Nociones generales acerca de curvas elípticas

Rocío Belén Sepúlveda Manzo,
con apuntes y un apéndice de José Cuevas Barrientos

Resumen. En ésta charla se repasan las nociones generales sobre curvas elípticas, con un lenguaje geométrico más robusto, y tiene como propósito formular la conjetura de Szpiro.

1. Generalidades sobre curvas elípticas

Definición 1.1: Sea K un cuerpo. Una ***curva elíptica*** E es una curva irreducible, proyectiva y suave sobre un cuerpo K, que es K-isomorfa a un cerrado de $\mathbb{P}^2_K$ dado por una ***ecuación de Weierstrass larga***

$$v^2w+a_1uvw+a_3vw^2 = u^3+a_2u^2w+a_4uw^2+a_6w^3, \qquad a_1,\dots,a_6 \in K. \tag{1}$$

La curva determinada por la ecuación anterior siempre contiene un punto (K-)racional distinguido $o = [0:1:0]$ tradicionalmente llamado «punto al infinito».

Observación 1.1.1: Sea $\lambda \in K^\times$ un escalar, podemos hacer la substitución $(u', v') = (\lambda^2 u, \lambda^3 v)$ y luego simplificar por λ^{-6}, con lo que obtendremos el cambio en el coeficiente a_i' por $\lambda^{-i}a_i$. Esto explica la elección sobre los índices i, a los cuales llamamos ***pesos***.

Si tomamos el cerrado dado por (1) e intersectamos con la carta afín $w = 1$, mediante las identificaciones $(x, y) = (u/w, v/w)$ obtendremos una ecuación un tanto más típica en la literatura y diremos que E está *inducida* por susodicha ecuación.

Ejemplo 1.2: Considere la cúbica (proyectiva) de Fermat $C\colon u^3 + v^3 = w^3$ sobre $\mathbb{Q}$. Es fácil verificar que efectivamente determina una subvariedad suave (e.g., por el criterio del jacobiano[1]), pero a simple vista no parece dada por ecuación de Weierstrass.

En primer lugar, aplicamos el cambio de variables $(u, v, w) \mapsto (u, v+w, w)$ y obtenemos que

$$u^3 + (v + w)^3 = w^3 \iff 3vw^2 + 3v^2w = -u^3 - v^3.$$

Pasando a la carta afín $v = 1$ con $(x, y) := (u/v, w/v)$, se obtiene la ecuación

$$3y^2 + 3y = -x^3 - 1. \tag{2}$$

Fecha: 26 de abril de 2024.

[1]Cfr. Liu [**3,** págs. 130, 147], Thm. 4.2.19 y Exr. 4.3.20.

Podemos multiplicar por 3^3 y ocupar $(x, y) \mapsto (-3x, -9y)$ para obtener la ecuación:

$$y^2 - 9y = x^3 - 27 \iff \left(y - \frac{9}{2}\right)^2 = x^3 - 27 + \frac{9^2}{2^2}.$$

La cual sí es una ecuación de Weierstrass con el cambio de variables $y \mapsto y - 9/2$. Por estética, puede multiplicar todo por 2^6 y obtener la ecuación $y^2 = x^3 - 2^4 \cdot 3^3$. ⌟

Realizaremos las dos siguientes reducciones a la ecuación de Weierstrass:

- Si $\operatorname{car} K \neq 2$, entonces empleando el cambio $(x, \frac{y}{2}) := (u, v + \frac{1}{2}(a_1 x + a_2))$ en la ecuación (1), uno obtiene la ***ecuación de Weierstrass simplificada***:

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6, \tag{3}$$

  donde los b_i's vienen dados por

$$\begin{gathered} b_2 := a_1^2 + 4a_2, \qquad b_4 := 2a_4 + a_1 a_3, \qquad b_6 := a_3^2 + 4a_6, \\ b_8 := a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2. \end{gathered} \tag{4}$$

- Si $\operatorname{car} K \neq 3$. Dada una curva proyectiva que, en la carta afín $z = 1$ toma forma de la ecuación (3), entonces el cambio de variables $(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$ nos da la ***ecuación de Weierstrass corta***:

$$y^2 = x^3 - 27c_4 x - 54c_6, \tag{5}$$

  donde

$$c_4 := b_2^2 - 24b_4, \qquad c_6 := -b_2^3 + 36b_2 b_4 - 216b_6. \tag{6}$$

Así, si $\operatorname{car} K \nmid 6$ nos podemos restringir a estudiar las curvas elípticas dadas por ecuaciones de Weierstrass cortas, las cuales agilizan cálculos.

Proposición 1.3 (Poincaré): Existe una única operación de grupo $+$ sobre $E(K)$ de modo que su neutro sea el punto al infinito o. Con ella $(E(K), +)$ es un grupo abeliano.

Podemos explicitar esta operación de grupo: en terminología de geometría algebraica, dados $P, Q \in E(K)$ la operación satisface que los siguientes divisores

$$[P] + [Q] + [-(P + Q)] \sim 3[o]$$

sea linealmente equivalentes. En «palabras más aterrizadas» esto se traduce en los siguientes diagramas conocidos como *operación cuerda-tangente*.

Una aplicación del criterio del jacobiano da lo siguiente:

Proposición 1.4: Sea K un cuerpo.

1. La curva proyectiva dada en la carta afín $z = 1$ por la ecuación de Weierstrass larga:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

es suave syss

$$\Delta := -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \neq 0,$$

donde los b_i's estan descritos por (4).

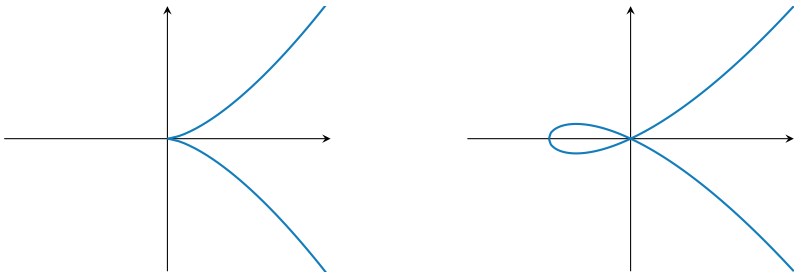
2. Si car $K \nmid 6$, entonces la curva proyectiva dada en la carta afín $z = 1$ por la ecuación

$$y^2 = x^3 + c_4 x + c_6$$

es suave syss

$$\Delta := -16(4c_4^3 + 27c_6^2) \neq 0.$$

En ambos casos, el Δ definido se llama el ***discriminante*** de la ecuación.



(a) $y^2 = x^3$, $\Delta = 0$. (b) $y^2 = x^3 + x^2$, $\Delta = 0$.

Figura 1. Ecuaciones de Weierstrass singulares.

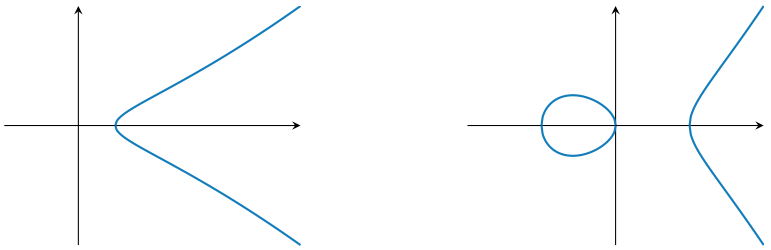
PISTA: El caso que nos interesa es el segundo, donde notamos que el Δ es -16 multiplicado por el discriminante del polinomio $x^3 + c_4 x + c_6$. Finalmente, el discriminante de un polinomio es no nulo syss dicho polinomio es separable, vale decir, si no tiene raíces repetidas sobre su cuerpo de escisión, la cual es fácil de verificar que corresponde a la condición para que la curva no tenga puntos singulares.

El caso 1 también se demuestra con un cálculo detallado en SILVERMAN **[7]**. □

Hacemos énfasis en que el discriminante es de la ecuación, no de la curva, ya que una misma curva elíptica admite distintas ecuaciones de Weierstrass con distintos discriminantes.

Corolario 1.4.1: Sea E una curva elíptica sobre $\mathbb{R}$ dada por una ecuación de Weierstrass (1). El conjunto de puntos $\mathbb{R}$-racionales $E(\mathbb{R})$ es conexo (con la topología subespacio sobre $\mathbb{P}^2(\mathbb{R})$) syss el discriminante Δ de (1) es negativo. De lo contrario, $E(\mathbb{R})$ tiene dos componentes conexas.

La situación se encuentra ilustrada en la fig. 2.



(a) $y^2 = x^3 - 1$, $\Delta = -2^4 \cdot 3^3$ (144.a3). (b) $y^2 = x^3 - 4x$, $\Delta = 2^{12}$ (64.a3).

Figura 2. Curvas elípticas.

2. Discriminante minimal y conductor

Definición 2.1: Sea E una curva elíptica sobre un cuerpo numérico K y sea $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ un primo. Una ecuación de Weierstrass (1) con discriminante Δ para E se dice ***minimal en*** $\mathfrak{p}$ (o, con respecto a $\mathfrak{p}$) si cada $a_1, \ldots, a_n \in \mathcal{O}_{K,\mathfrak{p}}$ (es decir, $\mathfrak{p}$ no divide a sus denominadores) y $\nu_{\mathfrak{p}}(\Delta) \geq 0$ es minimal sujeto a la condición anterior.

Observación 2.1.1: El discriminante Δ de una ecuación de Weierstrass (1) es una forma homogénea (con los pesos de la observación 1.1.1) de grado 12, esto significa que bajo el cambio de variables $(x', y') = (\lambda^2 x, \lambda^3 y)$ tras simplificar λ^{-6} obtendremos que $\Delta' = \lambda^{-12}\Delta$. En consecuencia, si $\nu_{\mathfrak{p}}(\Delta) < 12$, entonces (1) es minimal en $\mathfrak{p}$.

El recíproco no es cierto. Por ejemplo, uno puede probar que la ecuación de Weierstrass de la fig. 2b es minimal en 2 (esto debido a que $\nu_2(c_4) = 2 < 4$).

Definición 2.2: Sea E una curva elíptica sobre un cuerpo numérico K y sea (1) una ecuación de Weierstrass para E. Se dice que (1) es una ***ecuación minimal*** si lo es para todos los primos $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$.

No todas las curvas elípticas tienen ecuaciones minimales, de hecho:

Teorema 2.3 (Silverman): Sea K un cuerpo numérico. Todas las curvas elípticas sobre K poseen ecuaciones minimales syss su anillo de enteros $\mathcal{O}_K$ es un DIP. En particular, todas las curvas elípticas sobre $\mathbb{Q}$ poseen ecuaciones minimales.

Demostración: La implicancia «$\Longleftarrow$», que es la que empleamos, se deduce sin mucho esfuerzo de Silverman **[7,** pág. 245], Cor. VIII.8.3. El recíproco «$\Longrightarrow$» fue probado por Silverman **[5].** □

En $\mathbb{Q}$ hay, además, un criterio bastante sencillo de cuando una ecuación es minimal:

Proposición 2.4: Sea E una curva elíptica sobre $\mathbb{Q}$ dada por una ecuación de Weierstrass (1) de discriminante Δ. Entonces (1) es una ecuación minimal syss $|\Delta|$ es minimal, sujeto a la condición de que todos los $a_1, \ldots, a_6 \in \mathbb{Z}$. En consecuencia, al discriminante $d_{E/K} := \Delta$ se le llama ***discriminante minimal***.

Demostración: Si tenemos otra ecuación de Weierstrass con discriminante Δ' y coeficientes enteros, entonces, por definición de minimal en un primo p, se sabe que $\alpha_p := \nu_p(\Delta) \leq \nu_p(\Delta') =: \beta_p$. Luego

$$|\Delta| = \prod_p p^{\alpha_p} \mid \prod_p p^{\beta_p} = |\Delta'|,$$

por lo que $|\Delta| \leq |\Delta'|$ como se quería probar.

Para la parte de «en consecuencia» aún queda por verificar que Δ no varía por unidades. En $\mathbb{Z}$ la única unidad no trivial es -1 y vimos que el signo viene determinado por las componentes conexas de $E(\mathbb{R})$, las cuales no varían bajo $\mathbb{Q}$-isomorfismos de variedades algebraicas. □

La misma demostración prueba que, si E es una curva elíptica sobre K que posea ecuación minimal, entonces ésta es tal que su discriminante Δ minimiza $|\mathrm{Nm}_{K/\mathbb{Q}}(\Delta)|$.

En general uno puede definir el discriminante minimal como un ideal dado por el producto formal de las valuaciones $\mathfrak{p}$-ádicas de los discriminantes minimales relativos a $\mathfrak{p}$, aunque la definición es un poco «menos limpia». Esto determina no un entero algebraico, sino un ideal denotado $\mathfrak{d}_{E/K}$.

Definición 2.5: Sea E una curva elíptica con ecuación de Weierstrass minimal fija. Dado un primo $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$, denotaremos por $E_\mathfrak{p}$ a la curva proyectiva sobre $\Bbbk(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$ inducida por la reducción módulo $\mathfrak{p}$ de la ecuación minimal. Decimos que E tiene:

Buena reducción en $\mathfrak{p}$: si $E_\mathfrak{p}$ es suave.

Reducción multiplicativa en $\mathfrak{p}$: si $E_\mathfrak{p}$ es singular y sus singularidades son nodos (ver fig. 1b).

Reducción aditiva en $\mathfrak{p}$: si $E_\mathfrak{p}$ es singular y posee cúspides (ver fig. 1a).

Para una explicación de la terminología véase la observación A.4.1 más adelante.

El siguiente criterio es práctico para verificar cuando sucede determinado tipo de reducción:

Proposición 2.6: Sea E una curva elíptica sobre un cuerpo numérico K con una ecuación de Weierstrass minimal (1). Sea $\mathfrak{p}$ un primo de K tal que $\mathfrak{p} \nmid 6$, entonces:

(a) E tiene buena reducción en $\mathfrak{p}$ syss $\nu_p(\Delta) = 0$.
(b) E tiene reducción multiplicativa en $\mathfrak{p}$ syss $\nu_p(\Delta) > 0$ y $\nu_p(c_4) = 0$.

(c) E tiene reducción aditiva en $\mathfrak{p}$ syss $\nu_p(\Delta) > 0$ y $\nu_p(c_4) > 0$.

Aquí c_4 viene dado por la fórmula (6), donde los b_i's vienen de (4).

Esto es parte del algoritmo de Tate que, en su forma real, entrega muchísima más información.

Corolario 2.6.1: Sea E una curva elíptica sobre un cuerpo numérico K. Existen solo finitos primos $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ tales que E tiene mala reducción en $\mathfrak{p}$.

Definición 2.7: Sea E una curva elíptica sobre un cuerpo numérico K. Dado un primo $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ con $\mathfrak{p} \nmid 6$, se define

$$f_{\mathfrak{p}}(E) := \begin{cases} 0, & E \text{ tiene buena reducción en } \mathfrak{p}, \\ 1, & E \text{ tiene reducción multiplicativa en } \mathfrak{p}, \\ 2, & E \text{ tiene reducción aditiva en } \mathfrak{p}. \end{cases}$$

Se define el ***conductor*** de E como

$$\mathfrak{N}_{E/K} := \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}(E)}.$$

En general, el conductor es un ideal, pero si $K = \mathbb{Q}$, por ejemplo, determina un número entero.

Proposición 2.8: Para toda curva elíptica E sobre un cuerpo numérico K se cumple que $\mathfrak{N}_{E/K} \mid \mathfrak{d}_{E/K}$.

Demostración: Este es un resultado bastante no trivial y se deduce como corolario de la fórmula de Ogg (cfr. Silverman **[6,** pág. 389**]**, §IV.11). □

Con esto somos finalmente capaces de escribir lo siguiente:

Conjetura Szpiro, 1983 2.9: Para todo $\epsilon > 0$, existe una constante $\kappa_\epsilon > 0$ con la siguiente propiedad: para toda curva elíptica E sobre $\mathbb{Q}$ se satisface la siguiente desigualdad

$$|d_{E/\mathbb{Q}}| \leq \kappa_\epsilon \cdot N_{E/\mathbb{Q}}^{6+\epsilon}.$$

Observación 2.9.1: Salvo por los primos $p \mid 6$, el conductor es a lo más $\mathrm{Rad}(d_{E/\mathbb{Q}})^2$, así que el enunciado de la conjetura de Szpiro dice que $|d_{E/\mathbb{Q}}| \ll_\epsilon \mathrm{Rad}(d_{E/\mathbb{Q}})^{12+\epsilon}$. Esto tiene un «saborcito a la conjetura *abc*», el cual se precisará en las siguientes sesiones.

Esta relación se evidencia por lo siguiente:

Proposición 2.10: La conjetura de Szpiro implica el Último Teorema de Fermat asintótico (i.e., para exponentes suficientemente grandes).

DEMOSTRACIÓN: Cfr. SILVERMAN [**7,** pág. 256], Prop. VIII.11.2. □

APÉNDICE A. MÁS RESULTADOS GEOMÉTRICOS

Definición A.1: Una ***variedad abeliana*** es un grupo algebraico conexo, geométricamente reducido y propio sobre un cuerpo.

Otra definición equivalente es la de un grupo algebraico que es también una variedad proyectiva suave (cfr. GÖRTZ y WEDHORN [**2,** págs. 636, 669], Prop. 27.92 y Prop. 27.174). Más generalmente, uno puede definir la noción de un *esquema abeliano*, el cual es intuitivamente una familia de variedades abelianas y trabajar con ellas.

La siguiente proposición se sigue de un resultado apropiadamente llamado *lema de rigidez*:

Proposición A.2: Sean A, B un par de variedades abelianas sobre un cuerpo K y sea $f\colon A \to B$ un morfismo entre variedades algebraicas sobre K. Si $f(0_A) = 0_B$, entonces f es un homomorfismo.

En consecuencia, fijando un punto racional $o \in A(K)$, existe una única estructura de grupo algebraico sobre A que tiene al punto o como neutro.

DEMOSTRACIÓN: Cfr. [**2,** pág. 639], Prop. 27.101. □

Ahora podemos enunciar varias descripciones geométricas de la definición de curva elíptica:

Teorema A.3: Sea K un cuerpo y sea E un esquema algebraico sobre K. Son equivalentes:

1. E es una curva elíptica.
2. E es una curva geométricamente irreducible, proyectiva y suave, con al menos un punto racional $E(K) \neq \varnothing$ y de género $g(E) = 1$.
3. E es una variedad abeliana de dimensión 1 sobre K.

DEMOSTRACIÓN: La equivalencia 2 $\iff$ 3 está probada en [**2,** pág. 656], Thm. 27.147; mientras que 1 $\iff$ 2 es [**2,** pág. 657], Prop. 27.150. □

Proposición A.4: Sea G un grupo algebraico conmutativo, irreducible y suave de dimensión n sobre un cuerpo perfecto k (e.g., un cuerpo finito). Entonces posee los siguientes subgrupos normales:

- Una subvariedad abeliana A de dimensión a.
- Un subtoro T (i.e., un grupo algebraico tal que $T_{k^{\text{sep}}} \cong \mathbb{G}_{m,k^{\text{sep}}}^{t}$) de dimensión t.

- Un subgrupo unipotente U de dimensión u.

Tales que $G = A \cdot T \cdot U$. Además, todos ellos son conmutativos, conexos y suaves, la descomposición es única y se satisface la siguiente identidad:

$$a + t + u = n. \tag{7}$$

Demostración: Esto es una combinación del teorema de Barsotti-Chevalley (cfr. Milne [**4,** pág. 154], Thm. 8.27) junto a un teorema de estructura de grupos algebraicos conmutativos (cfr. [**4,** pág. 328], Thm. 16.13). □

Esto sumado a que los grupos unipotentes son, tras un cambio de base, potencias del grupo aditivo $\mathbb{G}_a$ (cfr. [**4,** pág. 297], Cor. 14.53); y que los toros son, tras un cambio de base, por definición, potencias del grupo multiplicativo $\mathbb{G}_m$ nos da:

Observación A.4.1: Sea E una curva elíptica sobre $\mathbb{Q}$. Resultados avanzados de geometría algebraica dicen que el subesquema abierto $N_p := (E_p)_{\mathrm{sm}}$ es la fibra especial del modelo de Néron (respecto a $\mathbb{Z}_p$, cfr. Bosch *et al.* [**1,** pág. 23]) de $E/\mathbb{Q}$. Por tanto, es un grupo algebraico conmutativo suave e irreducible. Así, la proposición anterior nos da una descomposición para N_p, y como tiene dimensión 1, han de cumplirse uno de los siguientes tres casos:

(a) $a = 1$ y N_p es una variedad abeliana (*buena reducción*).
(b) $t = 1$ y N_p es un toro (*reducción multiplicativa*).
(c) $u = 1$ y el cambio de base $N_p \times_{\mathbb{F}_p} \mathrm{Spec}(\mathbb{F}_p^{\mathrm{alg}}) \cong \mathbb{G}_{a,\mathbb{F}_p^{\mathrm{alg}}}$ (*reducción aditiva*).

Además, el caso (b) ahora admite una descomposición entre los siguientes subcasos:

(b.1) **Reducción multiplicativa escindida:** $N_p \cong \mathbb{G}_{m,\mathbb{F}_p}$, es decir, es un toro escindido.
(b.2) **Reducción multiplicativa no-escindida:** N_p es un $\mathbb{G}_{m,\mathbb{F}_p}$-torsor no trivial.

También, a raíz de la observación anterior, deberíamos indicar que la clasificación *correcta* de «buena/mala reducción» de una variedad abeliana de dimensión n consiste en la clasificación anterior, con énfasis en la fórmula de dimensiones (7).

Referencias

1. Bosch, S., Lütkebohmert, W. y Raynaud, M. *Néron models Grundlehren der mathematischen Wissenschaften* **21** (Springer-Verlag, 1990).
2. Görtz, U. y Wedhorn, T. *Cohomology of Schemes. With Examples and Exercises* (Springer Spektrum Wiesbaden, 2023).
3. Liu, Q. *Algebraic Geometry and Arithmetic Curves* (Oxford University Press, 2002).

4. Milne, J. S. *Algebraic Groups. The Theory of Group Schemes of Finite Type over a Field* (Cambridge University Press, 2017).
5. Silverman, J. H. Weierstrass equations and the minimal discriminant of an elliptic curve. *Mathematika* **31,** 245-251. doi:10.1112/S0025579300012468 (1984).
6. Silverman, J. H. *Advanced Topics in the Arithmetic of Elliptic Curves Graduate Texts in Mathematics* **151** (Springer-Verlag, 1994).
7. Silverman, J. H. *The arithmetic of elliptic curves* 2.ª ed. (Springer-Verlag, 2009).

Correo electrónico: rseplveda@uc.cl

Departamento de Matemáticas, Pontificia Universidad Católica de Chile. Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile
Correo electrónico: josecuevasbtos@uc.cl