a la demostración en [9].

□

31. **Observación.** *La multiplicidad de intersección se puede calcular fácilmente utilizando solamente las propiedades del Teorema 32, mediante el sencillo algoritmo de Fulton explicado en* [9].

32. **Observación.** *La propiedad g) del Teorema también resulta de la siguiente Fórmula de Noether:*

$$(f,g;p) = \sum_{q \to p} \mu_q(f)\ \mu_q(g),$$

donde la sumatoria es sobre los puntos q próximos *a p. La definición de punto próximo depende de la noción de explosión (blow-up) de un punto de una curva. También se los denomina* lugares *(places) de la curva sobre el punto (ver* [19]*). Un enunciado preciso de esta fórmula, con sugerencia para su demostración, se puede encontrar en* [15]*, Chapter V, Exercise (3.2).*

33. **Observación.** *Otro modo de entender y de demostrar la segunda parte de la propiedad g) es la siguiente. Sin pérdida de generalidad podemos suponer que $p = 0$. La Definición 22 tiene sentido también para $f, g \in k[[x,y]]$. Dadas $f, g \in k[x,y]$ podemos factorizarlas $f = \prod_i f_i$, $g = \prod_j g_j$ como producto de irreducibles $f_i, g_j \in k[[x,y]]$, ya que $k[[x,y]]$ es de factorización única, ver 2.6. Por e), que vale con demostración similar, tenemos $(f,g;0) = \sum_{i,j}(f_i, g_j; 0)$. Es claro que $\mu(f) = \sum_i \mu(f_i)$ y $\mu(g) = \sum_j \mu(g_j)$. Por lo tanto basta con ver g) para $f, g \in k[[x,y]]$ irreducibles. Resulta de la Proposición 3 que la forma inicial de un elemento irreducible de $k[[x,y]]$ es una potencia de una forma lineal. Si f, g no tienen tangentes comunes entonces (después de un cambio lineal de variables) tenemos $f = x^r + f'$, $g = y^s + g'$ con f', g' de multiplicidades respectivas $> r$ y $> s$. Basta entonces con ver que en este caso $(f,g;0) = rs$ (ejercicio). Similarmente, si f, g tienen tangentes comunes entonces $f = x^r + f'$, $g = x^s + g'$. Suponiendo $s \geq r$ tenemos $(f,g;0) = (f, g - x^{s-r}f; 0) > rs$, utilizando f) que también es claramente válida.*

9. Variantes y generalizaciones del Teorema de Bézout.

Existen diversas variantes y generalizaciones del Teorema de Bézout: intersección de n hipersuperficies en $\mathbb{P}^n$ [16], grado de la intersección de una variedad proyectiva con una hipersuperficie [15], (I.7), intersecciones de curvas en superficies más generales que $\mathbb{P}^2$ [15], (V.1), intersecciones de variedades de Schubert en Grassmannianas [14], etc.

Otras generalizaciones se engloban en la Teoría de Intersecciones, particularmente en la teoría del Anillo de Chow y de las Clases Características. Una introducción concisa a estos temas se puede encontrar en [15], Appendix A, y en [10]. Para mayores detalles se puede consultar [8] y [11].

Referencias

[1] S. Abhyankar, *Historical ramblings in algebraic geometry and related algebra*, The American Mathematical Monthly, 1976.

[2] S. Abhyankar, *Algebraic geometry for scientists and engineers*, Mathematical Surveys and Monographs, American Mathematical Society. 1

[3] N. Bourbaki, *Algebra II, Chap. IV*, Springer-Verlag. 3, 13

[4] F. Cukierman, *Cuádricas y cúbicas*. `http://mate.dm.uba.ar/~fcukier/Teaching.htm` 11, 4.1, 7, 7.1

[5] E. Brieskorn - H. Knorrer, *Plane algebraic curves*, Springer-Verlag. 1

[6] A. Chenciner, *Courbes algébriques planes*, Springer-Verlag. 1

[7] J. Dieudonne, *Calcul infinitesimal*. 1

[8] D. Eisenbud - J. Harris, *3264 and All That*, Cambridge University Press. 9

[9] W. Fulton, *Algebraic curves*, Springer-Verlag. 1, 2.7, 5, 5, 7.1, 8, 8, 31

[10] W. Fulton, *Introduction to intersection theory in algebraic geometry*, American Mathematical Society. 5, 25, 9

[11] W. Fulton, *Intersection theory*, Springer-Verlag. 5, 25, 9

[12] I. Gelfand - M. Kapranov - A. Zelevinsky, *Discriminants, Resultants and Multidimensional Determinants*. 13

[13] E. Ghys, A singular mathematical promenade. `https://ghys.perso.math.cnrs.fr/bricabrac/promenade.pdf` 1

[14] P. Griffiths - J. Harris, *Principles of Algebraic Geometry*, Wiley. 1, 9

[15] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag. 32, 9

[16] I. Shafarevich, *Basic algebraic geometry*, 2 Vols., Springer-Verlag. 9

[17] Stacks Project Blog, `http://www.math.columbia.edu/~dejong/wordpress/` 13

[18] B. L. van der Waerden, *Algebra*, Springer-Verlag. 3

[19] R. Walker, *Algebraic curves*, Springer-Verlag. 1, 3, 3.2, 7.1, 32

[20] O. Zariski - P. Samuel, *Commutative algebra*, Springer-Verlag 2.6

Fernando Cukierman,
Universidad de Buenos Aires / CONICET,
Departamento de Matemática, FCEN,
Ciudad Universitaria,
(1428) Buenos Aires,
ARGENTINA.
fcukier@dm.uba.ar