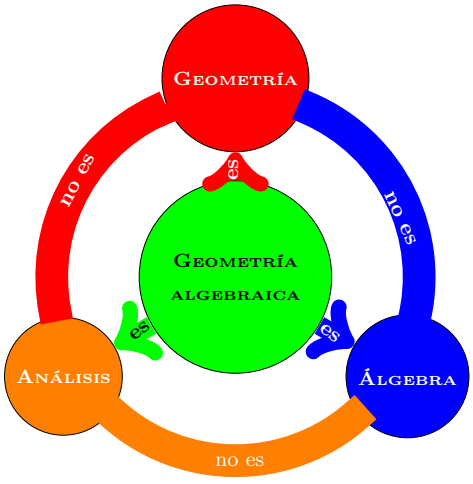
Miscelánea Matemática **67** (2018) 1-22 SMM

¿Qué es la geometría algebraica?

Laura Hidalgo Solís
Departamento de Matemáticas
Universidad Autónoma Metropolitana
Unidad Iztapalapa
hiso@xanum.uam.mx

1. Introducción

Cuando tuve el honor de ser invitada, por parte del Comité Editorial de Miscelanea Matemática, para presentar una plática de divulgación sobre ¿qué es la geometría algebraica? pensé en decirlo en pocas palabras, lo cual no es simple, pues no puede hacerse axiomáticamente, y no hay una única forma de introducirse a su estudio. Podríamos decir que «*la geometría algebraica es el estudio de los objetos geométricos, utilizando métodos algebraicos,*» pero entonces surge el problema de explicar qué significa esto, por lo cual decidí presentar la hermosa trilogía de la geometría algebraica clásica



utilizando las curvas proyectivas de grado a lo más tres, y proponer problemas elementales de clasificación, búsqueda de invariantes con respecto a determinados tipos de transformaciones, así como problemas de

intersecciones, entre otros. El propósito de la presente nota es presentar los fundamentos de geometría algebraica expuestos en dicha plática.

2. Hipersuperficies

A lo largo de las presentes notas, $\mathbb{C}$ denotará el campo de los números complejos, aunque la mayoría de las definiciones y resultados que aquí se presentan son válidos en cualquier campo algebraicamente cerrado.

Definición 2.1. El conjunto $\mathbb{A}^n = \{(a_1, a_2, \ldots, a_n)\ ; a_j \in \mathbb{C}\}$ se denomina el *espacio afín* de dimensión n. Los elementos de $\mathbb{A}^n$ se llaman *puntos.*

Nótese que el espacio afín $\mathbb{A}^n$ es simplemente el conjunto de puntos con coordenadas en $\mathbb{C}$, sin considerar la estructura de espacio métrico vectorial inducida por el campo $\mathbb{C}$. Escribiremos $P(a_1, \ldots, a_n)$ para denotar el punto $P \in \mathbb{A}^n$ de coordenadas $(a_1, \ldots, a_n)$.

- $\mathbb{A}^1 = \{(a_1)\ ; a_1 \in \mathbb{C}\}$, es la línea afín.
- $\mathbb{A}^2 = \{(a_1, a_2)\ ; a_j \in \mathbb{C}\}$, es el plano afín.
- $\mathbb{A}^3 = \{(a_1, a_2, a_3)\ ; a_j \in \mathbb{C}\}$, es el espacio afín.

Definición 2.2. Si $f \in \mathbb{C}[x_1, \ldots, x_n]$ es un polinomio, el conjunto de ceros de f, que a lo largo de la presente plática denotaremos $Z(f)$, es una *hipersuperficie.* Una hipersuperficie en $\mathbb{A}^2$ se denomina *curva plana afín.* Una hipersuperficie en $\mathbb{A}^3$ se denomina una *superficie afín.* El *grado de una hipersuperficie* es igual al grado del polinomio asociado.

Si $S \subset \mathbb{C}[x_1, \ldots, x_n]$, el conjunto $Z(S) = \bigcap_{f \in S} Z(f)$ se denomina un *conjunto algebraico.*

Es claro que, si $\lambda \in \mathbb{C}^\star = \mathbb{C} \setminus \{0\}$, entonces $Z(f) = Z(\lambda f)$. Si pensamos al polinomio $f \in \mathbb{C}[x_1, \ldots, x_n]$ como una función polinomial, entonces $Z(f) = f^{-1}(\{0\})$, y como $\{0\}$ es un conjunto cerrado, si queremos que las funciones polinomiales induzcan funciones continuas, los conjuntos $Z(f)$ deben ser conjuntos cerrados.

Nótese además que $Z(1) = \emptyset$, $Z(0) = \mathbb{A}^n$, $Z(fg) = Z(f) \cup Z(g)$, y por definición, la intersección arbitraria de hipersuperficies es un conjunto algebraico, lo cual demuestra que las hipersuperficies constituyen una base de conjuntos cerrados para una topología de $\mathbb{A}^n$. Esta topología se llama la *topología de Zariski de* $\mathbb{A}^n$, y es una topología no Hausdorff, pues todo conjunto abierto no vacío es denso, véase [2, cap. 6, §1].

Como ejemplos bien conocidos de curvas planas tenemos las líneas, como ceros de polinomios de grado uno, las cónicas, como ceros de polinomios de grado dos.

Una curva es *irreducible* si el polinomio asociado es irreducible, en otro caso decimos que es reducible. Por ejemplo, la línea $Ax+By+C=0$ es un ejemplo de curva irreducible, mientras que, si consideramos un polinomio $f \in \mathbb{C}[x,y]$ de grado dos, la cónica $Z(f)$ es reducible si es producto de dos factores lineales no necesariamente distintos, en este caso, cada factor lineal determina una línea recta, la cual se denomina una *componente irreducible* de la cónica.

Se puede determinar si la cónica es irreducible o no a partir de los coeficientes de la forma cuadrática asociada $f(x,y) = Ax^2 + Bxy + Cy^2 + Dx + Ey + F$, así la cónica es irreducible si, y solamente si,

$$\det \begin{pmatrix} A & B/2 & D/2 \\ B/2 & C & E/2 \\ D/2 & E/2 & F \end{pmatrix} \neq 0.$$

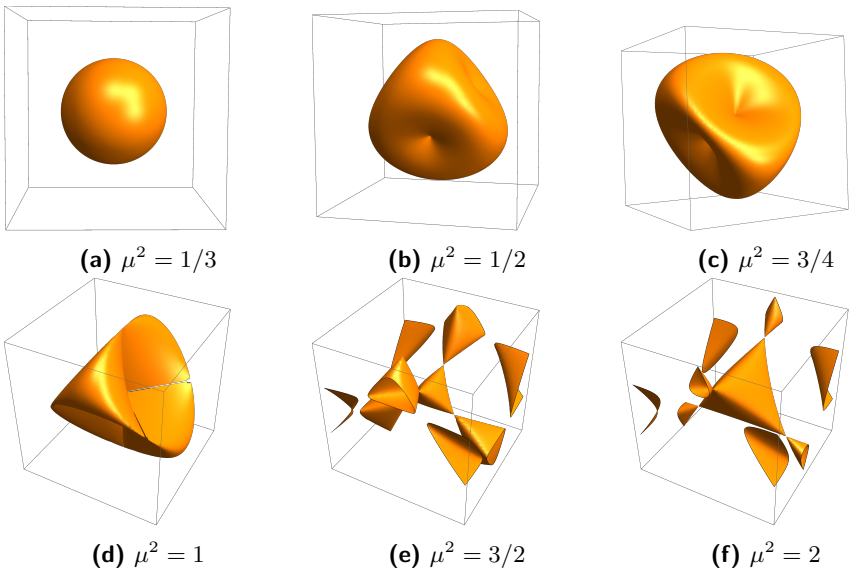
Como ejemplos de superficies tenemos los planos, a saber, $Z(Ax + By + Cz + D)$; y las superficies cuadráticas son ceros de polinomios de grado dos en tres variables.

En 1864 Ernst E. Kummer dio la familia de hipersuperficies en $\mathbb{A}^4$:

$$\begin{aligned} X_{4,\mu} &= \left\{(x,y,z,w) \in \mathbb{A}^4;\ (x^2+y^2+z^2-\mu^2 w)^2 - \lambda pqrs = 0\right\} \\ \lambda &= \frac{3\mu^2-1}{3-\mu^2}, \quad \mu \in \mathbb{R}, \end{aligned}$$

$p = w-z-\sqrt{2}x$, $q = w-z+\sqrt{2}x$, $r = w+z+\sqrt{2}y$, $s = w+z-\sqrt{2}y$.

Para $w=1$ tenemos una bella familia de superficies, que denotaremos nuevamente $X_{4,\mu}$, en $\mathbb{A}^3$, mostramos a continuación algunos ejemplos:



(a) $\mu^2 = 1/3$ **(b)** $\mu^2 = 1/2$ **(c)** $\mu^2 = 3/4$

(d) $\mu^2 = 1$ **(e)** $\mu^2 = 3/2$ **(f)** $\mu^2 = 2$

Figura 1. Ejemplos de superficies de Kummer para distintos valores de μ.

Cuando $\mu^2 = 1/3$ se tiene la doble esfera, es decir, como conjunto es una esfera, pero todos los puntos se cuentan con multiplicidad dos, de acuerdo con la definición (2.3).

Las superficies de Kummer $X_{4,\mu}$ son singulares para $1/3 < \mu^2 < 1$, por ejemplo, cuando $\mu^2 = 1/2$ la superficie $X_{4,1/2}$ tiene puntos singulares, a saber, 4 reales y 12 complejos, los cuales son puntos en la superficie donde el gradiente del polinomio asociado se anula. Cuando $\mu^2 = 1$, se tiene la superficie de Steiner. Si $1 < \mu^2 < 3$, tenemos las superficies de Kummer con 16 puntos singulares reales.

Definición 2.3. Sean $P(0,0) \in \mathbb{A}^2$ y $f \in \mathbb{C}[x,y]$ un polinomio de grado n, entonces

$$f = f_m + f_{m+1} + \cdots + f_n,$$

donde $f_k \in \mathbb{C}[x,y]$ es una forma de grado k, con $f_m \neq 0$.[1]

El número $m = m_P(f)$ se denomina la *multiplicidad de $Z(f)$ en P*. Así, $P(0,0) \in Z(f)$ si, y solamente si, $m_P(f) > 0$.

Por ejemplo, si $f(x,y) = x - y + x^2 - xy + y^3$, entonces $f(0,0) = 0$, $f_1(x,y) = x - y$, $f_2(x,y) = x^2 - xy$ y $f_3 = y^3$, por lo que $P(0,0)$ es un punto de multiplicidad 1.

Por otra parte, si $g(x,y) = x^2 - xy + y^3$, entonces $g(0,0) = 0$, $g_2(x,y) = x^2 - xy$ y $g_3 = y^3$, por lo que $P(0,0)$ es un punto de multiplicidad 2.

Para determinar la multiplicidad en cualquier otro punto $Q(a,b)$, simplemente aplicamos un cambio lineal de coordenadas. [2]

Definición 2.4. Dada una línea $\ell = \{(x,y) \in \mathbb{A}^2; a_1x + a_2y = 0\}$, parametrizada como $t \mapsto (a_2t, -a_1t)$, con $t \in \mathbb{C}$. Si $C = Z(f)$ es una curva afín irreducible con $P \in C$, se define *la multiplicidad de intersección de la línea ℓ y la curva C en el punto $P(0,0)$* como el máximo $r \in \mathbb{N}$ tal que $t^r \mid f(a_2t, -a_1t)$. A este número lo denotaremos $I_P(\ell, C)$. Si $P \notin C$, se define $I_P(\ell, C) = 0$.

Nuevamente, si deseamos conocer la multiplicidad de intersección de una línea ℓ y una curva C en un punto $Q \in \ell$, se aplica simplemente el cambio lineal de coordenadas $T(x,y) = (x - a, y - b)$.

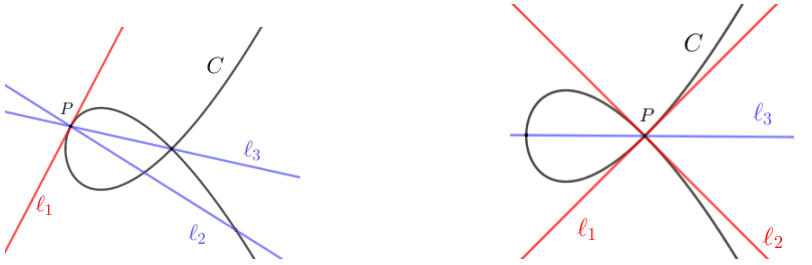
Por ejemplo, si consideramos la cónica $C = Z(f)$ con$f(x,y) = x^2 - y$ y las líneas $\ell_1 = Z(x)$ y $\ell_2 = Z(y)$, es claro que ℓ_1 se parametriza como $\phi_1(t) = (0, -t)$, de donde $f(0,-t) = t$, por lo cual $I_P(\ell_1, C) = 1$. Análogamente, ℓ_2 se parametriza como $\phi_2(t) = (t, 0)$, y se tiene $f(t,0) = t^2$ de donde $I_P(\ell_2, C) = 2$.

[1] Una forma es un polinomio en que cada uno de sus términos tienen el mismo grado. Una forma también se denomina polinomio homogéneo.

[2] Un cambio lineal de coordenadas en $\mathbb{A}^n$ es una función $T : \mathbb{A}^n \to \mathbb{A}^n$, de la forma $T(P) = (f_1(P), \ldots, f_n(P))$, donde los f_k son polinomios de grado 1 en n variables.

Proposición 2.1. *Si $C = Z(f)$ es una curva afín irreducible, y $P \in C$, entonces se satisface exactamente una de las siguientes condiciones:*

1. *Hay una única línea que interseca C con multiplicidad mayor que uno en P. Cualquier otra línea lo hace con multiplicidad exactamente uno en P.*
2. *Cada línea que pasa por P interseca a C con multiplicidad al menos 2.*



(a) Solo ℓ_1 intersecta la curva con multiplicidad mayor que uno en P.

(b) Toda recta ℓ intersecta la curva con multiplicidad mayor que uno en P.

Figura 2. Relación entre una recta y una curva.

Demostración. Supongamos que $P(0,0)$, de donde, una línea por P es de la forma $\ell = Z(g)$ donde $g(x_1, x_2) = a_1x_1 + a_2x_2$, y el polinomio f es de la forma $f(x_1, x_2) = \sum_{k=m}^{d} f_k(x_1, x_2)$, con $m \geq 1$, y $d = \deg f$, y f_k formas de grado k.

Es claro que la línea ℓ puede parametrizarse como $t \mapsto (a_2t, -a_1t)$, con $t \in \mathbb{C}$.
Por la definición (2.4), $I_P(\ell, C) = \text{máx}\{r \in \mathbb{N};\ t^r \mid f(a_2t, -a_1t)\}$.

Luego entonces

$$f(a_2t, -a_1t) = f_m(a_2, -a_1)t^m + \ldots + f_d(a_2, -a_1)t^d, \tag{1}$$

lo cual indica que la multiplicidad de intersección de ℓ y C en P es al menos m y, es mayor que m, si y solamente si, $f_m(a_2, -a_1) = 0$, es decir, si $g \mid f_m$. □

Además, si $C = Z(f)$ y $\ell = Z(g)$ donde $f, g \in \mathbb{C}[x_1, x_2]$ y $\deg g = 1$, con $P \notin \ell \cap C$, se define $I_P(\ell, C) = 0$. Finalmente, si f no es un polinomio irreducible, y g es un factor de f, se define $I_P(\ell, C) = \infty$. En general, si $g \not| f$, es decir, si ℓ no es una componente irreducible de C, se tiene que $\sum_{P \in \ell \cap C} I_P(\ell, C) \leq \deg(f)$. Para un estudio más detallado sobre la multiplicidad de intersección entre dos curvas véase [4, cap. III, §11], o bien, [1, cap. I §1 y §3].

Definición 2.5. Si $C = Z(f)$, se llama *línea tangente a C en P* a cualquier línea ℓ tal que $I_P(\ell, C) > m_P(f)$. Llamaremos *cono tangente a la curva C en el punto $P \in C$* a la unión de las rectas tangentes a C en P.

Un *punto múltiple, o singular,* de C es un punto $P \in C$ tal que $m_P(f) > 1$, mientras que un *punto no singular* es un punto $P \in C$ tal que $m_P(f) = 1$. En este último caso existe una única línea tangente a C en P, que denotamos $T_P(C)$.

Una *curva no singular* es aquella que no tiene puntos múltiples.

En general, si $f \in \mathbb{C}[x_1, x_2]$ y $P = (a_1, a_2) \in Z(f)$, entonces P es un punto no singular de $Z(f)$ si

$$\nabla f(P) = \left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P) \right) \neq (0, 0).$$

En éste caso, la *línea tangente* a la curva $Z(f)$ en P está dada como

$$\left\{ (x, y) \in \mathbb{A}^2;\ \frac{\partial f}{\partial x}(P)(x - a_1) + \frac{\partial f}{\partial y}(P)(y - a_2) = 0 \right\}.$$

Por ejemplo, consideremos la curva de grado seis $C = Z(f)$, dada por $f(x, y) = (x^2 + y^2)^3 - 4x^2y^2$, es claro que $f(0, 0) = 0$, y tenemos que $f_4(x, y) = -4x^2y^2$, y $f_6(x, y) = (x^2 + y^2)^3$, por lo que $P(0, 0)$ es un punto singular, y $m_P(f) = 4$.

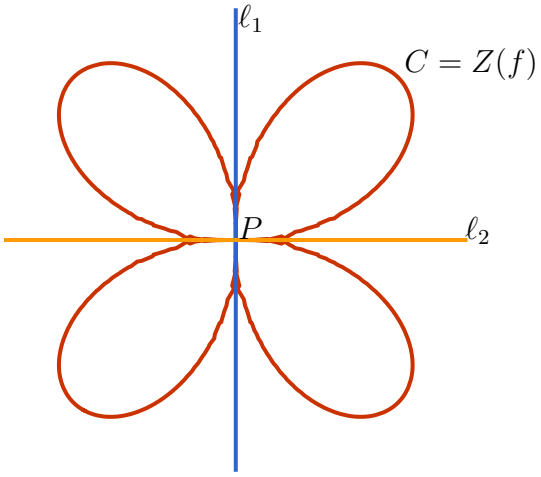


Figura 3. Ejemplo del cono tangente en el punto singular P.

Si $\ell_1 : x = 0$, entonces $t \mapsto (0, t)$ es una parametrización de ésta recta, y $f(0, t) = t^6$, por lo que $I_P(\ell_1, C) = 6 > 4 = m_P(f)$. De manera análoga, si $\ell_2 : y = 0$, entonces $t \mapsto (t, 0)$ es una parametrización de ℓ_2, $f(t, 0) = t^6$, así $I_P(\ell_2, C) = 6 > 4 = m_P(f)$. El cono tangente es $Z(x^2y^2)$, que como conjunto corresponde a $\ell_1 \cup \ell_2$.

Aún más, como $\nabla f = (-8xy^2+6x(x^2+y^2)^2, -8x^2y+6y(x^2+y^2)^2)$, al resolver el sistema $\{f = 0, f_x = 0, f_y = 0\}$ es fácil verificar que $P(0,0)$ es el único punto singular de C.

Como consecuencia de la proposición (2.1), ecuación (1), tenemos que una línea y una curva de grado d, que no contenga a la línea, se intersecan a lo más en d puntos, por ejemplo, dos líneas paralelas no se intersecan. Para poder garantizar que una línea y una curva de grado d se intersecan exactamente en d puntos, contando multiplicidades, es necesario anexar los puntos al infinito. Este resultado es conocido como la versión débil del teorema de Bezout [2, cap. 5, §3].

Cuando anexamos convenientemente al plano afín los puntos al infinito obtenemos el plano proyectivo. En el plano proyectivo una línea y una curva de grado d se intersecan exactamente en d puntos contando multiplicidades.

3. El plano proyectivo

Decimos que dos puntos $z, z' \in \mathbb{A}^{n+1} \setminus \{\vec{0}\}$ *son equivalentes* si existe un escalar $\lambda \in \mathbb{C}^*$ tal que $z' = \lambda z$. [3] Claramente, la relación es de equivalencia.

Definición 3.1. El *espacio proyectivo*, que denotaremos $\mathbb{P}^n$, es el conjunto de clases de equivalencia de $\mathbb{A}^{n+1}\setminus\{\vec{0}\}$, es decir $\mathbb{P}^n = (\mathbb{A}^{n+1}\setminus\{\vec{0}\})/\mathbb{C}^*$.

Los elementos de $\mathbb{P}^n$ son *puntos*. Un representante $(x_0, \ldots, x_n) \in \mathbb{A}^{n+1}$ de un punto de la clase $(x_0; \ldots; x_n) \in \mathbb{P}^n$ se denomina la *coordenada homogénea* del punto.

La función $\pi : \mathbb{A}^{n+1}\setminus\{0\} \to \mathbb{P}^n$, dada por $\pi(x_0, \ldots, x_n) = (x_0; \ldots; x_n)$, que asocia a cada punto de $\mathbb{A}^{n+1} \setminus \{0\}$ su clase de equivalencia, se denomina la *proyección canónica.*

Por ejemplo *la línea proyectiva*, también conocida como la esfera de Riemann, es $\mathbb{P}^1 = (\mathbb{A}^2 \setminus \{\vec{0}\})/\mathbb{C}^* \simeq \mathbb{A}^1 \cup \{\infty\} \simeq \mathbb{S}^2$.

En $\mathbb{P}^2$, los conjuntos $U_k := \{(x_0; x_1; x_2) \in \mathbb{P}^2 \mid x_k \neq 0\}, \quad k = 0, 1, 2$ constituyen una cubierta abierta, es decir, $\mathbb{P}^2 = \bigcup_{k=0}^{2} U_k$. Los conjuntos U_k son homeomorfos al plano afín, esto es $U_k \simeq \mathbb{A}^2$. Para ver esto, tomemos por ejemplo el abierto U_2, en particular $x_2 \neq 0$, y la función de $\mathbb{P}^2$ en U_2 dada por

$$\phi_2(x_0; x_1; x_2) = \left(\frac{x_0}{x_2}; \frac{x_1}{x_2}\right).$$

[3] Recordamos que $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

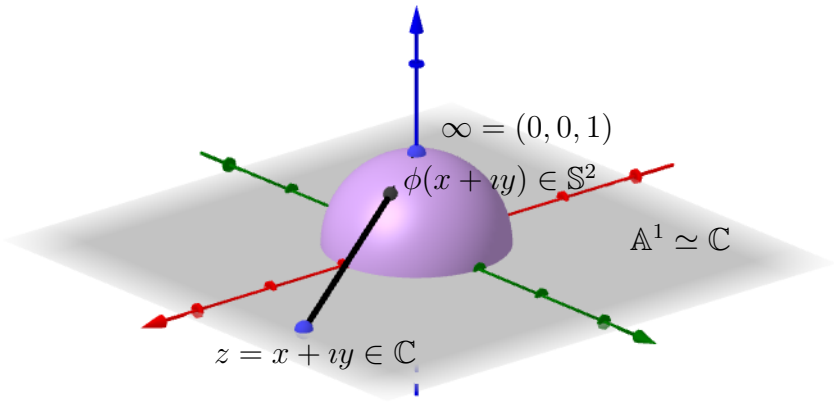


Figura 4. Representación geométrica de la línea proyectiva $\mathbb{P}^1$, al punto $z \in \mathbb{C}$ se le asocia $\phi(z) \in \mathbb{S}^2$, que se obtiene al intersecar la esfera $\mathbb{S}^2 \subset \mathbb{R}^3$ con la recta que une el $\infty = (0,0,1)$ con $z \simeq (x,y,0)$.

La función ϕ_2 es continua, y su inversa es aquella a que cualquier par ordenado (x_1, x_2) le asocia el punto en el plano proyectivo $(x_1; x_2; 1)$. El par (U_k, ϕ_k) se denomina un *sistema afín de coordenadas.*

Observemos que el plano proyectivo se obtiene agregando al plano afín todos sus puntos al infinito.

$$\mathbb{P}^2 \simeq \mathbb{A}^2 \cup \mathbb{P}^1 \simeq \mathbb{A}^2 \cup \mathbb{A}^1 \cup \{\infty\}.$$

Un *sistema de coordenadas proyectivas para* $\mathbb{P}^2$ está determinado por los cuatro puntos de coordenadas homogéneas $\pi(e_0) = (1;0;0)$, $\pi(e_1) = (0;1;0)$, $\pi(e_2) = (0;0;1)$ y $\pi(e_3) = (1;1;1)$. Cualesquiera tres puntos de este conjunto es imagen, bajo la proyección canónica, de un subconjunto linealmente independiente de $\mathbb{C}^3$.

Cabe notar que, si $\beta = \{e_0, e_1, e_2\}$ es la base canónica de $\mathbb{C}^3$, para $\lambda_k \in \mathbb{C}^*$, $k = 0, 1, 2$, también $\beta' = \{\lambda_0 e_0, \lambda_1 e_1, \lambda_2 e_2\}$ es una base de $\mathbb{C}^3$. Si ambas bases asignan a $\pi(e_3)$ las coordenadas homogéneas $(1;1;1)$, entonces $\pi(e_0+e_1+e_2) = (1;1;1) = \pi(\lambda_0 e_0+\lambda_1 e_1+\lambda_2 e_2)$, lo cual implica que $\lambda_0 = \lambda_1 = \lambda_2$, por lo cual las dos bases β y β' son proporcionales. Si $(a;b;c)$ proviene de (a,b,c) en la base β, entonces $(a;b;c)$ proviene de $(\lambda_0^{-1}a, \lambda_0^{-1}b, \lambda_0^{-1}c)$ en la base β'.

4. Curvas algebraicas

Definición 4.1. Sea $F = F(x_0, x_1, x_2)$ una forma de grado n, $(n \geq 1.)$

$$Z(F) = \{(x_0; x_1; x_2) \in \mathbb{P}^2;\ F(x_0, x_1, x_2) = 0,\ (x_0, x_1, x_2) \in (x_0; x_1; x_2)\}$$

se denomina una *curva algebraica plana* o simplemente una curva plana.

Como el plano proyectivo está dado por las clases de equivalencia de puntos en el espacio afín, podemos pensar a $Z(F)$ como un cono cuya base es una curva en el plano afín U_k, adjuntando los puntos al infinito.

Por ejemplo, la forma de grado tres $F(x, y, z) = x^3 + x^2z - y^2z$, es una curva proyectiva, y podemos visualizar a $Z(F)$ como un cono en el espacio afín $\mathbb{A}^3$

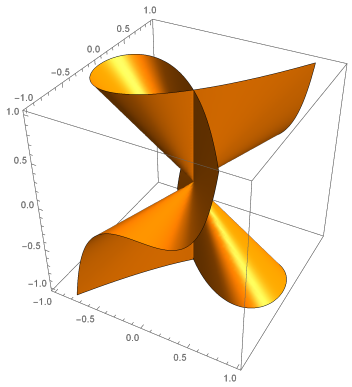
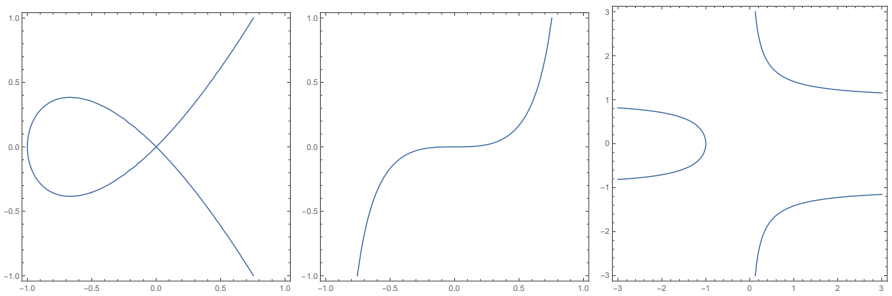


Figura 5. La curva $Z(x^3 + x^2z - y^2z)$ vista en $\mathbb{A}^3$.

Si tomamos la intersección del cono $Z(F) \subset \mathbb{A}^3$ con los planos afines $z = 1, y = 1$ y $x = 1$ tenemos las curvas afines, $Z(x^3 + x^2 - y^2)$, $Z(x^3 + x^2z - z)$ y $Z(1 + z - y^2z)$ respectivamente.



(a) $Z(x^3 + x^2 - y^2)$. **(b)** $Z(x^3 + x^2z - z)$ **(c)** $Z(1 + z - y^2z)$

Figura 6. Intersección de $Z(x^3 + x^2z - y^2z)$ con los planos afines U_k.

Cada una de las curvas afines anteriores, nos proporciona representantes de la curva proyectiva $Z(F)$ salvo los puntos al infinito, es decir, desde el punto de vista proyectivo, las tres curvas anteriores son lo mismo.

Lo anterior nos hace pensar que debe ser lo mismo estudiar curvas proyectivas planas y curvas afines planas, salvo los puntos al infinito.

Para relacionar las curvas proyectivas y las curvas afines, a cada curva proyectiva le asociaremos una curva afín, y recíprocamente.

Sea $F \in \mathbb{C}[x_0, x_1, x_2]$, una forma de grado $\deg F = d$, definimos el polinomio

$$F_*(x_1, x_2) := F(1, x_1, x_2) \in \mathbb{C}[x_1, x_2].$$

Recíprocamente, si $f \in \mathbb{C}[x_1, x_2]$ es un polinomio de grado $\deg f = d$, entonces

$$f = f_0 + f_1 + f_2 + \cdots + f_d$$

donde f_k es una forma de grado k, para $k = 0, 1, \ldots, d$. Definimos la forma f^* de grado d como:

$$f^*(x_0, x_1, x_2) := f_0 x_0^d + f_1 x_0^{d-1} + \cdots + f_{d-1} x_0 + f_d.$$

Es fácil ver que los operadores f^* y F_* se relacionan como sigue:

Proposición 4.1. *Si $F, G \in \mathbb{C}[x_0, x_1, x_2]$ son formas, y $f, g \in \mathbb{C}[x_1, x_2]$ son polinomios, entonces*

1. $(FG)_* = F_* G_*$; *y* $(fg)^* = f^* g^*$.
2. *Si r es la máxima potencia de x_0 que divide a F, entonces* $x_0^r (F_*)^* = F$; *y* $(f^*)_* = f$.
3. $(F+G)_* = F_* + G_*$; *y* $x_0^t (f+g)^* = x_0^r f^* + x_0^s g^*$, *donde* $r = \deg g$, $s = \deg f$ *y* $t = r + s - \deg(f+g)$.
4. *Salvo potencias de x_0, factorizar $F \in \mathbb{C}[x_0, x_1, x_2]$ es lo mismo que factorizar $F_* \in \mathbb{C}[x_1, x_2]$.*

Demostración. Véase [2, cap. 2, §6]. □

Así, salvo los puntos al infinito, es equivalente estudiar las curvas planas afines y las curvas algebraicas planas.

Definición 4.2. Si $\phi : \mathbb{A}^3 \to \mathbb{A}^3$ es un cambio lineal de coordenadas, entonces ϕ transforma líneas por el origen en líneas por el origen, por lo tanto ϕ determina una transformación $\varphi : \mathbb{P}^2 \to \mathbb{P}^2$, y se denomina un *cambio de coordenadas proyectivo.* Un cambio de coordenadas proyectivo también se denomina *proyectividad, colineación, transformación proyectiva, u homografía.*

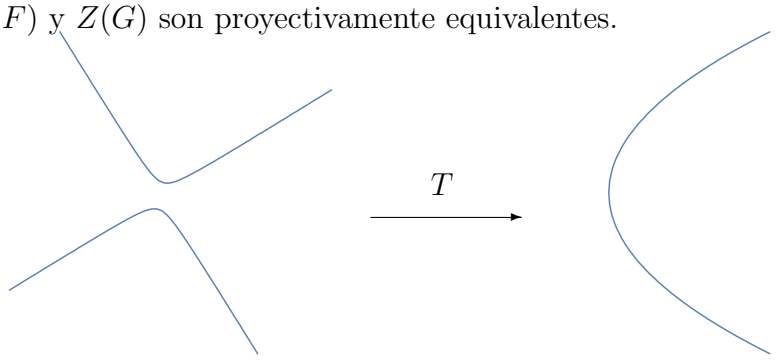
Así, la transformación proyectiva φ está determinada por el valor de φ en un sistema de coordenadas proyectivas de $\mathbb{P}^2$.

Es claro que si $id_{\mathbb{C}^3}$ es la transformación identidad, entonces la transformación que induce en $\mathbb{P}^2$ será $id_{\mathbb{P}^2}$. Aún más, el grupo de transformaciones proyectivas de $\mathbb{P}^2$ es isomorfo a $GL(3, \mathbb{C})/\{\lambda\, id_{\mathbb{C}^3}; \lambda \in \mathbb{C}^*\}$.

En particular, una cuarteta de puntos en $\mathbb{P}^2$ es un *marco proyectivo* cuando, y solamente cuando, cada tres de ellos son imagen de un conjunto linealmente independiente en $\mathbb{C}^3$.

Definición 4.3. Diremos que dos curvas algebraicas $Z(F)$ y $Z(G)$ en $\mathbb{P}^2$ son *proyectivamente equivalentes* si hay una transformación proyectiva $T : \mathbb{P}^2 \to \mathbb{P}^2$ tal que $G \circ T = F$.

Por ejemplo, si consideramos las cónicas $Z(F)$ y $Z(G)$ en $\mathbb{P}^2$, donde $F(x,y,z) = x^2 - y^2 + z^2 - xy + xz - yz$ y $G(x,y,z) = y^2 - xz$, entonces $Z(F)$ y $Z(G)$ son proyectivamente equivalentes.



(a) $Z(x^2 - y^2 + z^2 - xy + xz - yz)$. **(b)** $Z(y^2 - xz)$

Figura 7. Ejemplo de curvas algebraicas proyectivamente equivalentes.

Ya que, si $T(x,y,z) = (y+z, x+z, x+y)$, entonces

$$\begin{aligned} G \circ T(x,y,z) &= G(y+z, x+z, x+y) = (x+z)^2 - (y+z)(x+y) \\ &= x^2 + 2xz + z^2 - (xy + y^2 + xz + yz) \\ &= x^2 - y^2 + z^2 - xy + xz - yz = F(x,y,z) \end{aligned}$$

Definición 4.4. Un *invariante proyectivo* de una curva algebraica plana es una propiedad que es invariante bajo equivalencia proyectiva.

Claramente, un ejemplo de invariante proyectivo es el grado de una curva plana.

Es fácil ver que, si $F, G \in \mathbb{C}[x,y,z]$ son formas de grado 1, entonces $Z(F)$ y $Z(G)$ son curvas algebraicas proyectivamente equivalentes.

Proposición 4.2. *Todas las cónicas irreducibles son proyectivamente equivalentes.*

Demostración. Bastará mostrar que cualquier cónica irreducible C es proyectivamente equivalente a la cónica $x_0x_2 - x_1^2 = 0$.

Consideremos tres puntos distintos P_0, P_2 y P_3 en C, y sea P_1 el punto de intersección de las rectas tangentes a C en los puntos P_0 y P_2. Como la cónica es irreducible, los puntos P_0, P_1, P_2 y P_3 constituyen un marco proyectivo. Entonces, existe una transformación proyectiva T definida en $\mathbb{P}^2$, tal que, $T(P_0) = (1;0;0)$, $T(P_1) = (0;1;0)$, $T(P_2) = (0;0;1)$ y $T(P_3) = (1;1;1)$.

La cónica C' que pasa por los puntos $(1;0;0)$, $(0;1;0)$, $(0;0;1)$ y $(1;1;1)$ debe satisfacer una ecuación de la forma

$$\sum_{i+j+k=2} a_{i,j,k} x_0^i x_1^j x_2^k = 0$$

al resolver el sistema, podemos ver que C' está dada como

$$C' := \{(x_0; x_1; x_2) \ ; \ x_0x_2 - x_1^2 = 0\}.$$

Como esperábamos demostrar. □

Veamos ahora cuántos tipos de cúbicas algebraicas proyectivas distintas hay.

Una curva cúbica proyectiva $\mathcal{C}$, es el conjunto de ceros de un polinomio homogéneo de grado $d = 3$, en $\mathbb{C}[x_1, x_2, x_3]$, esto es, si

$$\begin{aligned} F(x_1, x_2, x_3) &= \alpha_0x_1^3 + \alpha_1x_1^2x_2 + \alpha_2x_1^2x_3 + \alpha_3x_1x_2^2 + \alpha_4x_1x_2x_3 \\ &\quad +\alpha_5x_1x_3^2 + \alpha_6x_2^3 + \alpha_7x_2^2x_3 + \alpha_8x_2x_3^2 + \alpha_9x_3^3 \end{aligned}$$

es un polinomio homogéneo de grado $d = 3$, entonces $\mathcal{C} = Z(F)$, es decir,

$$\mathcal{C} = \{(x_1; x_2; x_3) \in \mathbb{P}^2 \mid F(x_1, x_2, x_3) = 0\}.$$

El punto $(0; 0; 1)$ pertenece a la cúbica $\mathcal{C}$ si, y solamente si, $\alpha_9 = 0$.

Además, $\nabla F(0; 0; 1) = (\alpha_5, \alpha_8, 0)$, por lo que la línea tangente a $Z(F)$ en $(0; 0; 1)$ satisface la ecuación

$$\alpha_5x_1 + \alpha_8x_2 = 0.$$

La recta $x_2 = 0$ es tangente a la cúbica $\mathcal{C}$ cuando, y sólo cuando, $\alpha_5 = 0$ y, como consecuencia de la definición de punto singular, $\alpha_8 \neq 0$.

Sin perder generalidad, podemos suponer que $\alpha_8 = 1$.

Si suponemos que $\mathcal{C}$ es irreducible, entonces α_0 y α_2 no se anulan simultáneamente, ya que si $\alpha_0 = \alpha_2 = 0$ tendríamos

$$\begin{aligned} F(x_1, x_2, x_3) &= \alpha_1x_1^2x_2 + \alpha_3x_1x_2^2 + \alpha_4x_1x_2x_3 + \alpha_6x_2^3 + \alpha_7x_2^2x_3 + x_2x_3^2 \\ &= x_2\left(\alpha_1x_1^2 + \alpha_3x_1x_2 + \alpha_4x_1x_3 + \alpha_6x_2^2 + \alpha_7x_2x_3 + x_3^2\right) \end{aligned}$$

de donde, el polinomio F no sería irreducible.

Cabe recordar que una curva de grado $d = 3$ tiene al menos uno, y a lo más tres puntos de inflexión, en particular, podemos suponer que $(0; 0; 1)$ es un punto de inflexión de la curva $Z(F)$, y ésto sucede cuando, y solamente cuando el hessiano de F evaluado en $(0; 0; 1)$ es cero, de donde $-8\alpha_2 = 0$.

Bajo estas hipótesis

$$\begin{aligned} F(x_1, x_2, x_3) &= \alpha_0x_1^3 + \alpha_1x_1^2x_2 + \alpha_3x_1x_2^2 + \alpha_4x_1x_2x_3 \\ &\quad +\alpha_6x_2^3 + \alpha_7x_2^2x_3 + x_2x_3^2. \end{aligned}$$

Realizando la transformación proyectiva

$$T(x_1, x_2, x_3) = (x_1, x_3, x_2),$$

obtenemos

$$\begin{aligned} F(x_1,x_2,x_3) &= \alpha_0 x_1^3 + \alpha_1 x_1^2 x_3 + \alpha_3 x_1 x_3^2 + \alpha_4 x_1 x_3 x_2 \\ &\quad + \alpha_6 x_3^3 + \alpha_7 x_3^2 x_2 + x_3 x_2^2. \quad \alpha_0 \neq 0. \end{aligned}$$

Ya que $\alpha_0 \neq 0$, tenemos que la curva $\mathcal{C}$ está dada como los puntos $(x_1; x_2; x_3) \in \mathbb{P}^2$ que son solución de la ecuación

$$x_2^2 x_3 + \alpha_4 x_1 x_2 x_3 + \alpha_7 x_2 x_3^2 = \alpha_0 x_1^3 + \alpha_1 x_1^2 x_3 + \alpha_3 x_1 x_3^2 + \alpha_6 x_3^3.$$

Por otra parte, si hacemos el cambio de variables proyectivo

$$(x_1, x_2, x_3) = \left(\frac{x}{\sqrt[3]{\alpha_0}}, y, z \right)$$

obtenemos:

$$x_2^2 x_3 + \frac{\alpha_4}{\sqrt[3]{\alpha_0}} x_1 x_2 x_3 + \alpha_7 x_2 x_3^2 = x_1^3 + \frac{\alpha_1}{\sqrt[3]{\alpha_0^2}} x_1^2 x_3 + \frac{\alpha_3}{\sqrt[3]{\alpha_0}} x_1 x_3^2 + \alpha_6 x_3^3.$$

Definición 4.5. Una *curva elíptica* es proyectivamente equivalente a una curva algebraica que satisface una ecuación de la forma

$$\mathcal{E} : y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3. \tag{2}$$

Y la ecuación (2) se denomina la *ecuación canónica,* o *ecuación de Weierstrass* de la curva elíptica $\mathcal{E}$.

Si aplicamos ahora el cambio de variables proyectivo

$$(x, y, z) = \left(x', y' - \frac{a_1}{2} x', z' \right),$$

a la curva elíptica dada en la ecuación (2) obtenemos una ecuación donde se ha eliminado el término xyz, a saber

$$\mathcal{E} : y'^2 z + a_3 y' z'^2 = x'^3 + \left(\frac{1}{4} a_1^2 + a_2 \right) x'^2 z' + \left(\frac{1}{2} a_1 a_3 + a_4 \right) x' z'^2 + a_6 z'^3.$$

Y ahora, si consideramos

$$(x', y', z') = \left(x - \frac{a_2}{3} z, y - \frac{a_3}{2} z, z \right)$$

obtenemos

$$\begin{aligned} y^2 z &= x^3 + \frac{a_1^2}{4} x^2 z \\ &\quad + \left(a_4 + \frac{a_1 a_3}{2} - \frac{a_1^2 a_2}{6} - \frac{a_2^2}{3} \right) x z^2 \\ &\quad \left(\frac{a_3^2}{4} + \frac{2 a_2^3}{27} + \frac{a_1^2 a_2^2}{36} - \frac{a_1 a_2 a_3}{6} - \frac{a_2 a_4}{3} + a_6 \right) z^3. \end{aligned}$$

Finalmente, si

$$(x, y, z) = \left(X + \frac{a_1^2}{12}Z, Y, Z\right)$$

tenemos

$$\begin{aligned} Y^2Z &= X^3 + \left(a_4 + \frac{a_1a_3}{2} - \frac{a_1^2a_2}{6} - \frac{a_2^2}{3} - \frac{a_1^4}{48}\right)XZ^2 \\ &\quad + \left(\frac{a_1^6}{864} + \frac{a_1^2a_2^2}{18} + \frac{a_1^4a_2}{72} - \frac{a_1^3a_3}{24} - \frac{a_1^2a_4}{12} + \frac{a_3^2}{4} + \frac{2a_2^3}{27}\right. \\ &\quad \left. - \frac{a_1a_2a_3}{6} - \frac{a_2a_4}{3} + a_6\right)Z^3 \end{aligned}$$

es decir, una curva elíptica es proyectivamente equivalente a una curva algebraica que satisface una ecuación de la forma

$$\mathcal{E} : y^2z - x^3 - axz^2 - bz^3 = 0, \quad \text{con} \quad a, b \in \mathbb{C}. \tag{3}$$

Nótese que, si $F(x, y, z) = y^2z - x^3 - axz^2 - bz^3$, entonces

$$\nabla F = (-3x^2 - az^2, 2yz, y^2 - 2axz - 3bz^2),$$

por lo que, si $4a^3 + 27b^2 \neq 0$, entonces $Z(F)$ es una curva no singular, y si $4a^3 + 27b^2 = 0$, la curva $Z(F)$ es singular.

Sin embargo, no toda curva algebraica que satisfaga una ecuación de la forma (3) es una curva elíptica. El siguiente resultado nos proporciona una caracterización de las curvas cúbicas, y en particular nos dice cuando una curva cúbica es una curva elíptica.

Teorema 4.1 (Caracterización de las curvas elípticas)**.** *Dada la curva cúbica $\mathcal{E}_{a,b} : y^2z = x^3 + axz^2 + bz^3$, con $a, b \in \mathbb{C}$, entonces*

1. *$\mathcal{E}_{a,b}$ es una cúbica y define una curva elíptica si, y solamente si, $4a^3 + 27b^2 \neq 0$.*
2. *Toda curva elíptica es isomorfa a una curva de la forma $\mathcal{E}_{a,b}$.*
3. *Dos curvas $\mathcal{E}_{a,b}$ y $\mathcal{E}_{a',b'}$ son proyectivamente equivalentes cuando, y solamente cuando, existe $\lambda \in \mathbb{C}$ tal que $a' = \lambda^4 a$ y $b' = \lambda^6 b$; además el isomorfismo está dado por*

$$\varphi(x; y; z) = (c^2x; c^3y; z).$$

Para una demostración de éste resultado véase [3, teo. 5.3, p. 23], o bien, [4, prop. 1.4, p. 45].

Si $x^3 + ax + b = (x - x_1)(x - x_2)(x - x_3)$, realizando el cambio de coordenadas proyectivo $(x; y; z) \mapsto (X - x_1Z; Y; Z)$ tenemos $Y^2Z = X(X - (x_2 - x_1)Z)(X - (x_3 - x_1)Z)$.

Por otra parte, si ahora realizamos el cambio de coordenadas proyectivas $(X;Y;Z) \mapsto \big((x_2-x_1)x;(x_2-x_1)^{3/2}y;z\big)$ obtenemos

$$y^2z = x(x-z)\left(x - \frac{x_3-x_1}{x_2-x_1}z\right).$$

Definición 4.6. La expresión

$$\mathcal{E}_\lambda : y^2z = x(x-z)(x-\lambda z), \tag{4}$$

donde $\lambda = \dfrac{x_3-x_1}{x_2-x_1}$ se conoce como la *forma de Legendre* de la curva elíptica $\mathcal{E}_{a,b}$.

Recíprocamente, si $y^2z = x(x-z)(x-\lambda z)$ con $\lambda \neq 0,1$, por medio del cambio de variables proyectivo

$$(x;y;z) \mapsto \left(X + \frac{\lambda+1}{3}Z, Y, Z\right).$$

Se obtiene la forma de Weierstrass,

$$\mathcal{E}_{a,b} : y^2z = x^3 + axz^2 + bz^3,$$

donde

$$a = -\frac{\lambda^2-\lambda+1}{3}, \quad b = -\frac{2}{27}\lambda^3 + \frac{1}{9}\lambda^2 + \lambda - \frac{2}{27}.$$

Nótese además que

$$4a^3 + 27b^2 = -\lambda^4 + 2\lambda^3 - \lambda^2 = -\lambda^2(\lambda^2 - 2\lambda + 1) = -\lambda^2(\lambda-1)^2,$$

de donde $4a^3 + 27b^2 = 0$ si, y solamente si, $\lambda = 0$ o $\lambda = 1$.

La forma de Legendre $y^2z = x(x-z)(x-\lambda z)$ es la forma común de escribir una curva elíptica.

El valor

$$j(\mathcal{E}_{a,b}) = 1728\,\frac{4a^3}{4a^3+27b^2} = 256\,\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} = j(\mathcal{E}_\lambda).$$

es un invariante proyectivo. Véase [3, lema 10.15, p. 48].

Los valores λ, $1-\lambda$, $\dfrac{1}{\lambda}$, $\dfrac{1}{1-\lambda}$, $\dfrac{\lambda}{\lambda-1}$ y $\dfrac{\lambda-1}{\lambda}$ dan el mismo valor de $j(\mathcal{E}_\lambda)$, y por ende, las curvas elípticas asociadas a estos valores son proyectivamente equivalentes.

Teorema 4.2 (Caracterizando las curvas cúbicas)**.** *Toda cúbica irreducible es proyectivamente equivalente a una de las siguientes:*

1. $y^2z = x^3$, *es una curva singular con su punto cúspide en* $(0;0;1)$.
2. $y^2z = x^2(x+z)$, *es una curva singular con un nodo simple en* $(0;0;1)$.
3. $y^2z = x(x-z)(x-\lambda z)$, *donde* $\lambda \in \mathbb{C} \setminus \{0,1\}$. *Esta curva es no singular.*

Demostración. Para una demostración véase el libro [4, prop. 1.7]. □

5. La ley de grupo para curvas elípticas

Consideremos la cúbica no singular $\mathcal{E}$ en su forma canónica

$$y^2z = x^3 + axz^2 + bz^3$$

En particular $4a^3 + 27b^2 \neq 0$, y el punto $O = (0; 1; 0)$ es un punto de inflexión en $\mathcal{E}$, el cual corresponde al punto al infinito de la curva afín $\mathcal{E}_* : y^2 = x^3 + ax + b$. Por definición el punto O es el neutro aditivo del grupo $\mathcal{E}$.

Geométricamente, la ley de grupo sobre la curva $\mathcal{E}$ queda determinada como sigue:

Si $P = (x; y; 1) \in \mathcal{E}$, entonces $-P = (x; -y; 1)$ y además $P+Q+R = O$ si P, Q y R son colineales.

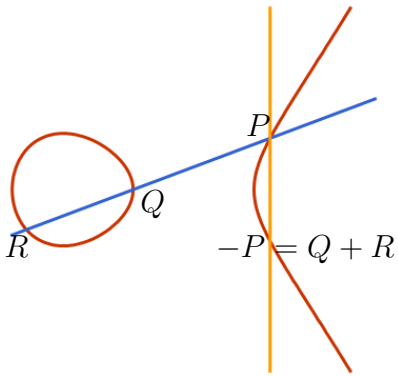


Figura 8. La ley de grupo en $\mathcal{E}$.

Como se muestra en la figura anterior, si $Q, R \in \mathcal{E}$ y ℓ es la línea que pasa por Q y R, como consecuencia de la versión débil del teorema de Bezout [2, cap. 5, §3], existe $P \in \mathcal{E}$ tal que, ℓ interseca la curva $\mathcal{E}$ exactamente en los puntos P, Q y R, lo cual denotaremos como $\ell.\mathcal{E} = P + Q + R$. (Si $Q = R$ la recta ℓ es la tangente a $\mathcal{E}$ en Q.) Sin embargo, no es útil definir la suma de Q con R como P, pues en este caso no habría un elemento identidad.

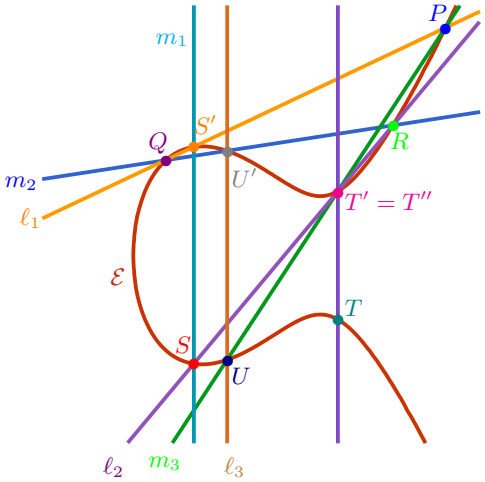
Por esta razón se define O como el punto al infinito de la curva $\mathcal{E}$ en U_2 y $Q + R = -P$, es decir, si ℓ' es la recta que pasa por O y P, entonces existe un punto $S \in \mathcal{E}$ tal que $\ell'.\mathcal{E} = O + P + S$. El punto S es, por definición, $-P = Q + R$.

Claramente la operación es cerrada, conmutativa, todo elemento tiene un inverso, así el único problema es mostrar que la operación es asociativa, lo cual es consecuencia de la siguiente proposición.

Proposición 5.1. *Si dos curvas cúbicas en $\mathbb{P}^2$ se intersecan en exactamente nueve puntos, entonces cada curva cúbica que pasa por ocho de los puntos también pasa por el noveno.*

Para una demostración de éste resultado puede verse el libro de Fulton [2, cap. 5 §6 prop. 3, p. 124], o bien, el libro de Walker [5, cap. III, 6.2].

Para ver la asociatividad de la ley de grupo, si $P, Q, R \in \mathcal{E}$, y ℓ_1 es la recta que pasa por P y Q, entonces existe $S' \in \mathcal{E}$ tal que $\ell_1.\mathcal{E} = P+Q+S'$. Además, si m_1 es la recta que pasa por O y S', se tiene que existe $S \in \mathcal{E}$ tal que $m_1.\mathcal{E} = O+S+S'$. Finalmente, existe una recta ℓ_2 con $\ell_2 \cap \mathcal{E} = S+R+T$. Análogamente, $m_2 \cap \mathcal{E} = Q+R+U$, $\ell_3 \cap \mathcal{E} = O+U+U'$ y $m_3 \cap \mathcal{E} = P+U+T''$, como se muestra en la siguiente figura:



$S = P + Q$
$T = (P + Q) + R$
$U = Q + R$
se demuestra que $T' = T''$, así
$(P + Q) + R = T = P + (Q + R)$

Figura 9. La propiedad asociativa de la ley de grupo.

Como $(P+Q)+R = -T'$ y $P+(Q+R) = -T''$, si consideramos la cúbicas $\mathcal{E}' = \ell_1\ell_2\ell_3$ y $\mathcal{E}'' = m_1m_2m_3$, entonces

$$\mathcal{E}.\mathcal{E}' = O + P + Q + R + S + S' + U + U' + T',$$

y

$$\mathcal{E}.\mathcal{E}'' = O + P + Q + R + S + S' + U + U' + T''$$

como consecuencia de la proposición (5.1) se tiene $T' = T''$, lo cual implica que la suma es asociativa. □

Aún más, los puntos de orden dos distintos de cero, es decir $P+P = O$, son de la forma $(x; 0; 1)$ donde x es una raíz cúbica de $p(x) = x^3 + ax + b$.

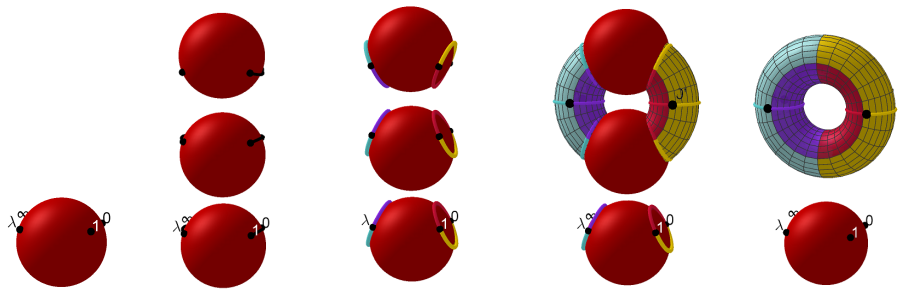
6. La superficie asociada

Dada la curva elíptica $E_\lambda : y^2z = x(x-z)(z-\lambda z)$, la aplicación natural

$$\begin{aligned} \pi : E_\lambda &\longrightarrow \mathbb{P}^1 \\ (x;y;z) &\mapsto (x;z), \quad \text{para} \quad z \neq 0, \\ (0;1;0) &\mapsto (1;0). \end{aligned}$$

es un cubriente doble de la esfera de Riemann $\mathbb{P}^1 \simeq \mathbb{S}^2$, el cual se ramifica exactamente sobre los puntos $0, 1, \lambda, \infty \in \mathbb{P}^1$.

Si realizamos cortes por curvas simples que no se intersecan, digamos de 0 a 1 y de λ a ∞ y pegamos apropiadamente los lados correspondientes, podemos ver que localmente E_λ es homeomorfo a un abierto en $\mathbb{C}$, que corresponde a una superficie de Riemann compacta de género uno, esto es, una superficie compacta con una estructura compleja y que topológicamente es un toro como se muestra en la figura a continuación:

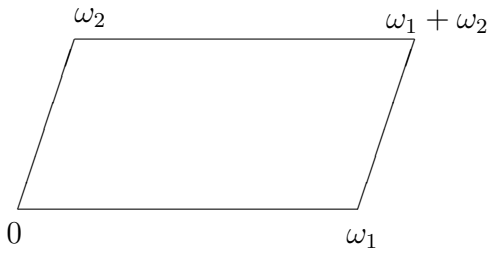


(a) Marcando **(b)** Copiando **(c)** Cortando **(d)** Pegando **(e)** El toro

Figura 10. Una curva elíptica es un toro.

Pero un toro es homeomorfo a $\mathbb{S}^1 \times \mathbb{S}^1$, o equivalentemente, a $\mathbb{C}/\mathbb{Z}^2$, por ende, el dominio fundamental de $\mathcal{E}_\lambda$ es un paralelogramo.

Para la retícula $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, con $\mathrm{Im}(\omega_1/\omega_2) > 0$, los puntos $0, \omega_1, \omega_1 + \omega_2$, y ω_2 son los vértices de un paralelogramo, denominado el *paralelogramo fundamental* de Λ.



La función $\mathcal{P}$ de Weierstrass asociada a la retícula Λ se define como

$$\mathcal{P}(\zeta) = \frac{1}{\zeta^2} + \sum_{\omega \in \Lambda^*} \left(\frac{1}{(\zeta - \omega)^2} - \frac{1}{\omega^2} \right)$$

con $\omega = m_1\omega_1 + m_2\omega_2$, y $\Lambda^* = \Lambda \setminus \{(0,0)\}$.

El desarrollo en serie de Laurent de la función $\mathcal{P}$ de Weierstrass es de la forma

$$\mathcal{P}(\zeta) = \frac{1}{\zeta^2} + \sum_{k=1}^{\infty} a_k \zeta^{2k} = \frac{1}{\zeta^2} + \sum_{k=2}^{\infty} (2k-1) G_k \, \zeta^{2k-2},$$

donde

$$G_k = \sum_{\omega \in \Lambda^*} \frac{1}{\omega^{2k}}.$$

De lo anterior es fácil ver que la función $\mathcal{P}$ satisface lo siguiente:

$$\begin{aligned}
\mathcal{P}(\zeta) &= \frac{1}{\zeta^2} + 3G_2\zeta^2 + 5G_3\zeta^4 + \cdots \\
\mathcal{P}'(\zeta) &= -\frac{2}{\zeta^3} + 6G_2\zeta + 20G_3\zeta^3 + \cdots \\
\mathcal{P}'(\zeta)^2 &= \frac{4}{\zeta^6} + 36\frac{G_2}{\zeta^2} + 60G_3 + \cdots \\
4\mathcal{P}(\zeta)^3 &= \frac{4}{\zeta^6} + \frac{36}{\zeta^2} + 60G_3 + \cdots \\
60G_2\mathcal{P}(\zeta) &= 60\frac{G_2}{\zeta^2} + 0 + \cdots
\end{aligned}$$

Consecuentemente

$$\mathcal{P}'(\zeta)^2 - 4\mathcal{P}(\zeta)^3 + 60\mathcal{P}(\zeta) = -140G_3 + \cdots$$

es una función doblemente periódica, y sin polos.

Por lo tanto

$$\mathcal{P}'(\zeta)^2 = 4\mathcal{P}(\zeta)^3 - 60G_2\mathcal{P}(\zeta) - 140G_3$$

Si $g_2 = 60G_2$ y $g_3 = 140G_3$ la ecuación anterior se transforma en

$$\mathcal{P}'(\zeta)^2 = 4\mathcal{P}(\zeta)^3 - g_2\mathcal{P}(\zeta) - g_3. \tag{5}$$

La cual es una ecuación diferencial de primer orden en $\mathcal{P}(\zeta)$.

La ecuación (5) puede resolverse explícitamente como:

$$\zeta = \int \frac{dw}{\sqrt{4w^3 - g_2 w - g_3}} + \textit{constante}.$$

Es decir, la función $\mathcal{P}$ de Weierstrass es la inversa de una integral elíptica.

De manera más precisa

$$\zeta - \zeta_0 = \int_{\mathcal{P}(\zeta_0)}^{\mathcal{P}(\zeta)} \frac{dw}{\sqrt{4w^3 - g_2 w - g_3}},$$

donde la trayectoria de integración es la imagen bajo $\mathcal{P}$ de una trayectoria de ζ_0 a ζ que evita los ceros y polos de $\mathcal{P}'(\zeta)$, y donde el signo de la raíz cuadrada debe ser igual al de $\mathcal{P}'(\zeta)$.

Supongamos que

$$\begin{aligned} \mathcal{P}'(\zeta)^2 &= 4\mathcal{P}(\zeta)^3 - g_2\mathcal{P}(\zeta) - g_3 \\ &= (\mathcal{P}(\zeta) - e_1)(\mathcal{P}(\zeta) - e_2)(\mathcal{P}(\zeta) - e_3), \end{aligned}$$

donde e_1, e_2 y e_3 son las raíces del polinomio $4w^3 - g_2 w - g_3$.

Para encontrar los valores e_k se determinan los ceros de $\mathcal{P}'(\zeta)$:

$$\mathcal{P}(\omega_1 - \zeta) = \mathcal{P}(\zeta) \quad \Rightarrow \quad \mathcal{P}'(\omega_1 - \zeta) = -\mathcal{P}'(\zeta)$$

Así $\mathcal{P}'(\omega_1/2) = 0$. Análogamente:

$$\mathcal{P}'(\omega_2/2) = 0 \quad \text{y} \quad \mathcal{P}'((\omega_1 + \omega_2)/2) = 0.$$

De donde $\dfrac{\omega_1}{2}, \dfrac{\omega_2}{2}$ y $\dfrac{\omega_1 + \omega_2}{2}$ no son congruentes por pares módulo Λ. Por lo tanto, estos puntos son precisamente los tres ceros simples de $\mathcal{P}'(\zeta)$, es decir

$$e_1 = \mathcal{P}\left(\frac{\omega_1}{2}\right),\ e_2 = \mathcal{P}\left(\frac{\omega_2}{2}\right),\ e_3 = \mathcal{P}\left(\frac{\omega_1 + \omega_2}{2}\right).$$

Esto es, la curva elíptica

$$y^2 = 4x^3 - g_2 x - g_3$$

queda parametrizada por $x = \mathcal{P}(\zeta), \quad y = \mathcal{P}'(\zeta)$.

Por ejemplo, si $y^2 = 4x^3 - x$, los periodos se expresan como las integrales elípticas

$$\begin{aligned} \omega_1 &= 2\int_{1/2}^{\infty} \frac{dx}{\sqrt{4x^3 - x}} \approxeq 3.7081, \\ \omega_2 &= 2\imath\int_{-\infty}^{-1/2} \frac{dx}{\sqrt{4x^3 - x}} \approxeq 3.7081\imath. \end{aligned}$$

En este caso, la curva elíptica tiene como dominio fundamental un cuadrado, cuyos lados se identifican para formar el toro.

7. Conclusión

Así, a lo largo de la presente nota hemos visto que, cuando trabajamos sobre el campo de los números complejos, una curva elíptica siempre admite una representación canónica, también conocida como su forma de Weierstrass y, vía un cambio de variables, la curva elíptica puede reescribirse en la forma $y^2z - x^3 - axz^2 - bz^3 = 0$ la cual tiene un único punto al infinito en $O = (0; 1; 0)$. Que una curva cúbica satisfaga una ecuación de Wierstrass no implica que la curva sea una curva elíptica, ya que puede tener puntos singulares, y la condición $4a^3 + 27b^2 \neq 0$ equivale a pedir que dicha curva sea no singular Además, las curvas elípticas admiten una estructura de grupo, lo cual es importante en la teoría de códigos y la criptografía.

Vimos que una curva elíptica también tiene asociada una forma de Legendre, y que dos curvas elípticas son equivalentes cuando tienen el mismo $j-$invariante, lo cual demuestra que las curvas elípticas están parametrizadas por un número complejo λ, módulo razón cruzada.

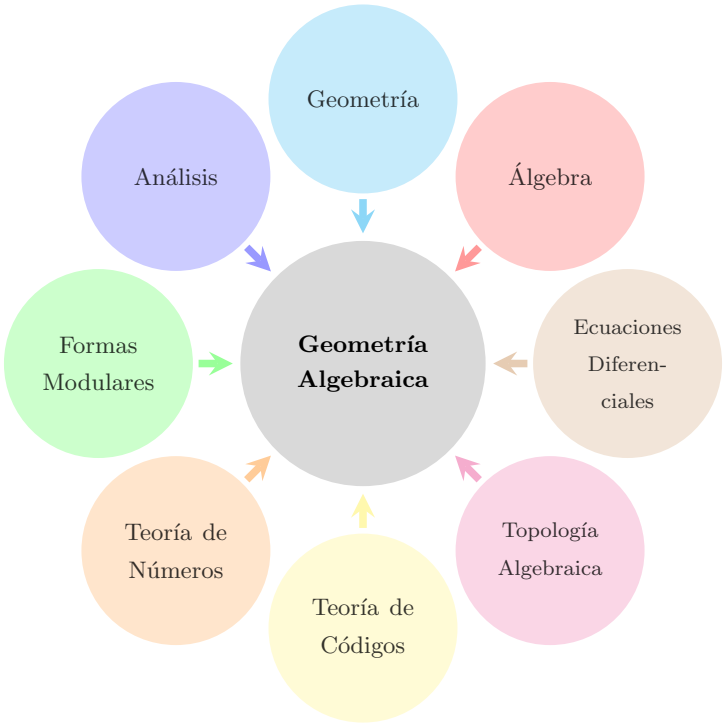
Al escribir una cúbica no singular en su forma de Legendre, se tiene asociada de manera natural, un superficie de género uno ramificada sobre los puntos $0, 1, \infty, \lambda$. Y como toda superficie de género uno es de la forma $\mathbb{C}/\Lambda$, para un retículo Λ. La función $\mathcal{P}$ de Weierstrass asociada a Λ, es una función meromorfa, que satisface una ecuación diferencial de primer orden en $\mathcal{P}$, la cual es la inversa de una integral elíptica, de aquí el nombre de curvas elípticas. A su vez, la curva elíptica $y^2 = 4x^3 - g_2x - g_3$, queda parametrizada por $x = \mathcal{P}(\zeta), y = \mathcal{P}'(\zeta)$.

En otras palabras, un objeto algebraico, a saber una ecuación polinomial, determina un objeto geométrico la superficie de Riemann asociada $\mathbb{C}/\Lambda$, y este a su vez un objeto analítico, la función meromorfa $\mathcal{P}_\Lambda$ de Weierstrass, y recíprocamente.

A curvas de grados superiores se les puede asociar superficies de Riemann, esto es, las superficies de Riemann son dominios de funciones multivariables. Sin embargo, las curvas de grados superiores no tienen una estructura de grupo, se les puede asociar de manera natural un grupo topológico encajable en un espacio proyectivo, denominado su variedad jacobiana, y el estudio de la curva, la superficie de Riemann asociada y la variedad jacobiana son equivalentes.

Además, las superficies de Riemann de géneros superiores son los lugares naturales para resolver algunas ecuaciones diferenciales parciales tales como la ecuación del calor, la ecuación Kadomstev Petviashvilli que es una ecuación diferencial parcial que ayuda a describir el movimiento de onda no lineal y la ecuación Korteweg de Vries que describe, en una dimensión espacial, la propagación de ondas de longitud de onda larga en medios dispersivos.

Esperamos que el presente trabajo motive a los jóvenes en el estudio del presente tema, así como el de las áreas afines, entre las cuales tenemos:



Bibliografía

[1] R. Bix, *Conics and Cubics. A concrete Introduction to Algebraic Curves*, 2.ª ed., Springer, New York, 2006.
[2] W. Fulton, *Algebraic Curves*, Benjamin, Elmsford, New York, 1969.
[3] J. Milne, «Elliptic Curves», notes for Math 679, Univesity of Michigan, Winter 1996. Hay una versión posterior, corregida y aumentada del 2006 que puede encontrarse en la siguiente liga: `http://www.jmilne.org/math/Books/ectext6.pdf`.
[4] J. H. Silverman, *The Aritmetic of Elliptic Curves*, 2.ª ed., Springer, New York, 2009.
[5] R. Walker, *Algebraic Curves*, Springer-Verlag, New York, 1978.