Curvas elípticas

En esta parte trabajaremos con un cuerpo K y denotaremos K^2 al plano afín y $\mathbb{P}^2(K)$ al plano proyectivo. El cuerpo $\overline{K}$ es la clausura algebraica de K. Al conjunto de ceros de un polinomio homogéneo $F \in K[x,y,z]$ no nulo

$$\mathcal{C}_F = \left\{ [x_0 : y_0 : z_0] \in \mathbb{P}^2(\overline{K}) \ : \ F(x_0, y_0, z_0) = 0 \right\}$$

se lo llama *curva algebraica plana proyectiva definida sobre* K. Por conveniencia denotaremos $\mathcal{C}_F(K)$ a los puntos de la curva con coordenadas en K, es decir, $\mathcal{C}_F \cap \mathbb{P}^2(K)$.

Lema 8.1. *Consideremos una curva $\mathcal{C}_F$ dada por un polinomio homogéneo (no nulo) $F \in \overline{K}[x,y,z]$ de grado $d \geq 0$ y sea $L(x,y,z) = ax + by + cz \in \overline{K}[x,y,z]$ un polinomio lineal (no nulo) que no divide a $F(x,y,z)$. Entonces $|\mathcal{C}_F \cap \mathcal{C}_L| \leq d$.*

Proof. Supongamos sin pérdida de generalidad que $a \neq 0$. Sustituyendo $x = -\frac{by+cz}{a}$ en $F(x,y,z) = 0$ obtenemos un polinomio homogéneo $G(y,z) \in \overline{K}[y,z]$ cuyos ceros $[y_0 : z_0]$ están en correspondencia uno a uno con los puntos de la intersección $\mathcal{C}_F \cap \mathcal{C}_L$. Por construcción, se tiene que $F \equiv G \pmod{L}$ en $\overline{K}[x,y,z]$. Como $L \nmid F$ y L es irreducible (por ser de grado 1), se sigue que $L \nmid G$ y en particular, G es un polinomio no nulo. Además, por construcción, G es homogéneo de grado d. Cada cero $[y_0 : z_0]$ de G corresponde con el factor lineal $y_0 z - z_0 y$, o un asociado, en la factorización de G. Esto prueba que no puede haber mas de d ceros. □

El lema 8.1 nos da una idea de como definir la multiplicidad de intersección $\mathrm{mult}_P(L,F)$ de una función lineal no nula $L = ax + by + cz \in \overline{K}[x,y,z]$ y un polinomio homogéneo no nulo $F \in \overline{K}[x,y,z]$ de grado d en un punto común $P = [x_0 : y_0 : z_0] \in \mathcal{C}_L \cap \mathcal{C}_F$. Suponiendo que $a \neq 0$ y que $L \nmid F$, podemos hacer la sustitución $G(y,z) = F(-\frac{by+cz}{a}, y, z)$ como en la demostración del lema y definir la multiplicidad de intersección como el orden con el que factor $y_0 z - z_0 y$ aparece en $G(y,z)$.

$$\mathrm{mult}_P(L,F) = \max \left\{ n \geq 0 \ : \ (y_0 z - z_0 y)^n \mid F\left(-\frac{by+cz}{a}, y, z \right) \right\} \qquad \text{si } a \neq 0 \text{ y } L \nmid F$$

De ese modo tenemos que la suma de las multiplicidades de intersección de todos los puntos comunes es *exactamente* d por estar trabajando en el cuerpo algebraicamente cerrado $\overline{K}$.

$$\sum_{P \in \mathcal{C}_L \cap \mathcal{C}_F} \mathrm{mult}_P(L,F) = \deg(G) = \deg(F) = d \tag{1}$$

Por coherencia, deberíamos comprobar que si la función lineal tiene también $b \neq 0$ y hacemos la sustitución $H(x,z) = F(x, -\frac{ax+cz}{b}, z)$, el orden con el que el factor $z_0 x - x_0 z$ aparece en H coincide con el que definimos antes.

$$\begin{aligned}
& (z_0 x - x_0 z)^n \mid H(x,z) \\
\iff \quad & (z_0 x - x_0 z)^n \mid F\left(x, -\frac{ax+cz}{b}, z \right) \\
\iff \quad & \left(z_0 (-\frac{by+cz}{a}) - x_0 z \right)^n \mid F\left(-\frac{by+cz}{a}, y, z \right) \\
\iff \quad & (-b z_0 y - c z_0 z - a x_0 z)^n \mid G(y,z) \\
\iff \quad & (-b z_0 y + b y_0 z)^n \mid G(y,z) \\
\iff \quad & (z_0 y - y_0 z)^n \mid G(y,z)
\end{aligned}$$

La segunda implicación se sigue de hacer el cambio de variables $x = -\frac{by+cz}{a}$ y la penúltima de que el punto $[x_0 : y_0 : z_0]$ satisface la ecuación de la recta L. Con esta comprobación vemos que en realidad podemos "despejar" cualquiera de las variables de la función lineal (siempre que su coeficiente sea no nulo), sustituirlo en $F(x, y, z)$ y luego mirar en el polinomio que queda de dos variables cuales son las multiplicidades.

$$\operatorname{mult}_P(L, F) = \max\left\{n \geq 0 \,:\, (z_0x - x_0z)^n \mid F\left(x, -\frac{ax+cz}{b}, z\right)\right\} \qquad \text{si } b \neq 0 \text{ y } L \nmid F$$

$$\operatorname{mult}_P(L, F) = \max\left\{n \geq 0 \,:\, (y_0x - x_0y)^n \mid F\left(x, y, -\frac{ax+by}{c}\right)\right\} \qquad \text{si } c \neq 0 \text{ y } L \nmid F$$

Veamos ahora otra forma de calcular la multiplicidad de interescción. Supongamos nuevamente $a \neq 0$ y sea $P = [x_0 : y_0 : z_0] \in \mathcal{C}_L \cap \mathcal{C}_F$. No puede ser $y_0 = z_0 = 0$, ya que en ese caso tendríamos $x_0 = 0$ por la ecuación de la recta, lo que no define ningún punto. Supongamos que $z_0 \neq 0$. Podemos parametrizar la recta L en el plano afín $z = z_0$

$$\begin{aligned} x &= x_0 + \frac{bt}{a} \\ y &= y_0 - t \\ z &= z_0 \end{aligned}$$

utilizando el parámetro t. Si sustituimos esto en el polinomio F, nos queda

$$R(t) = F\left(x_0 + \frac{bt}{a}, y_0 - t, z_0\right) \in \overline{K}[t]$$

y la multiplicidad de intersección $\operatorname{mult}_P(L, F)$ será la mayor potencia de t que divide a $R(t)$. Tenemos que comprobar que esta definición coincide con la que vimos antes.

$$\begin{aligned} & t^n \mid R(t) \\ \iff \quad & t^n \mid F\left(x_0 + \frac{bt}{a}, y_0 - t, z_0\right) \\ \iff \quad & t^n \mid F\left(\frac{x_0z}{z_0} + \frac{bt}{a}, \frac{y_0z}{z_0} - t, z\right) \\ \iff \quad & \left(\frac{y_0z}{z_0} - y\right)^n \mid F\left(\frac{x_0z}{z_0} + \frac{b}{a}\left(\frac{y_0z}{z_0} - y\right), y, z\right) \\ \iff \quad & (y_0z - z_0y)^n \mid F\left(\frac{ax_0z + by_0z - az_0y}{bz_0}, y, z\right) \\ \iff \quad & (y_0z - z_0y)^n \mid F\left(\frac{-cz - ay}{b}, y, z\right) \\ \iff \quad & (y_0z - z_0y)^n \mid G(y, z) \end{aligned}$$

La segunda implicación se obtiene homogeneizando, la siguiente haciendo el cambio de variables $t = y_0z/z_0 - y$ y la penúltima utilizando que P satisface la ecuación de la recta.

Hemos sido cuidadosos de hablar siempre de la multiplicidad de intersección de los polinomios L y F y no de las curvas $\mathcal{C}_L$ y $\mathcal{C}_F$. Si bien esta diferencia de lenguaje no afecta en absoluto a lo de la recta, puede haber ambigüedades en el caso de la curva. El problema proviene de que puede haber muchos polinomios que definan exactamente la misma curva. Por ejemplo, si consideramos $F_1 = (xz - y^2 + z^2)^3(x^3 + 3xz^2)^8 \in \mathbb{C}[x, y, z]$ y $F_2 = (xz - y^2 + z^2)(x^3 + 3yz^2) \in \mathbb{C}[x, y, z]$, ambos definen la misma curva $\mathcal{C}_{F_1} = \mathcal{C}_{F_2}$. Si quitamos las potencias de los factores, este problema desaparece.

Teorema 8.2. *Hay una correspondencia biyectiva entre curvas algebraicas planas proyectiva y polinomios de $\overline{K}[x, y, z]$ que no tienen factores repetidos (libres de cuadrados) salvo constantes multiplicativas.*

Gracias al teorema 8.2 tiene sentido ahora hablar tanto del grado de una curva algebraica plana proyectiva como de la multiplicidad de intersección de una recta y una curva. En ambos casos se utiliza el (único) polinomio libre de cuadrados que define la curva.

Si una recta corta a una curva con multiplicidad mayor o igual que 2, se dice que es *tangente* a la curva. Un punto de la curva por el que solo pasa una recta tangente se dice *simple* y en caso contrario se dice *singular*.

Consideremos una curva $\mathcal{C}_F$ con F libre de cuadrados y un punto $P = [x_0 : y_0 : z_0]$ en la curva. Vamos a ver que si $\nabla F(P) \neq (0,0,0)$, entonces la recta

$$\frac{\partial F}{\partial x}(P) \cdot x + \frac{\partial F}{\partial y}(P) \cdot y + \frac{\partial F}{\partial z}(P) \cdot z = 0$$

pasa por P y es la única tangente a la curva. Lo primero se deduce de la identidad de Euler

$$\frac{\partial F}{\partial x} \cdot x + \frac{\partial F}{\partial y} \cdot y + \frac{\partial F}{\partial z} \cdot z = \deg(F) \cdot F$$

sustituyendo el punto P. Para ver que esta recta es tangente, supongamos que $a = \frac{\partial F}{\partial x}(P) \neq 0$ y $z_0 \neq 0$. Tenemos que comprobar que t^2 divide a $F(x_0 + bt/a, y_0 - t, z_0)$, donde $b = \frac{\partial F}{\partial y}(P)$. Desarrollando en potencias de t, tenemos que

$$F\left(x_0 + \frac{bt}{a}, y_0 - t, z_0\right) = F(P) + \left(\frac{b}{a}\frac{\partial F}{\partial x}(P) - \frac{\partial F}{\partial y}(P)\right) \cdot t + \text{términos con } t^2 + \cdots$$

en donde se ve claramente que el término independiente y el lineal se anulan. Por otra parte, si $ax + by + cz = 0$ es una tangente cualquiera en P (con $a \neq 0$), repetimos el razonamiento y llegamos a que $a = \frac{\partial F}{\partial x}(P)$ (sin pérdida de generalidad) y $b = \frac{\partial F}{\partial y}(P)$, ya que debe ser

$$\frac{b}{a}\frac{\partial F}{\partial x}(P) - \frac{\partial F}{\partial y}(P) = 0.$$

Utilizando que $ax_0 + by_0 + cz_0 = 0$ y la identidad de Euler, nos queda que también será

$$c = -\frac{ax_0 + by_0}{z_0} = -\frac{\frac{\partial F}{\partial x}(P) \cdot x_0 + \frac{\partial F}{\partial y}(P) \cdot y_0}{z_0} = \frac{\partial F}{\partial z}(P)$$

lo que demuestra la unicidad de la recta tangente.

Teorema 8.3. *Sea $F \in \overline{K}[x,y,z]$ un polinomio homogéneo no nulo libre de cuadrados. Un punto $P \in \mathcal{C}_F$ es simple si y solo si $\nabla F(P) \neq (0,0,0)$. En este caso, la ecuación de la única recta tangente es $\nabla F(P) \cdot (x,y,z) = 0$.*

Vamos a necesitar algunos resultados básicos de geometría algebraica. En una primera lectura, se pueden omitir las demostraciones, ya que son bastante complicadas.

Teorema 8.4. *Sean $F, G \in K[x,y,z]$ polinomios homogéneos mónicos en x de grados $d = \deg(F) \geq 1$ y $e = \deg(G) \geq 1$. Son equivalentes:*

1. *Existe $H \in K[x,y,z]$ homogéneo de grado $\deg(H) \geq 1$ tal que $H \mid F$ y $H \mid G$.*
2. *Existen $A, B \in K[x,y,z]$ homogéneos no nulos tales que $AF + BG = 0$, $\deg_x(A) \leq e - 1$ y $\deg_x(B) \leq d - 1$.*

3. *El determinante de la matriz*

$$\begin{bmatrix} F_0(y,z) & F_1(y,z) & \cdots & F_d(y,z) & & & \\ & F_0(y,z) & F_1(y,z) & \cdots & F_d(y,z) & & \\ & & \ddots & & & \ddots & \\ & & & F_0(y,z) & F_1(y,z) & \cdots & F_d(y,z) \\ G_0(y,z) & G_1(y,z) & \cdots & \cdots & G_e(y,z) & & \\ & \ddots & & & & \ddots & \\ & & G_0(y,z) & G_1(y,z) & \cdots & \cdots & G_e(y,z) \end{bmatrix} \in K[y,z]^{(d+e)\times(d+e)}$$

es cero.

Proof. $(1 \Rightarrow 2)$: Como los polinomios F y G son mónicos en x, cualquier factor común H tendrá $\deg_x(H) \geq 1$. Basta tomar $A = G/H$ y $B = -F/H$.
$(2 \Rightarrow 1)$: Supongamos que no existe H. Esto significa que F y G no tienen ningún factor común en $K[x,y,z]$. Como $F \mid BG$ y $K[x,y,z]$ es un dominio de factorización única, debe ser $F \mid B$. Esto es una contradicción, ya que $\deg_x(B) < \deg_x(F) = \deg(F)$.
$(2 \Rightarrow 3)$: El sistema de ecuaciones $AF+BG = 0$ tiene solución (no nula) en $K[y,z]$ donde las incógnitas son los e coeficientes de A y los d coeficientes de B. Como hay $d+e$ incógnitas y $d+e$ ecuaciones y el sistema es homogéneo, se sigue que el determinante del sistema es cero. La matriz de este sistema es la traspuesta de la matriz de arriba.
$(3 \Rightarrow 2)$: Analizando el mismo sistema de ecuaciones, sabemos que debe existir una solución no nula en $K(y,z)$ para los coeficientes de A y B, ya que el determinante del sistema homogéneo es cero. Limpiando denominadores (lo que solo requiere multiplicar por polinomios en $K[y,z]$), obtenemos $A, B \in K[x,y,z]$ con $\deg_x(A) \leq e-1$ y $\deg_x(B) \leq d-1$. □

Al determinante de la matriz de arriba se lo llama *resultante de F y G con respecto a la variable x* y se lo escribe $\mathrm{Res}_x(F,G)$.

Teorema 8.5. *Sean $F, G \in K[x,y,z]$ polinomios homogéneos mónicos en x de grados $d = \deg(F) \geq 1$ y $e = \deg(G) \geq 1$. Entonces $\mathrm{Res}_x(F,G) \in K[y,z]$ es cero o un polinomio homogéneo de grado de y existen $A, B \in K[x,y,z]$ homogéneos de grados $\deg_x(A) \leq e-1$ y $\deg_x(B) \leq d-1$ tales que $\mathrm{Res}_x(F,G) = AF + BG$.*

Proof. El determinante de la matriz M es una suma de $(d+e)!$ productos de la forma

$$M_{1,\sigma(1)} M_{2,\sigma(2)} \cdots M_{d+e,\sigma(d+e)}$$

donde σ es una permutación de las $d+e$ columnas. Cada una de las entradas es cero o un polinomio homogéneo. Veremos que cada sumando no nulo es siempre de grado de. En efecto, $\deg(M_{i,\sigma(i)}) = d - i + \sigma(i)$ para $i = 1, \ldots, e$ y $\deg(M_{i,\sigma(i)}) = e + 1 - i + \sigma(i)$ para $i = e+1, \ldots, e+d$. Sumando para $i = 1, \ldots, d+e$ nos queda grado de. Para la otra parte, supondremos que $\mathrm{Res}_x(F,G) \neq 0$, ya que el caso cero lo analizamos en el teorema anterior. Aplicamos la regla de Cramer al sistema de ecuaciones $AF + BG = 1$ con incógnitas los coeficientes de A y B en $K(y,z)$. El único denominador que aparece es el determinante del sistema $\mathrm{Res}_x(F,G)$. Limpiando ese denominador, obtenemos a la resultante como combinación lineal (con coeficientes en $K[x,y,z]$) de F y G. En caso de que A y B no sean homogéneos, podemos simplemente extraer sus partes homogéneas de grado $d(e-1)$ y $(d-1)e$. □

Teorema 8.6 (Bezout)**.** *Sean $F, G \in \overline{K}[x,y,z]$ polinomios homogéneos no nulos de grados $d = \deg(F) \geq 1$ y $e = \deg(G) \geq 1$. Entonces sucede una y solo una de las siguientes:*

1. *F y G tienen un factor común $H \in \overline{K}[x,y,z]$ de grado $\deg(H) \geq 1$*
2. *$|\mathcal{C}_F \cap \mathcal{C}_G| \leq de$.*

Proof. Aplicando un cambio lineal de variables genérico, podemos suponer sin pérdida de generalidad que F y G son mónicos en x. Si no sucede (1), el teorema 8.4 nos dice que $\mathrm{Res}_x(F,G)$ es un polinomio no nulo y el teorema 8.5, nos dice que es homogéneo de grado de. Cada punto $[x:y:z] \in \mathcal{C}_F \cap \mathcal{C}_G$ nos da un cero $[y:z]$ de la resultante, ya que esta es combinación lineal de F y G. En particular, hay a lo sumo de posibles $[y:z]$. Sustituyendo estos en F, obtenemos un polinomio mónico en x y por lo tanto finitos posibles valores de x en $\overline{K}$ que satisfacen esa ecuación. Esto implica que la intersección de las curvas es finita. Nuevamente haciendo un cambio lineal genérico de coordenadas, podemos suponer sin pérdida de generalidad que todos los puntos de la intersección tienen $[y:z]$ distintos, lo que prueba (2). Solo resta ver que si sucede (1), no puede suceder (2). Esto es inmediato ya que cualquier polinomio H de grado $\deg(H) \geq 1$ tiene infinitas soluciones en el cuerpo $\overline{K}$ y además $\mathcal{C}_H \subseteq \mathcal{C}_F \cap \mathcal{C}_G$. □

Proof of theorem 8.2. En primer lugar, observemos que cualquier curva puede ser definida por un polinomio libre de cuadrados en $\overline{K}[x,y,z]$. Lo que resta ver es que si tenemos dos polinomios $F, G \in \overline{K}[x,y,z]$ libres de cuadrados distintos, entonces $\mathcal{C}_F \neq \mathcal{C}_G$. Sea H un factor irreducible de F que no esté en G. Aplicando el teorema de Bezout, sabemos que $\mathcal{C}_H \cap \mathcal{C}_G$ es un conjunto finito. Como $\mathcal{C}_H$ es infinito, podemos elegir $P \in \mathcal{C}_H \setminus \mathcal{C}_G$. Ese punto también estará en $\mathcal{C}_F$, ya que $H \mid F$. Esto prueba que en $\mathcal{C}_F$ hay al menos un punto que no está en $\mathcal{C}_G$, tal como afirmábamos. □

Teorema 8.7. *Sea $F, G \in \overline{K}[x,y,z]$ polinomios homogéneos no nulos de grados $d = \deg(F) \geq 1$ y $e = \deg(G) \geq 1$. Entonces $\mathcal{C}_F \cap \mathcal{C}_G \neq \emptyset$.*

Proof. A través de un cambio genérico lineal de coordenadas, podemos suponer sin pérdida de generalidad que F y G son mónicos en x. En el caso de que F y G tengan un factor común H, esto es inmediato, ya que cualquier punto $P \in \mathcal{C}_H(\overline{K})$ cumple lo pedido (y hay infinitos de estos). En el otro caso, sabemos que $\mathrm{Res}_x(F,G) = AF + BG \in \overline{K}[y,z]$ es un polinomio homogéneo no nulo de grado $de \geq 1$ (por los teoremas 8.4 y 8.5) para ciertos $A, B \in \overline{K}[x,y,z]$. Como estamos trabajando sobre el cuerpo algebraicamente cerrado $\overline{K}$, existirá un $[y_0:z_0]$ que anule a la resultante. Los polinomios $F(x, y_0w, z_0w), G(x, y_0w, z_0w) \in \overline{K}[x,w]$ homogéneos (mónicos en x) satisfacen

$$A(x,y_0w,z_0w)F(x,y_0w,z_0w) + B(x,y_0w,z_0w)G(x,y_0w,z_0w) = \mathrm{Res}_x(F,G)(y_0w,z_0w) = 0$$

y por lo tanto tienen un factor común en $\overline{K}[x,w]$ (con el mismo razonamiento que en la implicación $2 \Rightarrow 1$ del teorema 8.4). Tomando un cero $[x_0 : w_0]$ de ese factor común, obtenemos el punto $[x_0 : y_0w_0 : z_0w_0]$ que anula a F y G. □

Definición 8.8. Una *curva elíptica definida sobre K* es una curva proyectiva plana $\mathcal{C}_F$ para un cierto $F \in K[x,y,z]$ homogéneo no nulo de grado 3 tal que:

1. $\mathcal{C}_F(K) \neq \emptyset$.
2. Para todo $P \in \mathcal{C}_F$ se tiene

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

es decir, $\mathcal{C}_F$ es una curva *lisa* (sin puntos singulares).

Una curva elíptica $\mathcal{C}_F$ siempre está dada por un polinomio irreducible en $\overline{K}[x,y,z]$. En efecto, si el polinomio F se pudiera factorizar como $F = GH$ para ciertos $G, H \in \overline{K}[x,y,z]$ homogéneos (de grados ≥ 1), podríamos tomar un punto P tal que $G(P) = H(P) = 0$ (por el teorema 8.7) y comprobar que

$$\nabla F(P) = \nabla(GH)(P) = G(P) \cdot \nabla H(P) + H(P) \cdot \nabla G(P) = (0,0,0)$$

lo que contradice la propiedad (2) de la definición 8.8.

Recordemos que una recta corta a una curva elíptica en exactamente 3 puntos (contados con multiplicidades).

Definición 8.9. Sea $\mathcal{C}_F$ una curva elíptica definida sobre K. Sean $P, Q \in \mathcal{C}_F(K)$ puntos de la curva (pueden ser el mismo). Entonces la recta que pasa por P y Q (la tangente en caso de ser $P = Q$) corta a la curva en un tercer punto que se denota $P * Q \in \mathcal{C}_F(K)$ (que también podría ser el mismo).

Para que la definición anterior tenga sentido, habría que comprobar que el punto $P*Q$ está en $\mathcal{C}_F(K)$. Para esto, basta ver que la recta que pasa por los dos puntos P y Q (o la tangente si $P = Q$) tiene coeficientes en K y que si un polinomio homogéneo de grado 3 en $K[y, z]$ tiene dos factores en $K[y, z]$, el tercer factor también lo estará.

Definición 8.10. Sea $\mathcal{C}_F$ una curva elíptica definida sobre K y sea $\mathcal{O} \in \mathcal{C}_F(K)$ un punto fijo de la curva. La operación $+ : \mathcal{C}_F(K) \times \mathcal{C}_F(K) \to \mathcal{C}_F(K)$ se define como $P + Q = \mathcal{O} * (P * Q)$.

Teorema 8.11. *Sea $\mathcal{C}_F$ una curva elíptica definida sobre K y sea $\mathcal{O} \in \mathcal{C}_F(K)$ un punto fijo de la curva. Entonces $(\mathcal{C}_F(K), +)$ es un grupo abeliano con neutro $\mathcal{O}$.*

Antes de demostrar nuestro resultado principal sobre curvas elípticas, necesitaremos dos resultados importantes.

Proposición 8.12. *Sean $A_1, \ldots, A_8 \in \mathbb{P}^2(\overline{K})$ tales que no hay 4 alineados y no hay 7 en una cónica (una curva algebraica proyectiva de grado 2). Entonces el $\overline{K}$-espacio vectorial*

$$\mathbb{S} = \left\{F \in \overline{K}[x, y, z] \text{ homogéneo de grado } 3 \,:\, F(A_1) = \cdots = F(A_8) = 0\right\}$$

tiene dimensión 2.

Proof. El espacio de los polinomios homogéneos de grado 3 tiene dimensión 10, ya que hay 10 coeficientes en esos polinomios. Cada ecuación $F(A_i) = 0$ es lineal en los coeficientes. Como hay 8 ecuaciones, tenemos que $\dim(\mathbb{S}) \geq 2$. Lo que resta ver es que estas ecuaciones son linealmente independientes. Para eso, bastará con demostrar que siempre hay un polinomio $F \in \overline{K}[x, y, z]$ tal que $F(A_1) = \cdots = F(A_7) = 0$ pero $F(A_8) \neq 0$. Consideramos los siguientes polinomios:

$$F_1 = Q_{A_1A_2A_3A_4A_5} \cdot L_{A_6A_7}$$
$$F_2 = Q_{A_1A_2A_3A_4A_6} \cdot L_{A_5A_7}$$
$$F_3 = Q_{A_1A_2A_3A_4A_7} \cdot L_{A_5A_6}$$

donde Q_{ABCDE} denota un polinomio homogéneo no nulo de grado 2 (cónica) que se anula en $ABCDE$ y L_{AB} es un polinomio homogéneo no nulo de grado 1 (recta) que se anula en AB. La existencia de las cónicas está garantizada porque hay 6 coeficientes y solo 5 restricciones lineales. Así hemos producido tres polinomios homogéneos F_1, F_2 y F_3 de grado 3 no nulos. Veamos que alguno de estos no se anulará en A_8. Procederemos por contradicción, es decir, supondremos que $F_1(A_8) = F_2(A_8) = F_3(A_8) = 0$. Sabemos que el punto A_8 no puede estar en dos de las rectas $L_{A_6A_7}$, $L_{A_5A_7}$, $L_{A_5A_6}$ ya que en caso contrario habría 4 puntos alineados. Esto demuestra que A_8 debe estar en dos de las cónicas, que sin pérdida de generalidad supondremos que $Q_{A_1A_2A_3A_4A_5}(A_8) = 0$ y $Q_{A_1A_2A_3A_4A_6}(A_8) = 0$. Si estas dos cónicas no comparten un factor común, el teorema de Bezout nos dice que se cortarían en a lo sumo 4 puntos, pero estas tienen en común a $A_1A_2A_3A_4A_8$. Entonces deben tener un factor común. La posibilidad de que ambas cónicas coincidan queda descartada puesto que si no tendríamos los 7 puntos $A_1A_2A_3A_4A_5A_6A_8$ en una cónica. La única posibilidad que queda es que el factor común sea de grado 1, es decir,

$$Q_{A_1A_2A_3A_4A_5A_8} = L_1 \cdot L_2$$
$$Q_{A_1A_2A_3A_4A_6A_8} = L_1 \cdot L_3$$

para ciertas rectas $L_1, L_2, L_3 \in \overline{K}[x, y, z]$ y la recta L_2 distinta de la L_3. Como estas cónicas tienen 5 puntos en común $A_1A_2A_3A_4A_8$ y las rectas L_2 y L_3 se cortan en a lo sumo un punto, tendrá que haber al menos 4 de esos puntos en L_1. Contradicción. □

Teorema 8.13 (Cayley-Bacharach)**.** *Sean $F, G, H \in \overline{K}[x, y, z]$ polinomios homogéneos de grado 3 no nulos con F irreducible. Supongamos que $\mathcal{C}_G$ y $\mathcal{C}_H$ se intersectan en 9 puntos* distintos *$A_1, A_2, \ldots, A_9$ y que F se anula en $A_1, \ldots, A_8$. Entonces F también se anulará en A_9.*

Proof. Empecemos por observar que los puntos $A_1, \ldots, A_8$ satisfacen las hipótesis de la proposición anterior. Por Bezout cualquier recta cortará a $\mathcal{C}_F$ en a lo sumo 3 puntos y cualquier cónica cortará a $\mathcal{C}_F$ en a lo sumo 6 puntos, ya que F no tiene factor común con ningún polinomio de grado 1 y 2 por ser irreducible. También es claro que $F, G, H \in \mathcal{S}$. El polinomio G no puede ser un múltiplo escalar de H, ya que si no $\mathcal{C}_G = \mathcal{C}_H$ y su intersección sería infinita. Como $\dim(\mathbb{S}) = 2$, debe ser $\mathbb{S} = \langle G, H\rangle$ y por lo tanto F es combinación lineal de G y H. Como $G(A_9) = H(A_9) = 0$, también se tiene $F(A_9) = 0$. □

Sketch of the proof of theorem 8.11. La operación $*$ es conmutativa por definición, por lo que la operación de suma también lo será: $P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * (Q * P) = Q + P$. El elemento $\mathcal{O}$ es el neutro aditivo, ya que $\mathcal{O} + P = \mathcal{O} * (\mathcal{O} * P) = P$ por definición. El inverso aditivo de un P es $Q = (\mathcal{O} * \mathcal{O}) * P$. En efecto,

$$P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * (P * ((\mathcal{O} * \mathcal{O}) * P)) = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O}.$$

Solo falta demostrar la asociatividad de la suma, es decir, que $P + (Q + R) = (P + Q) + R$. Esto es equivalente a ver que $P * (Q + R) = (P + Q) * R$. Consideremos los polinomios homogéneos de grado 3 dados por los siguientes productos de tres rectas:

$$G = L_{\mathcal{O},P*Q,P+Q} \cdot L_{Q,R,Q*R} \cdot L_{P,Q+R,P*(Q+R)}$$
$$H = L_{\mathcal{O},Q*R,Q+R} \cdot L_{P,Q,P*Q} \cdot L_{R,P+Q,(P+Q)*R}$$

Por construcción G y H se anulan en los ocho puntos $\mathcal{O}$, P, Q, R, $P * Q$, $P + Q$, $Q * R$, $Q + R$. Como estos 8 están sobre la curva elíptica, el noveno punto de intersección $\mathcal{C}_G \cap \mathcal{C}_H$ también estará sobre $\mathcal{C}_F$. Como F y G se cortan en los ocho puntos mencionados antes y en $P * (Q + R)$, debe ser que el noveno punto de intersección de G y H sea $P * (Q + R)$. Haciendo el razonamiento simétrico, cambiando G por H, concluímos que el noveno punto es $(P + Q) * R$. Esto prueba que $P * (Q + R) = (P + Q) * R$, tal como queríamos. Un detalle técnico es que este razonamiento asume que los nueve puntos son distintos entre sí. Dejo como ejercicio (difícil) completar los casos que faltan. □

Problema 8.1. Las curvas *cusp* y *node* se definen con las ecuaciones $y^2z - x^3 = 0$ y $y^2z - x^3 - x^2z = 0$, respectivamente. Mostrar que el punto $S = [0 : 0 : 1]$ está en ambass curvas y es su único punto singular.

Problema 8.2. Calcular los puntos de intersección de la recta $x + y = 0$ con las curvas cusp y node y en cada uno de esos puntos, las multiplicidades de intersección.

Problema 8.3. Sea K un cuerpo con $\text{char}(K) \neq 2$. Demostrar que la curva definida por

$$F(x, y, z) = y^2z - x^3 - xz^2 = 0$$

es una curva elíptica que pasa por el punto $\mathcal{O} = [0 : 1 : 0]$. Implementar la función `puntos(p)` que tome un primo $p \geq 3$ y devuelva la lista de puntos de $\mathcal{C}_F(\mathbb{Z}/p\mathbb{Z})$, cada uno de estos escritos como una tupla de tres componentes. Tener especial cuidado de no repetir el mismo punto dos veces en la lista (esto es no trivial, ya que un mismo punto puede tener varias representaciones $[x : y : z]$).

Problema 8.4. En la curva del problema 8.3, definimos la adición utilizando el neutro $\mathcal{O} = [0 : 1 : 0]$. Mostrar que la tangente a la curva en $\mathcal{O}$ corta a la curva solamente en el punto $\mathcal{O}$ con multiplicidad de intersección 3 y por lo tanto $\mathcal{O} * \mathcal{O} = \mathcal{O}$. Mostrar que el inverso de un punto $P = [x : y : 1]$ de la curva es $-P = [x : -y : 1]$. Implementar en Python3 las funciones `inverso(P,p)` y `suma(P,Q,p)` que calculen el inverso y la suma de puntos $P, Q \in \mathcal{C}_F(\mathbb{Z}/p\mathbb{Z})$. ¿Cuál es la estructura de los grupos para $p = 3, 5, 7, 11, 13$? ¿Cuántos puntos de orden 2 y 3 hay en cada uno de esos casos?

Problema 8.5. Un punto P de una curva elíptica se dice de inflexión si $P * P = P$, es decir, la tangente que pasa por P corta a la curva solamente en P con multiplicidad 3. Demostrar que en la curva del problema 8.3, un punto P es de inflexión si y solo si $3P = \mathcal{O}$. Mostrar que en una curva elíptica cualquiera, la condición de ser punto de inflexión es $3P = \mathcal{O} * \mathcal{O}$.

Problema 8.6. Mostrar que una curva algebraica plana proyectiva $\mathcal{C}_F$ dada por un polinomio irreducible $F \in \overline{K}[x, y, z]$ de grado 3 no puede tener dos puntos singulares.
Hint: Analizar las multiplicidades de intersección de la recta que pasaría por dos puntos singulares con la curva.

Problema 8.7. La curva de *Fermat* está definida por la ecuación $x^3 + y^3 - z^3 = 0$. Demostrar que es una curva elíptica si $\text{char}(K) \neq 3$. Consideremos el punto $\mathcal{O} = [1 : 0 : 1]$ de la curva y la adición definida con ese neutro. ¿Cuál es el inverso de un punto $[x : y : z]$ de la curva? Implementar las funciones `puntos(p)`, `inverso(P,p)` y `suma(P,Q,p)` para $\mathcal{C}_F(\mathbb{Z}/p\mathbb{Z})$ como en los problemas 8.3 y 8.4.

Problema 8.8. Sea K un cuerpo tal que $\text{char}(K) \neq 2, 3$. Una curva en forma de Weierstrass corresponde con la ecuación

$$F(x, y, z) = y^2z - x^3 - axz^2 - bz^3 = 0$$

para ciertos $a, b \in K$. Demostrar que $\mathcal{C}_F$ es elíptica si y solo si el polinomio $x^3 + ax + b$ no tiene raíces múltiples en $\overline{K}$, o equivalentemente, que $4a^3 + 27b^2 \neq 0$. Mostrar que en estas curvas, el punto $\mathcal{O} = [0 : 1 : 0]$ es de inflexión. Tomando a $\mathcal{O}$ como neutro de la adición, obtener fórmulas para el inverso y la suma. Notar que el problema 8.3 es un caso particular de este. Implementar las funciones `puntos(a,b,p)`, `inverso(P,a,b,p)`, `suma(P,Q,a,b,p)` y `mult(k,P,a,b,p)` para trabajar con estas curvas elípticas. La función `mult(k,P,a,b,p)` debe calcular kP con el método de la exponenciación binaria para cualquier $k \in \mathbb{Z}$.