Teorema de Bézout

Pedro Montero

Universidad Técnica Federico Santa María
Valparaíso, Chile

04 de Agosto de 2021

§49. Local versus Global (continuación)

Recuerdo

La vez anterior probamos que si $f, g \in \mathbb{C}[X,Y]$ no-constantes sin factores irreducibles comunes, entonces

$$\mathbb{C}[X,Y]/\langle f,g\rangle \xrightarrow{\sim} \bigoplus_{p\in V(f)\cap V(g)} \mathcal{O}_{\mathbb{A}^2,p}/\langle f,g\rangle$$

es un isomorfismo. En particular,

$$\dim_{\mathbb{C}}(\mathbb{C}[X,Y]/\langle f,g\rangle) = \sum_{p\in V(f)\cap V(g)} \mu_p(f,g).$$

Esto permite relacionar los números de intersección **locales** $\mu_p(f,g)$ con el objeto **global** $\mathbb{C}[X,Y]/\langle f,g\rangle$. Más aún, permite establecer la cota[1]

$$\#\{p \in V(f)\cap V(g)\} \le \dim_{\mathbb{C}} \mathbb{C}[X,Y]/\langle f,g\rangle.$$

[1] Notar que esta cota **no** toma encuenta multiplicidades (!).

Ejercicio Sean $f, g \in \mathbb{C}[X,Y]$ no-constantes, con $m = \deg(f)$ y $n = \deg(g)$, y con partes principales f_m y g_n. Supongamos que f_m y g_n no tienen factores irreducibles comunes. Probar que todo $h \in \langle f, g \rangle \subseteq \mathbb{C}[X,Y]$ de grado $d := \deg(h)$ puede escribirse como $h = af + bg$ para ciertos polinomios a, b de grados $\deg(a) \leq d - m$ y $\deg(b) \leq d - n$.

Estamos listos para enunciar el primer paso hacia el Teorema de Bézout.

Teorema

Sean $f, g \in \mathbb{C}[X,Y]$ no-constantes, con $m = \deg(f)$ y $n = \deg(g)$, y sin factores irreducibles comunes. Entonces,

1. $\dim_{\mathbb{C}}(\mathbb{C}[X,Y]/\langle f, g\rangle) \leq mn$.
2. Si las partes principales f_m y g_n no tienen factores irreducibles comunes, entonces

$$\dim_{\mathbb{C}}(\mathbb{C}[X,Y]/\langle f, g\rangle) = mn.$$

Demostración

Para todo $d \geq m + n$ consideremos la sucesión de $\mathbb{C}$-e.v. dada por[2]

$$\mathbb{C}[X,Y]_{\leq d-m} \times \mathbb{C}[X,Y]_{\leq d-n} \xrightarrow{\alpha} \mathbb{C}[X,Y]_{\leq d} \xrightarrow{\pi} \mathbb{C}[X,Y]/\langle f, g\rangle$$

donde $\alpha(a,b) := af + bg$, y donde π es la proyección al cociente.

Si $(a,b) \in \ker(\alpha)$ entonces $af = -bg$ y luego, dado que f, g no tienen factores comunes, $a = cg$ y $b = -cf$ para cierto $c \in \mathbb{C}[X,Y]_{\leq d-m-n}$. Así,

$$\ker(\alpha) = \mathbb{C}[X,Y]_{\leq d-m-n} \cdot (g, -f), \text{ con } \dim_{\mathbb{C}} \ker(\alpha) = \binom{d-m-n+2}{2}.$$

Dado que $\mathrm{Im}(\alpha) \subseteq \ker(\pi)$, tenemos que

$$\begin{aligned} \dim_{\mathbb{C}} \mathrm{Im}(\pi) &= \binom{d+2}{2} - \dim_{\mathbb{C}} \ker(\pi) \leq \binom{d+2}{2} - \dim_{\mathbb{C}} \mathrm{Im}(\alpha) \\ &= \binom{d+2}{2} - \binom{d-m+2}{2} - \binom{d-n+2}{2} + \dim_{\mathbb{C}} \ker(\alpha) = mn. \end{aligned}$$

[2] Aquí, $V_d := \mathbb{C}[X,Y]_{\leq d}$ es el e.v. de polinomios de grado $\leq d$. Así, $\dim_{\mathbb{C}}(V_d) = \binom{d+2}{2}$.

Demostración (continuación)

La cota $\dim_{\mathbb{C}} \mathrm{Im}(\pi) \leq mn$ es indep. de d (siempre que $d \geq m+n$) y luego es válida para la imagen del morfismo *sobreyectivo*

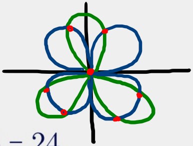
$$\pi : \mathbb{C}[X,Y] \twoheadrightarrow \mathbb{C}[X,Y]/\langle f,g\rangle,$$

i.e., $\dim_{\mathbb{C}}(\mathbb{C}[X,Y]/\langle f,g\rangle) \leq mn$.

Finalmente, basta notar que si f_m y g_n no tienen factores irreducibles comunes, entonces el Ejercicio anterior implica que $\ker(\pi) \subseteq \mathrm{Im}(\alpha)$, i.e., tenemos la igualdad $\ker(\pi) = \mathrm{Im}(\alpha)$ y por ende las desigualdades son igualdades en este caso. □

Ejemplo: La clase pasada vimos que si $f = (X^2+Y^2)^2 + 3X^2Y - Y^3$ y $g = (X^2+Y^2)^3 - 4X^2Y^2$ entonces

$$\mu_{(0,0)}(f,g) = 14.$$



Por otro lado, $\dim_{\mathbb{C}} \mathbb{C}[X,Y]/\langle f,g\rangle \leq \deg(f)\deg(g) = 4 \cdot 6 = 24.$

§50. Curvas planas proyectivas y Teorema de Bézout

Espacio proyectivo (cf. Clase 5)

Sea $n \in \mathbb{N}$. El **espacio proyectivo de dimensión** n (sobre $\mathbb{C}$), denotado $\mathbb{P}^n$, es el conjunto de rectas vectoriales en $\mathbb{C}^{n+1}$. Equivalentemente,

$$\mathbb{P}^n \stackrel{\text{def}}{=} (\mathbb{C}^{n+1} - \{0\})/\sim,$$

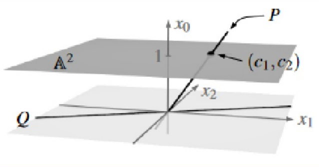
donde $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ si existe $\lambda \in \mathbb{C}^*$ tal que $x_i = \lambda y_i$ para todo $i \in \{0, \ldots, n\}$. Denotamos por $[x_0, \ldots, x_n] \in \mathbb{P}^n$ la clase de $(x_0, \ldots, x_n)$.

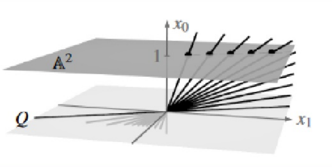
Notar que

$$\iota : \mathbb{A}^n \hookrightarrow \mathbb{P}^n, \ (x_1, \ldots, x_n) \longmapsto [1, x_1, \ldots, x_n]$$

permite ver $\mathbb{A}^n$ dentro de $\mathbb{P}^n$, y la imagen de esta inclusión coincide con

$$U_0 := \{[x_0, \ldots, x_n] \in \mathbb{P}^n \mid x_0 \neq 0\}.$$

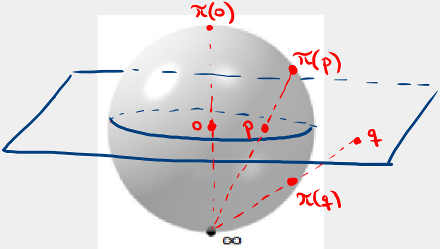




Los puntos de $H_0 := \mathbb{P}^n \setminus U_0 = \{x_0 = 0\}$ son de la forma $[0, x_1, \ldots, x_n]$ y por ende hay una biyección $H_0 \cong \mathbb{P}^{n-1}$.

Luego, $\mathbb{P}^n \overset{\text{def}}{=} U_0 \amalg H_0 \cong \mathbb{A}^n \amalg \mathbb{P}^{n-1}$, y decimos que U_0 (resp. H_0) es la **parte afín** (resp. el **hiperplano al infinito**) de $\mathbb{P}^n$.

Por ejemplo, $\mathbb{P}^1 = \mathbb{A}^1 \amalg \mathbb{P}^0 = \mathbb{A}^1 \amalg \{\infty\}$, donde $\infty := [0, 1]$.



$\mathbb{P}^1_{\mathbb{C}} = \hat{\mathbb{C}}$ (esfera de Riemann)

El plano proyectivo $\mathbb{P}^2$

Consideramos el plano proyectivo $\mathbb{P}^2$, con coordenadas $[x, y, z] \in \mathbb{P}^2$.

Dado que (x, y) denotan usualmente las coordenadas de $\mathbb{A}^2$, es que consideramos

$$\iota : \mathbb{A}^2 \hookrightarrow \mathbb{P}^2, \ (x, y) \longmapsto [x, y, 1]$$

en este caso. Así,

$$L := \{[x, y, z] \in \mathbb{P}^2 \mid z = 0\} \cong \mathbb{P}^1$$

es la **recta al infinito**.

⚠ A pesar de ser la elección más típica, también podemos elegir **cualquier** recta

$$L = \{[x, y, z] \in \mathbb{P}^2 \mid ax + by + cz = 0\}$$

y considerar $\mathbb{A}^2 \cong \mathbb{P}^2 \setminus L$ (mediante un cambio de coordenadas en $\mathrm{GL}_3(\mathbb{C})$).

Curvas planas proyectivas

Una curva plana proyectiva $C \subseteq \mathbb{P}^2$ es el lugar de ceros de un polinomio **homogéneo** no-constante $F \in \mathbb{C}[X, Y, Z]$. Explícitamente,

$$C = V(F) \stackrel{\text{def}}{=} \{[x, y, z] \in \mathbb{P}^2 \text{ tal que } F(x, y, z) = 0\}.$$

Como en el caso afín, decimos que $\deg(F)$ es el grado de la curva C.

Por ejemplo, $F = YZ - X^2$ define una curva $C = V(F)$ de grado 2.

Atención

Es importante restringirse a polinomios **homogéneos** $F \in \mathbb{C}[X, Y, Z]$ para que la ecuación "$F = 0$" esté bien definida en $\mathbb{P}^2$. En el ejemplo, si se tiene $[x, y, z] = [\lambda x, \lambda y, \lambda z]$ entonces

$$F(\lambda x, \lambda y, \lambda z) = \lambda^2(yz - x^2) = \lambda^2 F(x, y, z).$$

Hay una correspondencia biyectiva entre

$$\left\{ \begin{array}{c} \text{Polinomios de} \\ \text{grado } d \text{ en } \mathbb{C}[X,Y] \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Polinomios homogéneos de grado } d \\ \text{en } \mathbb{C}[X,Y,Z] \text{ no divisibles por } Z \end{array} \right\}$$

$$f(X,Y) = \sum_{i,j} a_{ij} X^i Y^j \longmapsto F(X,Y,Z) \stackrel{\text{def}}{:=} \sum_{i,j} a_{ij} X^i Y^j Z^{d-i-j}$$

$$f(X,Y) \stackrel{\text{def}}{:=} F(X,Y,1) \longleftarrow F(X,Y,Z)$$

Por ejemplo,

1. A $f = Y - X^2$ asociamos $F = YZ - X^2$, con $F(X,Y,1) = Y - X^2 = f$.
2. A $f = 4 + X + Y + 2X^3Y$ asociamos

$$F = 4Z^4 + XZ^3 + YZ^3 + 2X^3Y,$$

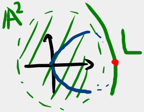
con $F(X,Y,1) = 4 + X + Y + 2X^3Y = f$.

Parte afín y Clausura proyectiva

Sea $F \in \mathbb{C}[X,Y,Z]$ homogéneo no-constante y sea $C = V(F) \subseteq \mathbb{P}^2$.

La parte afín de C es $C_a := V(f) \subseteq \mathbb{A}^2$, donde $f = F(X,Y,1)$. Equivalentemente, $C_a \cong C \cap \mathbb{A}^2$ donde $\mathbb{A} \hookrightarrow \mathbb{P}^2$. Del mismo modo, decimos que

$$C_\infty := C \cap L \overset{\text{def}}{=} \{[x,y,0] \in \mathbb{P}^2 \mid F(x,y,0) = 0\} \subseteq L \cong \mathbb{P}^1$$



son los puntos al infinito de C.

Sea $f \in \mathbb{C}[X,Y]$ no-constante y sea $C = V(f) \subseteq \mathbb{A}^2$ curva afín.

La clausura proyectiva de C es $\overline{C} := V(F) \subseteq \mathbb{P}^2$, donde F es el polinomio homogéneo asociado a f. Dado que F no es divisible por Z, $\overline{C}$ no contiene la recta al infinito L como componente, y $\overline{C}_a = C$.

Sin embargo, $\overline{C}$ puede tener $\overline{C}_\infty \neq \varnothing$. Si $f = f_0 + f_1 + \ldots + f_d$ suma de partes homogéneas, entonces $F = Z^d f_0 + Z^{d-1} f_1 + \ldots + Z f_{d-1} + f_d$ y luego

$$\overline{C}_\infty = \{[x,y,0] \in \mathbb{P}^2 \mid f_d(x,y) = 0\} \subseteq L \cong \mathbb{P}^1.$$

Sea $p \in \mathbb{P}^2$ un punto. El anillo local de $\mathbb{P}^2$ en p es

$$\mathcal{O}_{\mathbb{P}^2,p} := \left\{ \frac{F}{G} \;\middle|\; F, G \in \mathbb{C}[X,Y,Z] \text{ homogéneos del mismo grado y } G(p) \neq 0 \right\}.$$

Si $p = [x_0, y_0, 1] \in \mathbb{A}^2 \subseteq \mathbb{P}^2$, entonces $\mathcal{O}_{\mathbb{P}^2,p} \xrightarrow{\sim} \mathcal{O}_{\mathbb{A}^2,(x_0,y_0)}$, $\frac{F}{G} \mapsto \frac{F(X,Y,1)}{G(X,Y,1)}$.

El anillo $\mathcal{O}_{\mathbb{P}^2,p}$ **no** contiene $\mathbb{C}[X,Y,Z]$ como subanillo. Sin embargo, si $F_1, F_2 \in \mathbb{C}[X,Y,Z]$ son polinomios homogéneos *definimos* el ideal generado por F_1 y F_2, $\langle F_1, F_2 \rangle \subseteq \mathcal{O}_{\mathbb{P}^2,p}$, mediante

$$\langle F_1, F_2 \rangle \overset{\text{def}}{:=} \left\{ \frac{a_1}{b_1}F_1 + \frac{a_2}{b_2}F_2 \;\middle|\; a_i, b_i \text{ homogéneos con } \deg(a_iF_i) = \deg(b_i) \right\}$$

Si $p = [x_0, y_0, 1] \in \mathbb{A}^2 \subseteq \mathbb{P}^2$, el isomorfismo $\mathcal{O}_{\mathbb{P}^2,p} \xrightarrow{\sim} \mathcal{O}_{\mathbb{A}^2,(x_0,y_0)}$ envía $\langle F_1, F_2 \rangle$ en $\langle f_1, f_2 \rangle$, donde $f_i = F_i(X,Y,1)$.

Multiplicidades de intersección

Sean $F, G \in \mathbb{C}[X,Y,Z]$ homogéneos no-constantes y $p \in \mathbb{P}^2$. Definimos la multiplicidad (o número) de intersección de F y G en p mediante

$$\mu_p(F,G) := \dim_{\mathbb{C}}(\mathcal{O}_{\mathbb{P}^2,p}/\langle F,G\rangle) \in \mathbb{N} \cup \infty.$$

Si $p = [x_0, y_0, 1] \in \mathbb{A}^2 \subseteq \mathbb{P}^2$, entonces $\mu_p(F,G) = \mu_{(x_0,y_0)}(f,g)$, donde $f = F(X,Y,1)$ y $g = G(X,Y,1)$.

⚠ En la práctica, siempre podemos reducirnos al caso afín eligiendo la recta al infinito L adecuadamente. Por ejemplo:

Si $F = YZ - X^2$ y $G = Z$, entonces $p = [0,1,0] \in V(F) \cap V(G)$. Escogemos $L = \{y = 0\}$, con parte afín $\mathbb{A}^2 \cong \{y = 1\} \subseteq \mathbb{P}^2$ con coordenadas (x,z). Luego, tenemos $F \mapsto f = Z - X^2$, $G \mapsto g = Z$ y $p \mapsto (0,0)$, de donde:

$$\mu_p(F,G) = \mu_{(0,0)}(Z - X^2, Z) = 2.$$

Teorema de Bézout

Teorema (Étienne Bézout, 1779)

Sean $F, G \in \mathbb{C}[X,Y,Z]$ homogéneos no-constantes sin factores irreducibles comunes. Entonces,

$$\sum_{p \in V(F) \cap V(G)} \mu_p(F,G) = \deg(F) \cdot \deg(G).$$

Demostración: Sean $f = F(X,Y,1)$ y $g = G(X,Y,1)$. Sea $q \in \mathbb{A}^2 \subseteq \mathbb{P}^2$ un punto tal que $q \notin V(f) \cup V(g)$, i.e., $f(q)g(q) \neq 0$.

Dado que $\Gamma := V(F) \cap V(G)$ es un conjunto finito, podemos considerar una recta $L \subseteq \mathbb{P}^2$ que pase por q y que no intersecte Γ.

Haciendo un cambio de coordenadas en $\mathrm{GL}_3(\mathbb{C})$, podemos asumir que $L = \{z = 0\}$ es la recta al infinito. En particular, tenemos $\deg(f) = \deg(F) := n$, $\deg(g) = \deg(G) := m$ y $\Gamma \subseteq \mathbb{A}^2 \subseteq \mathbb{P}^2$ coincide con $V(f) \cap V(g) \subseteq \mathbb{A}^2$.

Demostración (continuación)

El Teorema del comienzo de hoy implica que

$$\sum_{p\in V(F)\cap V(G)} \mu_p(F,G) = \sum_{p\in V(f)\cap V(g)} \mu_p(f,g) = \dim_{\mathbb{C}}(\mathbb{C}[X,Y]/\langle f,g\rangle \leq mn$$

Más aún, notar que todo polinomio homogéneo en **dos** variables se puede factorizar: si $H(X,Y)$ es de grado d, entonces $H(X,Y) = Y^d H(X/Y,1)$ y el polinomio $h(T) := H(T,1) = a(T-\lambda_1)\cdots(T-\lambda_r)$ se factoriza. Luego,

$$H(X,Y) = aY^{d-r}(X-\lambda_1 Y)\cdots(X-\lambda_r Y).$$

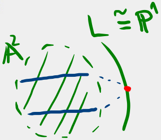
Aplicando esto a las partes principales $f_n(X,Y)$ y $g_m(X,Y)$, tenemos que los factores lineales corresponden a los puntos $\overline{V(f)}_\infty = V(F)\cap L$ y $\overline{V(g)}_\infty = V(G)\cap L$ al infinito.

La elección de L nos dice entonces que f_n y g_m no tienen factores comunes, y por ende $\sum_{p\in V(F)\cap V(G)} \mu_p(F,G) = mn$. $\square$

Ejemplo (todas las rectas se intersectan)

Sean $F, G \in \mathbb{C}[X, Y, Z]$ polinomios homogéneos de grado 1. El Teorema de Bézout implica que $V(F) \cap V(G)$ consiste en un **único** punto, i.e., todas las rectas en $\mathbb{P}^2$ se intersectan (!).

Por ejemplo, si consideramos en $\mathbb{A}^2$ las rectas afines paralelas



$$f = aX + bY + c \quad \text{y} \quad g = aX + bY + d,$$

con $c \neq d$. Entonces $V(f) \cap V(g) = \varnothing$ en $\mathbb{A}^2$.

Sin embargo, si consideramos las clausuras proyectivas dadas por las curvas $V(F) \subseteq \mathbb{P}^2$ y $V(G) \subseteq \mathbb{P}^2$, donde

$$F = aX + bY + cZ \quad \text{y} \quad G = aX + bY + dZ,$$

entonces $V(F) \cap V(G) = \{[-b, a, 0]\}$.

Ejemplo (dos curvas afines)

Sean $f = X + Y^2$ y $g = X + Y^2 - X^3$.

Las curvas afines $V(f) \subseteq \mathbb{A}^2$ y $V(g) \subseteq \mathbb{A}^2$ se intersectan en $p = (0,0)$. Más aún,

$$\mu_p(f,g) = \mu_p(f,-X^3) = 3\mu_p(f,X) = 3 \cdot 2 = 6.$$

Por otra parte, el Teorema de Bézout implica que si

$$F = XZ + Y^2 \quad \text{y} \quad G = XZ^2 + Y^2 Z - X^3,$$

entonces $\sum_{p \in V(F) \cap V(G)} \mu_p(F,G) = 2 \cdot 3 = 6$. En particular, deducimos que F y G no poseen puntos de intersección en la recta al infinito.

Esto último se puede verificar directamente: dado que $F(X,Y,0) = Y^2$ y $G(X,Y,0) = -X^3$, tendríamos que $V(F) \cap V(G) \cap L$ sería $[0,0,0] \notin \mathbb{P}^2$.

Comentarios finales

Comentarios

- Hay muchas aplicaciones del álgebra (abstracta) a situaciones concretas fuera de la matemática (notablemente física, química, y ciencias de la computación).
- En matemáticas, también les permitirá tener un lenguaje común (y muy eficiente) para plantear y resolver diversos problemas.
- La geometría algebraica se interesa en estudiar las variedades algebraicas más generales, y resolver problemas de geometría (resp. de álgebra) utilizando técnicas algebraicas (resp. geométricas).

Nos vemos en MAT426 ☺