Apuntes de los días 03/10 - 10/10 - 13/10

1. CURVAS ALGEBRAICAS Y SUS ECUACIONES

Antes de continuar con el estudio del plano proyectivo y en particular, con el estudio de las curvas algebraicas en el plano proyectivo, veremos algunos resultados acerca de las posibles ecuaciones que se definen a una curva algebráica en $\mathbb{C}^2$

Definición 1.1. Un subconjunto $\mathcal{C} \in \mathbb{C}^2$, se le llama una *curva algebráica afín* si existe un polinomio $f(x, y) \in \mathbb{C}[x, y]$ tal que $grad(f) \geq 1$ y $\mathcal{C} = V_{\mathbb{C}} = \{(a, b) \in \mathbb{C}^2 | f(a, b) = 0\}$ $(V = variedad)$ ♦

Es decir un subconjunto de $\mathbb{C}^2$ será llamado una *curva algebraica afín* si es el conjunto de ceros de un polinomio no constante en $\mathbb{C}[x, y]$.
Observe, que por ejemplo

$$\mathbb{C}_1 := V_{\mathbb{C}}(x^2 + y^2) \quad \text{y} \quad \mathbb{C}_2 := V_{\mathbb{C}}\left((x^2 + y^2)^2\right)$$

definen el mismo conjunto de puntos en $\mathbb{C}^2$, pero los polinomios que definen a $\mathbb{C}_1$ y $\mathbb{C}_2$ son diferentes.
Más generalmente, es fácil verificar que si $f(x, y) \in \mathbb{C}[x, y]$, entonces

$$V_{\mathbb{C}}(f) = V_{\mathbb{C}}(\alpha f) = V_{\mathbb{C}}(f^n)$$

para todo $\alpha \in \mathbb{C}^* := \mathbb{C} \setminus \{0\}$ y $n \in \mathbb{Z}_{\geq 1}$.
Esto nos muestra que en general una curva algebraica afín puede ser definida por una infinidad de polinomios, y por ende la ecuación polinomial que la define no es única.

Veremos, sin embargo, que en esencia, las posibilidades listadas anteriormente son las únicas que se pueden dar.

Hemos visto que no obstante, sobre los números reales la situación no se puede controlar de esta manera, pues por ejemplo
$V_{\mathbb{R}}(x^2 + y^2 + 1) = \emptyset = V_{\mathbb{R}}(y^2 + 1)$ pero no existe constante $\alpha \in \mathbb{C}^*$ y $n \in \mathbb{Z}_{\geq 1}$ tal que $\alpha(x^2 + y^2 + 1)^n = y^2 + 1$
Nos concentraremos entonces de momento en trabajar sobre los números complejos y por lo tanto escribimos $V(f)$ en lugar de $V_{\mathbb{C}}(f)$ de ahora en adelante.

Sobre $\mathbb{C}$ una curva algebraica afín pasa a ser un conjunto de puntos en $\mathbb{C}^2 = \mathbb{R}^4$.

Esto causa que se pierda la posibilidad de visualizar las curvas algebraicas afines en $\mathbb{C}^2$ como si se puede hacer en $\mathbb{R}^2$.

Sin embargo, desde el punto de vista topológico las curvas algebraicas en $\mathbb{C}^2$ corresponden a superficies (vistas sobre $\mathbb{R}$) de naturaleza "relativamente simple", llamadas esferas con "agarraderas" o "manijas" (en inglés, spheres with n-handles).

Para poder obtener este punto de vista se debe trabajar sobre el espacio proyectivo de $\mathbb{P}^2_{\mathbb{C}}$ lo cual causa que se agreguen puntos en el infinito a las curvas algebráicas afines. Algunos ejemplos, son los siguientes:

FIGURA 1. Ejemplos de varias curvas reales y complejas con puntos en el infinito.

$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, (Elipse)

$y^2 = x^3 + x^2 - x + 1$, (curva elíptica)

$y^2 = x^3 - x$, (curva elíptica)

$y^2 = x^3 + x^2$, (cúbica nodal)

$y^2 = x^3$, (cúbica cuspidal)

$x^4 + y^4 = 1$, (curva de Fermat con $n = 4$)

Debe advertirse que a pesar de que estas figuras representan a la curva algebráica compleja dada desde un punto de vista topológico, éstas no representan la manera en la que cada curva se encuentra dentro de $\mathbb{C}^2 = \mathbb{R}^4$.

Por otro lado, los puntos denotados por ∞ ó ∞_i en las figuras corresponden a los puntos en el infinito que se agregan a cada curva afín cuando se consideran dentro del plano proyectivo $\mathbb{P}^2_{\mathbb{C}}$.

Volvemos ahora a considerar el problema de las posibles ecuaciones que definen a una curva algebráica afín en $\mathbb{C}^2$

Observe que si $f(x,y), g(x,y) \in \mathbb{C}[x,y]$ son polinomios no constantes y f divide a g, i.e, existe un polinomio $h(x,y) \in \mathbb{C}[x,y]$ tal que $g = f \cdot h$, entonces $V(f) \subset V(g)$ pues todo cero $(a,b) \in \mathbb{C}^2$ de $f(x,y)$ también es un cero de $g(x,y)$.

Esto muestra que si $\mathcal{C}_1 := V(f)$ y $\mathcal{C}_2 := V(g)$ y $f|g$, entonces $\mathcal{C}_1 \subset \mathcal{C}_2$, i.e, $\mathcal{C}_1$ es una "subcurva" de $\mathcal{C}_2$

Sorpendentemente, a diferencia de la situación en los núumeros reales, donde por ejemplo

$$\emptyset = V_{\mathbb{R}}(x^2 + y^2 + 1) \subset V_{\mathbb{R}}(y) = \text{eje x}$$

pero claramente $x^2+y^2+1 \not| y$, en los números complejos se cumple el inverso del hecho anterior.

Este resultado se puede ver como un precursor del famoso teorema conocido como el Nullstellensatz de Hilbert.

Lema 1.2 (Lema de Study)**.** *Sea $f, g \in \mathbb{C}[x,y]$ con f inrreducible de $grado(f) \geq 1$. Entonces si $V(f) \subset V(g)$, se tiene que $f|g$*

La demostración la veremos más adelante.

Como consecuencia sencilla del lema de Stady, podemos demostrar que ninguna curva algebráica en $\mathbb{C}^2$ es vacía, cosa que vimos si ocurre en $\mathbb{R}^2$

Este colorario es una versión débil del Nullstellensatz

Corolario 1.3. *Sea $f \in \mathbb{C}[x,y]$ un polinomio con $grado(f) \neq 0$. Entonces, $V_{\mathbb{C}}(f) \neq \emptyset$*

Demostración. Supongamos por contradicción que $V_{\mathbb{C}}(f) = \emptyset$. Entonces $V_{\mathbb{C}}(f) \subset V_{\mathbb{C}}(g)$, para todo $g \in \mathbb{C}[x,y]$

Como $\mathbb{C}[x,y]$ es un anillo de factorización única entonces f siempre tiene al menos un factor irreducible.

Hay dos casos:

1. Si $f \equiv 0 \in \mathbb{C}[x,y]$, cualquier polinomio irreducible h divide a f
2. Si $grado(f) \geq 1$, por el teorema de factorización única, f tiene al menos un factor irreducible h

Entonces tenemos que $\emptyset = V_{\mathbb{C}}(h) \subset V_{\mathbb{C}}(f) \subset V_{\mathbb{C}}(g)$. Por el lema de Study esto implica que $h|g \ \forall g \in \mathbb{C}[x,y]$ y esto es una contradicción. ☐

Corolario 1.4. *Colorario: Si $\mathbb{C}$ es una curva algebraica afín en $\mathbb{C}^2$, estonces $\mathbb{C} \neq \emptyset$*

Posponemos la demostración del Lema de Study para después, ya que requerimos desarrollar un poco de la teoría básica sobre resultantes primero.

Por ahora, continuaremos la investigación de las posibles ecuaciones que definen a una curva algebraica afín.

Hemos visto antes que cada factor g de un polinomio $f \in \mathbb{C}[x,y]$ define una subcurva $V(f) \subset V(g)$.

Estudiaremos esto de una forma más completa haciendo uso del hecho que $\mathbb{C}[x,y]$ es lo que se conoce como un dominio de factorización única. (u.f.d.)

Entonces sea $f \in \mathbb{C}[x,y]$ de $grado \geq 1$. Sabemos que existen polinomios irreducibles $f_1,\ldots,f_r \in \mathbb{C}[x,y]$ tal que $f = f_1^{k_1}\cdots f_r^{k_r}$ para algunos enteros $k_1,\ldots,k_r \in \mathbb{Z}_{\geq 1}$

Esta factorización es única salvo por el orden de los factores irreducibles f_j por la posible multiplicación por constantes.

Entonces, se puede ver que:

$$V(f) = V(f_1)\cup\ldots\cup V(f_r)$$

Ejercicio: demostrar que $\subseteq$ y $\supseteq$

Es decir, que la curva algebraica $V(f)$ se puede descomponer como una unión de componentes $V(f_j)$.

Definición 1.5. Una curva algebraica $\mathbb{C} \subset \mathbb{C}^2$ es *reducible* si existen curvas $\mathcal{C}_1$ y $\mathcal{C}_2$ tal que $\mathcal{C}_1 \neq \mathcal{C}_2$ y $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$

Decimos que una curva algebraica afín $\mathcal{C}$ es irreducible si no es reducible, i.e, dada una descomposición $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ se debe tener que $\mathcal{C}_1 = \mathcal{C}_2$ ⧫

Ejemplo 1.6. Sea $f(x,y) = x^2 - y^2$, entonces $V_f = V(x-y)\cup V(x+y)$ pues $f = x^2 - y^2 = (x-y)(x+y)$, i.e, V_f es reducible pues $V(x-y) \neq V(x+y)$ (son diferentes por ejemplo porque $(1,1) \in V(x-y)$ pero $(1,1) \notin V(x+y)$). $\diamond$

La definición de reducible o irreducible para una curva algebraica es un concepto paramétrico. Ahora veremos a que equivale esto desde un punto de vista algebraico.

Lema 1.7. *Una curva algebraica $\mathbb{C} := V(f) \subset \mathbb{C}^2$ es irreducible sii existe $k \in \mathbb{Z}_{\geq 1}$ y un polinomio irreducible $g \in \mathbb{C}[x,y]$ tal que $f = g^k$*

Demostración. $\Rightarrow$)
Supongamos que $\mathbb{C} = V(f)$ irreducible.

Sea $f = f_1^{\Re_1}\cdots f_r^{\Re_r}$ la factorización de f en términos de irreducibles en $\mathbb{C}[x,y]$.

Queremos demostrar que $r = 1$. Supongamos por contradicción que $r \geq 2$. Sabemos que $f_i \not| f_j$, $\forall i \neq j$.

Sean $h_1 := f_1\cdots f_{r-1}$ y $h_2 := f_r$

Luego, $h_2 \not| h_1$. Sin embargo tenemos que: $V(h_1) = V(f_1)\cup\ldots\cup V(f_{r-1})$ y $V(h_2) = V(f_r)$ así que $\mathbb{C} = V(f) = V(h_1)\cup V(h_2)$

Para contradecir la irreducibilidad de $\mathbb{C}$, queremos mostrar que $V(h_1) \neq V(h_2)$

Si se tuviera $V(h_1) = V(h_2)$, entonces se tendrá que $V(f_1) \subset V(h_1) = V(h_2)$ y por el Lema de Study se tendrá que $f_1|(h_2 = f_r)$ y esto es imposible. Por lo tanto debe tenerse $V(h_1) \neq V(h_2)$ y entonces esto contradice la irreducibilidad de $\mathbb{C}$

Por ende $r = 1$ y tenemos

$$f = f_1^{k_1} = g^k \text{ con } g := f_1, \;\; k := k_1$$

($\Leftarrow$) Por contrapositiva
Supongamos que $\mathbb{C}$ es reducible, i.e, que $\mathbb{C} = V(f) = V(h_1)\cup V(h_2)$ para $h_1,h_2 \in \mathbb{C}[x,y]$ con $V(h_1) \neq V(h_2)$

Sean f_1 y f_2 factores irreducibles de h_1 y h_2 respectivamente, tal que no existe una constante $c \in \mathbb{C}^x$ tal que $h_1 = ch_2$ (si no existieran tales factores, se tendría que $V(h_1) = v(h_2)$). Esto implica que $f_1 \not| f_2$ y $f_2 \not| f_1$. Luego, como
$V(f_i) \subseteq V(h_i) \subseteq V(f)$, por el Lema de Study vemos que $f_1|f$ y $f_2|f$, por lo que f tiene al menos dos factores irreducibles distintos y no asociable (no se cumple $f = g^k$). □

Teorema 1.8. *Toda curva algrebraica afín $\mathcal{C} \subset \mathbb{C}^2$ admite una descomposición $\mathcal{C} = \mathcal{C}_1\cup\ldots\cup\mathcal{C}_r$ donde $\mathcal{C}_1,\ldots,\mathcal{C}_r$ son curvas algebraicas irreducibles.*

Esta representación es única salvo posiblemente por el orden en que ocurren los $\mathcal{C}_j$

Demostración. Existencia: Sea $\mathcal{C} = V(f)$, Sea $f = f_1^{k_1} \cdots f_r^{k_r}$ una factorización de f como producto de irreducibles en $\mathbb{C}[x, y]$. Entonces, si $\mathcal{C}_i := V(f_i)$, se tiene que $\mathcal{C} = \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_r$.

Además por el lema anterior, $\mathcal{C}_i$ es irreducible pues f_i lo es.

Unicidad: Supongamos por contradicción que $\mathcal{C} = \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_r = \mathcal{C} = \mathcal{C'}_1 \cup \ldots \cup \mathcal{C'}_s$ son dos descomposiciones diferentes de $\mathcal{C}$ en componentes irreducibles.

Sea $f_1, \ldots, f_r \in \mathbb{C}[x, y]$ polinomios irreducibles tal que $\mathcal{C}_i = V(f_i)$ para $i = 1, \ldots, r$. De igual modo, sean $g_1, \ldots, g_s \in \mathbb{C}[x, y]$ polinomios irreducibles tal que

$$\mathcal{C'}_j = V(g_j), \text{ para } j = 1, \ldots, s$$

Como estamos suponiendo que las descomposiciones son diferentes, podemos asumir sin pérdida de generalidad que $\mathcal{C'}_s \neq \mathcal{C}_i$ para $i = 1, \ldots, r$

Luego como $V(g_s) = \mathcal{C'}_s \subseteq \mathcal{C} = V\left(f_1^{k_1} \cdots f_r^{k_r}\right)$ el Lema de Study implica que $g_s| \left(f_1^{k_1} \cdots f_r^{\Re_r}\right)$, es decir que $g_s|f_i$ para algún $i_s \in \{1, \ldots, r\}$ (por la irreducibilidad de g_s) .
Sin embargo, como ambos son irreducibles, debe existir una constante $c \in \mathbb{C}^x$ tal que $g_s = c \cdot f_{i_s}$

Pero esto implica que

$$\mathcal{C'}_s = V(g_s) = V(c \cdot f_{i_s} = V(f_{i_s}) = \mathcal{C}_{i_s}$$

y esto es una contradicción. □

Definición 1.9. Las subcurvas $\mathcal{C}_i$ en la descomposición

$$\mathcal{C} = \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_r$$

se llaman las *componentes irreducibles* de $\mathcal{C}$ ♦

Se puede pensar en la descomposición

$$\mathcal{C} = \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_r$$

en componentes irreducibles como un análogo de la descomposición de un espacio topológico en componentes conexos.

Más aún , se puede demostrar lo siguiente.

Teorema 1.10. *Toda curva algebraica irreducible $\mathcal{C} \subset \mathbb{C}^2$ es conexa como un espacio topológico.*

Nota: todos estos resultados son falsos sobre los números reales.

Así como los componentes irreducibles de una curva algebraica son únicos, veremos como consecuencia del Lema de Study, esto a su vez determina los posibles factores irreducibles de un polinomio de definición para la curva algebraica.

Corolario 1.11. *Sea $\mathcal{C} := V(f) \subset \mathbb{C}^2$ una curva algebraica afín sea $f = f_1^{k_1} \ldots f_r^{k_r}$, la factorización en irreducibles de f.*

Si $\mathcal{C} = V(g)$ para algún otro polinomio $g \in \mathbb{C}[x, y]$ entonces $g = \lambda f_1^{\ell_1} \cdots f_r^{\ell_r}$ para algunos $\lambda \in \mathbb{C}^x$ y $\ell_1, \ldots \ell_r \in \mathbb{Z}_{\geq 1}$

Ejercicio: Demostrar este corolario, usar el lema de $f = g^k$)

Definición 1.12. Sea $\mathcal{C} = V(f) \in \mathbb{C}^2$ una curva algebraica afín y sea $f = f_1^{k_1} \cdots f_r^{k_r}$ una factorización irreducible de f. Entonces decimos que

$$f_{\mathcal{C}} := f_1 \cdots f_r$$

es un *polinomio minimal* para la curva $\mathcal{C}$ ♦

Por el corolario anterior este polinomio es único salvo por la multiplicación por constantes.

Ejemplo 1.13. Sea $\mathcal{C} = V(y^2 - x^3 + x) \subset \mathbb{C}^2$. El conjunto de ceros reales de esta curva es

FIGURA 2. Ceros reales de $y^2 - x^3 + x$.

Esta es una curva elíptica con dos componentes reales como ya hemos visto ateriormente.

Sea $f := y^2 - x^3 + x \in \mathbb{C}^2$. Veamos que f es irreducible en $\mathbb{C}[x, y]$. Para ver esto, consideremos f como un polinomio en $\mathbb{C}[x][y]$. Supongamos por contradicción que se factoriza como un producto de dos polinomios en $\mathbb{C}[x][y]$ de menor grado (en y).

Entonces, deben existir polinomios $a_1(x),\ a_2(x),\ b_1(x),\ b_2(x) \in \mathbb{C}[x]$ tal que $y^2 - x^3 + x = (a_1(x)y + b_1(x)) \cdot (a_2(x)y + b_2(x))$

Esto implica que $a_1(x) \cdot a_2(x) = 1$ comparando los coeficientes de y^2 . Esto quiere decir que, $a_1(x) = a_1 = constante$ y $a_2(x) = a_2 = constante$ y además $a_1 \cdot a_2 = 1 \Rightarrow a_2 = \frac{1}{a_1}$

Entonces la factorización toma la forma $y^2 - x^3 + x = (a_1(x)y + b_1(x)) \cdot (a_2(x)y + b_2(x))$ y factorizando estas constantes obtenemos $(a_1 y + b_1(x)) \cdot \left(\frac{1}{a_1} y + b_2(x)\right) = a_1 \cdot \frac{1}{a_1} \left(y + \frac{b_1(x)}{a_1}\right) \cdot (y + a_1 b_2(x))$

Por ende, podemos definir $\tilde{b}_1(x) := \frac{b_1(x)}{a_1}$ y $\tilde{b}_2(x) := a_1 b_2(x)$ y entonces la factorización toma forma $y^2 - x^3 + x = \left(y + \tilde{b}_1(x)\right) \cdot \left(y + \tilde{b}_2(x)\right)$

En general, este mismo argumento se puede llevar a cabo con polinomios mónicos de mayor grado y es común asumir sin pérdida de generalidad que los factores en una posible factorización son también mónicos (Ejercicio).

Entonces deben cumplirse las ecuaciones

$$\begin{cases} \tilde{b}_1(x) + \tilde{b}_2(x) = 0 \Rightarrow \tilde{b}_2(x) = -\tilde{b}_1(x) \\ \tilde{b}_1(x) \cdot \tilde{b}_2(x) = -x^3 + x \end{cases}$$

Sustituyendo esto en la 2º ecuación obtenermos

$-\tilde{b}_1^2 = -x^3 + x$

$\Rightarrow \quad \tilde{b}_1^2 = x^3 - x = x(x-1)(x+1)$

Esta última ecuación es imposible en $\mathbb{C}[x]$ y por lo tanto tenemos una contradicción y $f = y^2 - x^3 + x$ es irreducible, $f_{\mathcal{C}} := f$ es un polinomio minimal para la curva elíptica $\mathcal{C}$ $\diamond$

Si una curva $\mathcal{C}$ no está descrita por un polinomio minimal, es decir , si

$$\mathcal{C} = V(f),\ \text{con } f = f_1^{k_1} \cdots f_r^{k_r}$$

la factorización en irreducibles de f y al menos un exponente k_i satisface que $k_i > 1$, entonces podemos considerar los exponentes k_i como multiplicidad del componente irreducible correspondiente $\mathcal{C}_i = V(f_i)$

Definición 1.14. Decimos que una suma formal $\mathcal{D} := k_1\mathcal{C}_1 + \cdots + k_r\mathcal{C}_r$ de curvas algebraicas irreducibles $\mathcal{C}_1, \cdots, \mathcal{C}_r \subset \mathbb{C}^2$ con $k_1, \cdots, k_r \in \mathbb{Z}$ es un *divisor*. Además, si cada coeficiente $k_i \geq 0$, decimos que $\mathcal{D}$ es un *divisor efectivo*. ⧫

Ejemplo 1.15. Sea $\mathcal{C} = v(x^2y^3(y^2 - x^2)) \subset \mathbb{C}^2$

La factorización de irreducibles de

$f := x^2y^3(y^2 - x^2)$

$f = f_1^2 \cdot f_2^3 \cdot f_3 \cdot f_4$

Con $f_1 = x$, $f_2 = y$, $f_3 = y - x$, $f_4 = y + x$

Acá tendríamos $k_1 = 2, k_2 = 3, k_3 = 1 = k_4$

Entonces el polinomio $f = f_1^2 \cdot f_2^3 \cdot f_3 \cdot f_4$ tendrá asociado el divisor efectivo

v $\mathcal{D} = 2V(f_1) + 3V(f_2) + 1V(f_3) + 1V(f_4) = 2V(x) + 3V(y) + 1V(y - x) + 1V(y + x)$ $\diamond$

Ejemplo 1.16. De manera similar, una factorización como $f = \frac{x^2(y+x)}{y^3(y-x)}$ determina el divisor (no efectivo) $\mathcal{D} = 2V(x) - 3V(y) + 1V(y + x) - 1V(y - x)$ $\diamond$

Utilizando el polinomio minimal podemos definir uno de los inveriantes más importantes de una curva algebraica, conocido como su grado.

Definición 1.17. Sea $\mathcal{C} := V(f) \subset \mathbb{C}^2$ una curva algebraica afín y supongamos que $f_{\mathcal{C}}$ es un polinomio minimal para $\mathcal{C}$.
Entonces definimos el *grado* de la curva $\mathcal{C}$ como $\mathrm{grad}(\mathcal{C}) := \mathrm{grad}(f_{\mathcal{C}})$

Si f no es un polinomio minimal para $\mathcal{C}$, decimos que el grado de f es el grado del divisor determinado por f.

♦

Ejemplo 1.18.

a) La cúbica espiral $\mathcal{C} = V(y^2 - x^3)$ es una curva algebraica de grado 3 pues $y^2 - x^3$ es un polinomio minimal para $\mathcal{C}$
b) La cúbica nodal $\mathcal{C} = V(y^2 - x^3 + x^2)$ es una curva algebraica de grado 3 pues $y^2 - x^3 + x^2$ es un polinomio minimal para $\mathcal{C}$
c) La hipérbola $\mathcal{C} = V(y^2 - x^2 - 1)$ es una curva algebraica de grado 2 pues $y^2 - x^2 - 1$ es un polinomio minimal para $\mathcal{C}$.

◇

La noción de grado de una curva nos permite formalizar el método discutido en el principio que a veces permite demostrar que ciertas curvas en $\mathbb{R}^2$ o en $\mathbb{C}^2$ no son algebraicas.
Éste método consiste en intersecar la curva dada con una recta. Más específicamente, sea $l \subset k^2$ con $k \in \{\mathbb{R}, \mathbb{C}\}$. Entonces l está dada por una parametrización:

$$\varphi : k \to l \subset k^2$$
$$t \mapsto (\varphi_1(t), \varphi_2(t))$$

Donde $\varphi_1, \varphi_2 \in k[T]$ son polinomios lineales, es decir $\varphi_i(T) = \alpha_i T + \beta_i$ con $\alpha_i, \beta_i \in k$ para $i = 1, 2$. Sea $\mathcal{C} := V_k(f) \subset k^2$ una curva algebraica, con $f \in k[x, y]$. Entonces los puntos de intersección de la curva con la recta son:

$$\begin{aligned}\mathcal{C} \cap l &= \{(a, b) \in k^2 \mid f(a, b) = 0 \text{ y existe } t \text{ tal que } (a, b) = (\varphi_1(t), \varphi_2(t))\} \\ &= \{(\varphi_1(t), \varphi_2(t)) \in K^2 \mid t \in k^2 \text{ y } f(\varphi_1(t), \varphi_2(t)) = 0\}\end{aligned}$$

Si definimos el polinomio

$$g(T) := f(\varphi_1(t), \varphi_2(t)) \in k[T]$$

Entonces tenemos que:

$$\mathcal{C} \cap l = \{(\varphi_1(t), \varphi_2(t)) \in k^2 \mid t \in k^2 \text{ y } g(t) = 0\}$$

Es decir, los puntos de intersección de la curva $\mathcal{C}$ con la recta l corresponden a los ceros en k del polinomio $g(T)$.

Lema 1.19. *La recta l está contenida en $\mathcal{C}$ si y sólo si $g(T)$ es el polinomio cero.*

Demostración. ($\Leftarrow$): Es trivial.
($\Rightarrow$): Si $l \subseteq \mathcal{C}$ entonces $g(t) = 0$ para todo $t \in k$ y como k es un cuerpo infinito debe tenerse que $g(T) \equiv 0 \in k(T)$. □

Por otro lado, note que como $\varphi_i(T)$ para $i = 1, 2$ son polinomios lineales entonces

$$\mathrm{grad}(g(T)) = \mathrm{grad}(f((\varphi_1(T), \varphi_2(T))) \leq \mathrm{grad}(f(x, y)).$$

En efecto dicha desigualdad puede ser estricta, por ejemplo si $f(x, y) = x - y$ y $\varphi_1(T) = \varphi_2(T) = T$ entonces $g(T) = f(T, T) = T - T = 0$.
La desigualdad anterior nos da el siguiente resultado:

Proposición 1.20. *Sea $\mathcal{C} \subseteq \mathbb{C}^2$ una curva algebraica de grado n y se $l \subset \mathbb{C}^2$ una recta no contenida en $\mathcal{C}$, entonces:*

$$\#(\mathcal{C} \cap l) \leq n$$

Donde $\#(A)$ denota la cardinalidad del conjunto A. De igual manera podemos enunciar una versión sobre $\mathbb{R}^2$:

Proposición 1.21. *Sea $\mathcal{C} = V_{\mathbb{R}}(f) \subseteq \mathbb{R}^2$ una curva algebraica y sea $l \subseteq \mathbb{R}^2$ una recta no contenida en $\mathcal{C}$. Entonces*

$$\#(\mathcal{C} \cap l) \leq \operatorname{grad}(f)$$

Dada una recta $l \subset k^2$ con $k \in \{\mathbb{R}, \mathbb{C}\}$ con parametrización:

$$\varphi : k \to l \subset k^2$$
$$t \mapsto (\varphi_1(t), \varphi_2(t))$$

con $\varphi_i \in k[T]$ dadas por $\varphi_i(T)\alpha_i T + \beta_i$ con $\alpha_i, \beta_i \in k$ para $i = 1, 2$, podemos caracterizar los polinomios $f(x, y) \in k[x, y]$ tales que $\operatorname{grad}(f(\varphi_1(T), \varphi_2(T))) < \operatorname{grad}(f(x, y))$ de la siguiente manera:
Sea $n = \operatorname{grad}(f(x, y))$. Entonces f se descompone como una suma de polinomios homogéneos de grado menor o igual a n de forma explícita como

$$f = \sum_{(i)} a_{(i)} x^{i_1} y^{i_2} = f_{(0)} + \cdots + f_{(n)}$$

Donde

$$f_{(j)} = \sum_{(i), i_1 + i_2 = j} a_{(i)} x^{i_1} y^{i_2} = \sum_{k=0}^{j} a_{j-k,k} x^{j-k} y^k$$

De manera que

$$\operatorname{grad}(f(\varphi_1(T), \varphi_2(T)) = \max\{\operatorname{grad}(f_{(j)}(\varphi_1(T), \varphi_2(T))) \mid j = 0, \cdots n$$

En particular observe que

$$\operatorname{grad}(f_{(j)}(\varphi_1(T), \varphi_2(T))) = j \Leftrightarrow f_{(j)}(\alpha_1, \alpha_2) \neq 0$$

Pues en efecto se tiene que

$$f_{(j)}(\varphi_1(T), \varphi_2(T)) = f_{(j)}(\alpha_1 T + \beta_1, \alpha_2 T + \beta_2) =$$
$$\sum_{k=0}^{j} a_{j-k,k} (\alpha_1 T + \beta_1)^{j-k} (\alpha_2 T + \beta_2)^k =$$
$$\left(\sum_{k=0}^{j} a_{j-k,k} \alpha_1^{j-k} \alpha_2^k T^j \right) + \text{ términos de menor grado.}$$

Entonces podemos concluir que los polinomios $f(x, y) \in k[x, y]$ tales que $\operatorname{grad}(f(\varphi_1(T), \varphi_2(T))) < \operatorname{grad}(f(x, y))$ son los polinomios para los cuales $f_{(n)}(\alpha_1, \alpha_2) = 0$.

Ejemplo 1.22. Veamos que el gráfico en $\mathbb{R}^2$ de la funcion $\sin x$ no es una curva algebraica en $\mathbb{R}^2$. Éste gráfico es el conjunto $\mathcal{G}_{\sin x} = \{(x, y) \in \mathbb{R}^2 \mid y = \sin x\}$, como se ve en la siguiente figura:

FIGURA 3. Gráfico de la funcion $y = \sin x$ en $\mathbb{R}^2$.

Supongamos por contradicción que $\mathcal{G}_{\sin x}$ es una curva algebraica, es decir, que existe $f(x, y) \in \mathbb{R}[x, y]$ con $\mathcal{G}_{\sin x} = V_{\mathbb{R}}(f)$. Sea $n = \operatorname{grad}(f) \geq 1$ (no puede ser el polinomio cero porque sería todo el plano y no puede ser constante porque no tendría al cero). Si l es el eje x entonces l no está contenida en $V_{\mathbb{R}}(f)$ pues claramente $l \not\subseteq \mathcal{G}_{\sin x}$. Sin embargo:

$$l \cap V_{\mathbb{R}}(f) = l \cap \mathcal{G}_{\sin x} = \{(k\pi, 0) \mid k \in \mathbb{Z}\}$$

Y como $\#(l \cap V_{\mathbb{R}}(f)) = \infty$ esto es una contradicción pues demostramos antes que $\#(l \cap V_{\mathbb{R}}(f)) \leq n$. De manera que $\mathcal{G}_{\sin x}$ no puede ser una curva algebraica. $\diamond$

Ejemplo 1.23. Veamos que la curva de ecuación polar $r = \frac{1}{2\pi}\theta$ no es una curva algebraica en $\mathbb{R}^2$. Esta curva es un ejemplo de una *Espiral de Arquímedes* y tiene el gráfico siguiente:

FIGURA 4. Gráfico de la ecuación polar $r = \frac{1}{2\pi}\theta$ o Espiral de Arquímedes.

Note que si $\theta = 2n\pi$ con $n \in \mathbb{Z}$ entonces el punto en coordenadas cartesianas $(n, 0)$ está contenido en la Espiral de Arquímedes. Por lo tanto, al igual que el ejemplo anterior, esta curva no es algebraica pues no contiene al eje x y sin embargo lo interseca en una cantidad infinita de puntos. $\diamond$

EJERCICIOS

Ejercicios de la sección 1.

1.1 Demuestre lo siguiente.

(a) Demuestre que la parábola $\mathcal{C} = V_{\mathbb{C}}(y - x^2) \subset \mathbb{C}^2$ es irreducible.

(b) Sea $I_{\mathcal{C}} := \{f(x,y) \in \mathbb{C}[x,y] \mid f|_{\mathcal{C}} \equiv 0\}$ el conjunto de polinomios en$\mathbb{C}[x,y]$ que se anulan en todo punto de la parábola $\mathcal{C}$. Demuestre que

$$\begin{aligned} I_{\mathcal{C}} &= (y - x^2)\mathbb{C}[x,y] \\ &:= \{(y - x^2)g(x,y) \in \mathbb{C}[x,y] \mid g(x,y) \in \mathbb{C}[x,y]\}. \end{aligned}$$

Sugerencia: Aplique el algoritmo de la división para dividir un polinomio $f(x,y) \in I_{\mathcal{C}}$ por el polinomio $y - x^2$, considerándo a $f(x,y)$ como un polinomio en $\mathbb{C}[x][y]$. Esto es posible pues el coeficiente principal de $Y - X^2 \in \mathbb{C}[x][y]$ es 1, y este es invertible en $\mathbb{C}[x]$.

1.2 Encuentre las componentes irreducibles de las siguientes curvas algebraicas en k^2 para $k \in \{\mathbb{R}, \mathbb{C}\}$.

(a) $V_k(y^2 - xy - x^2y + x^3)$.

(b) $V_k(y^2 - x(x^2 - 1))$.

(c) $V_k(x^3 + x - x^2y - y)$.

Utilice `SageMath` (o `CoCalc`) para graficar los puntos reales de cada una de las curvas algebraicas anteriores.

1.3 Demuestre que $V_{\mathbb{C}}(y^2 - x(x-1)(x-\lambda)) \subset \mathbb{C}^2$ es una curva algebraica irreducible para todo $\lambda \in \mathbb{C}$. De hecho, para $\lambda \neq 0, 1$, esta curva algebraica es una curva elíptica en *forma normal de Legendre*.

1.4 Sea k un cuerpo y sean $F, G \in k[x_1, \ldots, x_n]$. Demuestre que si F es homogéneo de grado $d \geq 0$ y si $G|F$, entonces G también es homogéneo.

1.5 Sea k un cuerpo y sea $f(x,y) \in k[x,y]$. Suponga al considerar f como un polinomio en $k[x][y]$, este es mónico, es decir, que

$$f = y^n + a_{n-1}(x)y^{n-1} + \cdots + a_1(x)y + a_0(x),$$

con $a_i(x) \in k[x]$ para $i = 0, 1, \ldots, n-1$. Demuestre que si existen polinomios $g, h \in k[x][y]$ tales que

$$f = gh,$$

entonces existen polinomios mónicos $\widetilde{g}, \widetilde{h} \in k[x][y]$ tales que

$$f = \widetilde{g}\widetilde{h}.$$

1.6 (**El Teorema Fundamental del Álgebra para polinomios homogéneos en** $\mathbb{C}[x, y]$)
Sea $f(x, y) \in \mathbb{C}[x, y]$ un polinomio homogéneo de grado $n \geq 1$. Demuestre que existen números complejos $\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n \in \mathbb{C}$ tales que $f(x, y)$ se factoriza como un producto de factores lineales de la forma

$$f(x, y) = \prod_{i=1}^{n} (\alpha_i x + \beta_i y).$$

Sugerencia: Use el Teorema Fundamental del Álgebra.

1.7 Demuestre que el gráfico en $\mathbb{R}^2$ de la función $y = \cos(x)$ no es una curva algebraica en $\mathbb{R}^2$.

1.8 Demuestre que el gráfico en $\mathbb{R}^2$ de la función *onda de cierra* $y = -\frac{2}{\pi}\arctan(\cot(\pi x))$ no es una curva algebraica en $\mathbb{R}^2$.