Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid

Puntos racionales de orden finito en curvas elípticas

Trabajo de fin de grado

Grado en Matemáticas

Autor: Miguel García Moya
Tutor: Enrique González Jiménez

Curso 2020-2021

Resumen

Las curvas elípticas, curvas de género 1 con un punto base, tienen la propiedad de que sus puntos racionales forman un grupo abeliano. Demostrar la estructura de grupo es sencillo excepto por la propiedad asociativa, que demostramos utilizando el Teorema de Riemann-Roch para establecer un homomorfismo de grupos con el grupo de Picard de la curva. Hacemos un inciso para estudiar curvas elípticas sobre los complejos, trabajando sobre retículos y la función $\wp$ de Weierstrass, para finalmente demostrar la relación entre curvas elípticas y toros sobre este cuerpo. Posteriormente nos centramos en los puntos racionales de orden finito de la curva elíptica, demostrando que el subgrupo de torsión es finito mediante el Teorema de Nagell-Lutz, un resultado que prueba que los puntos racionales de torsión tienen coordenadas enteras con ciertas propiedades de divisibilidad. Otras técnicas que estudiamos incluyen el uso de reducción módulo p para estudiar la estructura del grupo de torsión, y las propiedades de los polinomios de división, usando los resultados obtenidos en nuestro trabajo sobre los complejos para obtener una fórmula para la multiplicación de puntos y usarla para deducir la estructura del grupo de torsión. Se incluye en un apéndice unas nociones básicas de Geometría Algebraica que son necesarias para entender los resultados que se obtienen en el cuerpo del trabajo.

Abstract

Elliptic curves, defined as curves of genus 1 with a base point, have the property of their rational points forming an abelian group. Proving the group structure is simple, except for the associative property, which we prove by using the Riemann-Roch Theorem to set up an homomorphism with the Picard group of the curve. Next we briefly study elliptic curves over the complex numbers, working on lattices and the Weierstrass $\wp$-function to in the end prove the relation between elliptic curves and tori on that field. Next, we focus on rational points of finite order on the elliptic curve, proving that the torsion subgroup is finite by using the the Nagell-Lutz Theorem, a result that proves how rational torsion points have integer coordinates with fixed divisibility properties. Other techniques we study include reduction module p to study the group structure of the torsion subgroup, and the properties of the division polynomials, using the results obtained during our work over the complex numbers to find a formula for point multiplication and use it to find the group structure of the torsion subgroup. An appendix is included containing basic notions of algebraic geometry that are required to understand the results obtained in the main matter.

Índice general

Introducción

Las curvas elípticas son un tipo de curvas muy especiales. El estudio de sus propiedades revela una cantidad de resultados importantes de geometría y álgebra. En este documento, nos centraremos en una de las propiedades algebraicas de las curvas elípticas: la estructura de grupo que sus puntos poseen. En efecto, es posible definir de forma elemental una operación que otorga a los puntos de una curva elíptica estructura de grupo abeliano.

Esta operación de grupo se define intuitivamente de forma geométrica, mediante la denominada ley de las secantes y tangentes. Las propiedades algebraicas y geométricas de la operación así definida hacen que el estudio de estos puntos tenga numerosas aplicaciones en teoría de números y criptografía, entre otros. Una de las propiedades de especial interés es que el subconjunto de puntos racionales de una curva elíptica definida sobre $\mathbb{Q}$ es un subgrupo, que de hecho es finitamente generado.

Demostrar las propiedades que dan la estructura de grupo al conjunto de puntos es en su mayoría sencillo. No obstante, la propiedad asociativa es más difícil de probar. Existen diversos métodos para llegar a este resultado. En este documento se utilizará el Teorema de Riemann-Roch, un importante resultado de curvas algebraicas, para encontrar un isomorfismo de grupos entre el conjunto de puntos y el grupo de clases de divisores de grado 0 de la curva.

Debido al limitado espacio disponible, el cuerpo principal de este documento asume que el lector posee conocimientos básicos de Geometría Algebraica. No obstante, véase Apéndice A para una introducción a los conceptos y resultados que se han estudiado para el trabajo realizado en el cuerpo principal del documento.

Otra propiedad importante que demostramos es que toda curva elíptica puede representarse con una ecuación de la forma $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Adicionalmente, en el caso de curvas elípticas sobre $\mathbb{Q}$, esta ecuación se puede transformar para obtener otras formas más sencillas de manejar, como la forma $y^2 = x^3 + Ax + B$. Una curva elíptica con su ecuación en cualquiera de estas formas se dice que está en forma de Weierstrass. Gracias a esta propiedad, podremos estudiar curvas elípticas a partir de sus ecuaciones de Weierstrass sin pérdida de generalidad.

Una vez demostrado que los puntos de una curva elíptica forman un grupo, nuestro siguiente objeto de interés son los puntos de orden finito, o de torsión. Es decir, aquellos que vuelven a la identidad tras aplicarles la operación de grupo a sí mismos

una cantidad finita de veces. En particular, nos centraremos en encontrar los puntos racionales con esta propiedad.

En primer lugar, demostraremos el Teorema de Nagell-Lutz, que nos da una condición sobre las coordenadas de los puntos racionales de orden finito. Gracias a este resultado, podremos probar que el subgrupo de torsión del grupo de puntos racionales es finito.

Posteriormente, veremos cómo utilizar reducción módulo p, dado un primo, para obtener información sobre la estructura del grupo de torsión. En particular, veremos que la reducción módulo p restringida a los puntos de orden finito es una aplicación inyectiva.

Adicionalmente, trataremos algunas propiedades de las curvas elípticas sobre los números complejos. Principalmente, demostraremos que toda curva elíptica sobre $\mathbb{C}$ es equivalente a un toro. El objetivo de este inciso de análisis complejo será obtener una fórmula para las coordenadas de un punto sumado a sí mismo, y a partir de ella, la estructura del subgrupo de puntos de un orden dado. Para ello, utilizaremos los llamados polinomios de división, una serie de polinomios definidos para un n arbitrario mediante relaciones de recursión que describen el comportamiento del endomorfismo "multiplicación por n". En particular, definiremos una función que relaciona el comportamiento de los polinomios de división con el de la función $\wp$ de Weierstrass en el toro, que a su vez nos describirá tal endomorfismo.

Aunque principalmente trabajaremos sobre $\mathbb{Q}$ y ocasionalmente sobre $\mathbb{C}$, una buena parte de los resultados obtenidos son válidos para cuerpos arbitrarios. Con el objetivo de describir el trabajo realizado con la mayor generalidad posible, establecemos esta notación:

- K es un cuerpo perfecto, y $\overline{K}$ un cierre algebraico fijo.
- $G_{\overline{K}/K}$ es el grupo de Galois de la extensión $\overline{K}/K$.
- $\mathbb{A}^n = \{(x_1, ..., x_n) : x_i \in \overline{K}\}$ es el conjunto de puntos del espacio n-afín. Los puntos de $\mathbb{A}^n$ con coordenadas en K se denominan puntos K-racionales y el conjunto de ellos se denota $\mathbb{A}^n(K)$. Notamos que $G_{\overline{K}/K}$ actúa sobre $\mathbb{A}^n$ de la forma: sean $\sigma \in G_{\overline{K}/K}, P \in \mathbb{A}^n$, entonces $P^\sigma = (x_1^\sigma, ..., x_n^\sigma)$. Así, tenemos que equivalentemente

$$\mathbb{A}^n(K) = \{P \in \mathbb{A}^n : P^\sigma = P \qquad \forall \sigma \in G_{\overline{K}/K}\}$$

- $\mathbb{P}^n = \{[x_0, ..., x_n] \in \mathbb{A}^{(n+1)} : x_i \neq 0 \text{ para algún } i\}/\sim$, donde la relación de equivalencia es $(x_0, ..., x_n) \sim (y_0, ..., y_n)$ si y solo si existe $\lambda \in \overline{K}^*$ tal que $x_i = \lambda y_i$ para todo i, es el conjunto de puntos del espacio n-proyectivo. Definimos $\mathbb{P}^n(K)$ de forma equivalente.
- El conjunto de polinomios en $\overline{K}$ con n variables en el caso afín, y con $n+1$ variables en el caso proyectivo, se escribe $\overline{K}[X]$. Nótese que el espacio proyectivo de dimensión n es el caso de $n+1$ variables, explicando así la distinción.

CAPÍTULO 1
Aritmética de curvas elípticas

Una curva elíptica es una variedad proyectiva suave de dimensión 1 y género 1, junto con un punto base. Veremos como toda curva elíptica está dada por una ecuación que diremos en forma de Weierstrass. Así, podremos restringirnos a trabajar en este tipo de ecuaciones sin pérdida de generalidad.

Los puntos de una curva elíptica forman un grupo abeliano con una operación que denominaremos '+'. Definiremos esta operación y demostraremos que convierte al conjunto de puntos de la curva en un grupo.

Para demostrar la propiedad asociativa, utilizaremos el Teorema de Riemann-Roch para establecer un isomorfismo de grupos entre el grupo así definido y la parte de grado 0 del subgrupo de clases de divisores de la curva definida sobre K. Para más información sobre este teorema, ver Apéndice A.

Finalmente, enunciaremos el Teorema de Mordell, de suma importancia en la teoría de curvas elípticas.

1.1. Ecuaciones de Weierstrass

Definición 1.1. Una **curva elíptica** es un par $(E, \mathcal{O})$ donde E es una curva suave de género 1 y $\mathcal{O} \in E$. Generalmente, una curva elíptica se denota E, con $\mathcal{O}$ implícito.

Una curva elíptica está definida sobre K, denotado E/K, si E definida sobre K (como curva) y $\mathcal{O} \in E(K)$.

Una ecuación de Weierstrass es de la forma

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.1}$$

con $a_1, a_2, a_3, a_4, a_6 \in K$. Deshomogenizando mediante $x = X/Z, y = Y/Z$, tenemos la forma afín

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.2}$$

Tomando $Z = 0$, vemos que la ecuación es $X^3 = 0$. Por tanto, tenemos un único punto en el infinito $\mathcal{O} = [0, 1, 0]$.

Para simplificar la ecuación, podemos hacer la sustitución $y \longmapsto \frac{1}{2}(y - a_1x - a_3)$ que complete el cuadrado. Así, obtenemos una ecuación de la forma (véase Apéndice B para los coeficientes):

$$y^2 = 4x^3 + b_2x^2 + b_4x + b_6. \tag{1.3}$$

Adicionalmente, podemos hacer una sustitución más $(x, y) \longmapsto (\frac{x-3b_2}{36}, \frac{y}{108})$ para eliminar el término x^2, obteniendo una ecuación

$$y^2 = x^3 + Ax + B \tag{1.4}$$

Definición 1.2. Sea E una curva con ecuación de Weierstrass en forma $y^2 = x^3 + Ax + B$. El discriminante de E, denotado Δ, es

$$\Delta = -16(4A^3 + 27B^2).$$

Nótese que no todas estas sustituciones son posibles para cuerpos de característica 2 ó 3. Estas restricciones sobre la característica de K no nos afectarán demasiado, ya que nuestra intención es trabajar sobre $\mathbb{Q}$. No obstante, cuerpos de característica 2 ó 3 aparecen de forma natural incluso trabajando sobre $\mathbb{Q}$, como por ejemplo por reducción módulo p = 2, por lo que es importante tener estas distinciones en cuenta.

Proposición 1.3. *Una curva dada por una ecuación de Weierstrass es singular si y solo si $\Delta = 0$. En ese caso, existe un único punto singular.*

Demostración. Sea $F(X, Y, Z) = Y^2Z - X^3 - AXZ^2 - BZ^3 = 0$ la forma homogénea de la ecuación de la curva. Recordamos que un punto es singular si todas las derivadas parciales en el punto se anulan, en nuestro caso, $\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = \frac{\partial F}{\partial Z} = 0$. En primer lugar, vemos que en $\mathcal{O} = [0, 1, 0]$, $\frac{\partial F}{\partial Z}(\mathcal{O}) = 1 \neq 0$. Por tanto $\mathcal{O}$ no es singular. Ahora suponemos que $P_0 = [x_0, y_0, 1]$ es un punto singular de E. Entonces tenemos que

$$\begin{aligned}
\frac{\partial F}{\partial X}(x_0, y_0, 1) &= -3x_0^2 - A = 0, \\
\frac{\partial F}{\partial Y}(x_0, y_0, 1) &= 2y_0 = 0, \\
\frac{\partial F}{\partial Z}(x_0, y_0, 1) &= y_0^2 - 2Ax_0 - 3B = 0.
\end{aligned}$$

Por la segunda ecuación, $y_0 = 0$. Si $A = 0$, entonces la primera ecuación nos dice que $x_0 = 0$ y la tercera ecuación nos dice que $B = 0$. Esto se cumple si y solo si $\Delta = 0$. Si $A \neq 0$, entonces la tercera ecuación nos dice que $x_0 = -3B/2A$ y sustituyendo en la primera ecuación tenemos que $\frac{-27B^2-4A^3}{4A^2} = 0$, lo que ocurre si y solo si $\Delta = 0$. □

Proposición 1.4. *Si una curva E dada por una ecuación de Weierstrass es singular, entonces E es birracionalmente equivalente a $\mathbb{P}^1$.*

Demostración. Ver [8, III.1.6]. □

Trabajar en curvas cúbicas singulares es similar a trabajar con cónicas (ver [9, Ch. 1] para más información). Por tanto, a partir de aquí nos centraremos en curvas suaves dadas por ecuaciones de Weierstrass.

Para terminar la sección, demostramos que toda curva elíptica es birracionalmente equivalente a una curva dada por una ecuación de Weierstrass.

Proposición 1.5. *Sea $(E, \mathcal{O})$ una curva elíptica definida sobre K. Entonces existen funciones $x, y \in K(E)$ tales que la aplicación racional*

$$\phi : E \longrightarrow \mathbb{P}^2, \ \phi = [x, y, 1],$$

da un isomorfismo de E/K en una curva dada por una ecuación de Weierstrass

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

con coeficientes $a_1, ..., a_6 \in K$ y que satisface $\phi(\mathcal{O}) = [0, 1, 0]$.

Demostración. Miramos los espacios $\mathcal{L}(n(\mathcal{O}))$ para $n = 1, 2, ...$ (ver Definición A.32). Por Corolario A.39c, tenemos

$$l(n(\mathcal{O})) = n \quad \forall n \geq 1.$$

Por tanto, utilizando Proposición A.41 podemos tomar funciones $x, y \in K(E)$ tales que $\{1, x\}$ es base de $\mathcal{L}(2(\mathcal{O}))$ y $\{1, x, y\}$ es base de $\mathcal{L}(3(\mathcal{O}))$. Nótese que x debe tener un polo de orden exacto 2 en $\mathcal{O}$ e y debe tener un polo de orden exacto 3 en $\mathcal{O}$.

Ahora observamos que $\mathcal{L}(6(\mathcal{O}))$ tiene dimensión 6 pero contiene las siete funciones $1, x, y, x^2, xy, y^2, x^3$. Por tanto hay una relación lineal

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0,$$

donde por Proposición A.41 podemos tomar $A_1, ..., A_7 \in K$. Si $A_6A_7 = 0$, entonces tendríamos que las funciones $1, x, y, xy, x^2$ no son linealmente independientes. Esto no es posible, ya que $\{1, x, y, xy, x^2\}$ son base de $\mathcal{L}(5(\mathcal{O}))$, por lo que $A_6A_7 \neq 0$. Así, podemos reemplazar x e y por $-A_6A_7x$ y $A_6A_7^2y$ respectivamente, y dividiendo por $A_6^3A_7^4$ obtenemos una ecuación en forma de Weierstrass. Esto nos da una aplicación

$$\phi : E \longrightarrow \mathbb{P}^2, \ \phi = [x, y, 1],$$

cuya imagen C es descrita por una ecuación de Weierstrass. Como no es constante, ϕ es un morfismo sobreyectivo. Además, como y tiene un polo de mayor orden que x en $\mathcal{O}$, tenemos que $\phi(\mathcal{O}) = [0, 1, 0]$.

El siguiente paso es probar que la aplicación $\phi : E \longrightarrow C \subset \mathbb{P}^2$ tiene grado 1, o equivalentemente $K(E) = K(x, y)$. Considera la aplicación $[x, 1] : E \longrightarrow \mathbb{P}^1$. Como x tiene un polo de orden 2 en $\mathcal{O}$ y ningún otro polo, Proposición A.23a aplicada en $Q = [1, 0]$ nos dice que esta aplicación tiene grado 2. Por tanto, $[K(E) : K(x)] = 2$. Similarmente, $[y, 1] : E \longrightarrow \mathbb{P}^1$ tiene grado 3. Por tanto, $[K(E) : K(y)] = 3$. Por tanto $[K(E) : K(x, y)]$ divide a 2 y 3, así que debe ser 1, es decir, $K(E) = K(x, y)$.

Ahora mostramos que C es suave. Suponemos que C es singular. Entonces existe una aplicación racional $\psi : C \longrightarrow \mathbb{P}^1$ de grado 1. Por tanto $\psi \circ \phi : E \longrightarrow \mathbb{P}^1$ es una aplicación de grado 1 entre curvas suaves, así que debe ser isomorfismo. Pero E tiene género 1 y $\mathbb{P}^1$ tiene género 0. Por tanto, C no es singular.

Juntando todo, vemos que $\phi : E \longrightarrow C$ es una aplicación de grado 1 entre curvas suaves. Por Corolario A.21, es isomorfismo.

□

Con este resultado, vemos que podemos prescindir de tratar curvas elípticas con ecuaciones arbitrarias y centrarnos en curvas dadas por ecuaciones de Weierstrass.

1.2. La ley de grupo

Sea $(E, \mathcal{O})$ una curva elíptica definida sobre un cuerpo K. Como la ecuación que la define tiene grado 3, el Teorema de Bezout (ver Apéndice A.2) nos dice que toda recta en el plano proyectivo interseca a E en tres puntos, contando multiplicidad. De esta forma, podemos definir una operación de la siguiente forma:

Definición 1.6. Sean $P, Q \in E, P \neq Q$, definimos como $P * Q$ al tercer punto de intersección con E de la recta entre P y Q. Definimos como $P * P$ al otro punto de intersección con E de la recta tangente a E en P.
Nótese que si E/K y $P, Q \in E(K)$, entonces se cumple que $P * Q, P * P \in E(K)$. Esto es así ya que la recta entre $P \in E(K)$ y $Q \in E(K)$ debe estar definida sobre K, así que la intersección de esa recta con la curva E definida sobre K siempre da un punto con coordenadas en K.

Esta operación de composición, por desgracia, no convierte al conjunto de puntos de E en un grupo. Por ejemplo, se puede ver que no existe un elemento neutro. No obstante, hay una forma fácil de obtener una operación que convierte el conjunto de puntos en un grupo y hace de un punto $\mathcal{O} \in E$ el elemento neutro.

Definición 1.7. Sean $P, Q, \mathcal{O} \in E(K)$. Definimos $P + Q$ como el tercer punto de intersección con E de la recta entre $\mathcal{O}$ y $P * Q$. Es decir, $P + Q = (P * Q) * \mathcal{O}$.

Proposición 1.8. *a)* $P + \mathcal{O} = P$.

b) $P + Q = Q + P$.

c) *Dado* $P \in E$, *existe un elemento* $-P$ *tal que* $P + (-P) = \mathcal{O}$.

d) $P + (Q + R) = (P + Q) + R$.

Demostración. a) Vemos que la recta que define $P * \mathcal{O}$ contiene a los puntos $P, \mathcal{O}, P * \mathcal{O}$. Por tanto, la recta entre $\mathcal{O}$ y $P * \mathcal{O}$ es la misma recta, y el tercer punto de intersección con E es $P + \mathcal{O} = P$.

b) Vemos que el orden de los puntos no cambia la definición de la recta. Por tanto $P * Q = Q * P$ y $P + Q = Q + P$.

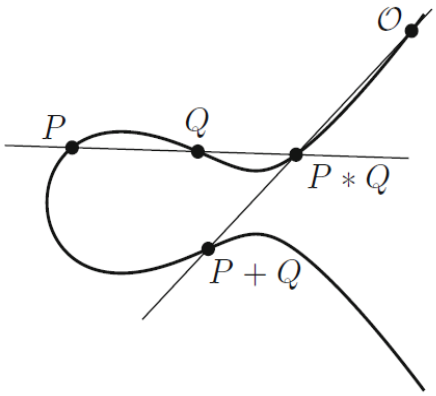

Figura 1.1: Ley de grupo en la curva

c) Tomando $S = \mathcal{O} * \mathcal{O}$ vemos que $(P * S) + P = \mathcal{O}$. Por tanto $P * S = -P$.

d) Esta prueba se hará en la sección 1.3.

□

Ahora, tomamos como punto base $\mathcal{O} = [0, 1, 0]$, el punto en el infinito. Este punto es de multiplicidad 3, ya que la recta tangente a E en $\mathcal{O}$ es la recta en el infinito $Z = 0$, que interseca en él 3 veces. Esto nos da una propiedad muy fácil de demostrar:

Proposición 1.9. *Sean $P, Q, R \in E$ puntos en la misma recta L. Entonces $(P+Q)+R = \mathcal{O}$.*

Demostración. Por definición, $P * Q = R$ y por tanto $(P + Q) * R = \mathcal{O}$. Ya que $\mathcal{O}$ tiene multiplicidad 3, tenemos que $\mathcal{O} * \mathcal{O} = \mathcal{O}$ y así $(P+Q)+R = ((P+Q)*R)*\mathcal{O} = \mathcal{O} * \mathcal{O} = \mathcal{O}$. □

Aunque nuestra construcción es perfectamente válida para curvas elípticas arbitrarias, hemos demostrado que no se pierde generalidad al trabajar en curvas dadas por ecuaciones de Weierstrass con punto base $\mathcal{O} = [0, 1, 0]$.

Véase Apéndice B para las fórmulas explícitas de la operación de grupo.

Queda por demostrar que la operación de grupo es asociativa, para lo que dedicaremos la siguiente sección.

1.3. Demostración de la propiedad asociativa

Demostrar la propiedad asociativa del grupo que hemos definido no es tan sencillo como demostrar el resto de propiedades. En este documento haremos una demostración utilizando el Teorema de Riemann-Roch para establecer un homomorfismo de grupos con el grupo de divisores de la curva.

Primero introducimos un lema que usaremos en la demostración.

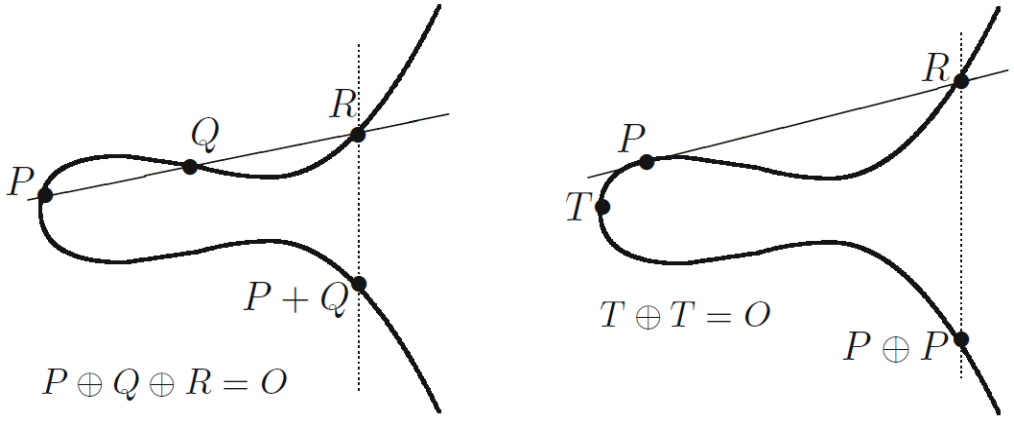

Figura 1.2: Ley de grupo en una curva elíptica con punto base $\mathcal{O} = [0, 1, 0]$

Lema 1.10. *Sea C una curva de género 1 y $P, Q \in C$. Entonces*

$$(P) \sim (Q) \Leftrightarrow P = Q$$

Demostración. Suponemos que $(P) \sim (Q)$. Escogemos $f \in \overline{K}(C)$ tal que

$$div(f) = (P) - (Q).$$

Entonces $f \in \mathcal{L}((Q))$. Por Corolario A.39c sabemos que $dim\ \mathcal{L}((Q)) = 1$. Pero $\mathcal{L}((Q))$ claramente contiene las funciones constantes. Por tanto $f \in \overline{K}$, así que $div(f) = 0$ y entonces $P = Q$. □

El siguiente resultado nos permitirá demostrar la propiedad asociativa.

Proposición 1.11. *Sea $(E, \mathcal{O})$ una curva elíptica.*

a) Para todo $D \in Div^0(E)$ existe un único $P \in E$ que satisface $D \sim (P) - (\mathcal{O})$. Llamamos

$$\sigma : Div^0(E) \longrightarrow E$$

a la aplicación que envía D a su P asociado.

b) σ es sobreyectiva.

c) Sean $D_1, D_2 \in Div^0(E)$. Entonces

$$\sigma(D_1) = \sigma(D_2) \text{ si y solo si } D_1 \sim D_2.$$

Por tanto σ induce una biyección (también denotada σ):

$$\sigma : Pic^0(E) \longrightarrow E.$$

d) El inverso a σ es la aplicación:

$$\kappa : E \longrightarrow Pic^0(E),\ P \longmapsto (\text{clase de divisor de } (P) - (\mathcal{O})).$$

e) *El grupo definido en E y el grupo en $Pic^0(E)$ son isomorfos.*

Demostración. a) E tiene género 1, así que Corolario A.39c nos dice

$$dim(\mathcal{L}(D + (\mathcal{O}))) = 1.$$

Sea $f \in \overline{K}(E)$ un elemento no cero de $\mathcal{L}(D + (\mathcal{O}))$, y $\{f\}$ es una base (ya que es espacio vectorial 1-dimensional). Como $f \in \mathcal{L}(D + (\mathcal{O}))$, tenemos que $div(f) \geq -D - (\mathcal{O})$. Dado que $deg(div(f)) = 0$ y $deg(D) = 0$, tenemos que existe $P \in E$ tal que

$$div(f) = -D - (\mathcal{O}) + (P).$$

Por tanto,

$$D \sim (P) - (\mathcal{O}),$$

lo que demuestra que existe un punto con tal propiedad.

Ahora supongamos que existe otro $P' \in E$ con tal propiedad. Entonces tenemos que

$$(P) \sim D + (\mathcal{O}) \sim (P')$$

y por Lema 1.10, $P = P'$. Por tanto P es único.

b) Dado $P \in E$, tenemos que

$$\sigma((P) - (\mathcal{O})) = P.$$

Por tanto σ es sobreyectiva.

c) Sean $D_1, D_2 \in Div^0(E)$ y sea $P_i = \sigma(D_i)$ para $i = 1, 2$. Entonces, por la definición de σ tenemos que

$$D_1 - D_2 \sim (P_1) - (P_2)$$

Por tanto si $P_1 = P_2$ tenemos que $D_1 \sim D_2$. Por otro lado, si $D_1 \sim D_2$ entonces $(P_1) \sim (P_2)$ y por Lema 1.10, $P_1 = P_2$.

d) Por *b*) sabemos que $\sigma((P) - (\mathcal{O})) = P$, así que $\kappa(P) =$ imagen en $Pic^0(E)$ de $(P) - (\mathcal{O})$. La imagen en $Pic^0(E)$ es la clase de divisor.

e) Sea E dado por una ecuación de Weierstrass y $P, Q \in E$. Ya hemos visto que κ es un isomorfismo, así que basta demostrar que es homomorfismo de grupos, es decir,

$$\kappa(P + Q) = \kappa(P) + \kappa(Q).$$

(Nótese que el primer $+$ es suma en el grupo de puntos mientras que el segundo $+$ es suma en $Pic^0(E)$).

Sea

$$f(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0$$

ecuación de la recta L en $\mathbb{P}^2$ que pasa por P y Q, y sea R el tercer punto de intersección. Sea

$$g(X, Y, Z) = \alpha' X + \beta' Y + \gamma' Z = 0$$

ecuación de la recta L' entre R y $\mathcal{O}$. Por la definición de suma en E y dado que la recta $Z = 0$ interseca en $\mathcal{O}$ con multiplicidad 3, tenemos que

$$div(f/Z) = (P) + (Q) + (R) - 3(\mathcal{O}).$$
$$div(g/Z) = (R) + (P + Q) - 2(\mathcal{O}).$$

Por tanto,

$$(P + Q) - (P) - (Q) + (\mathcal{O}) = div(g/f) \sim 0.$$

Así que

$$\kappa(P + Q) + \kappa(P) - \kappa(Q) = 0.$$

Lo que demuestra que κ es un homomorfismo de grupos.

□

Corolario 1.12. *Sea $(E, \mathcal{O})$ una curva elíptica, y $P, Q, R \in E$. Entonces $(P+Q)+R = P + (Q + R)$.*

Demostración. Como el grupo en $Pic^0(E)$ cumple la propiedad asociativa, también lo hace el conjunto de puntos de E. □

Teorema 1.13. *Sea $(E, \mathcal{O})$ curva elíptica definida sobre un cuerpo K. Entonces $(E(K), +)$ es un grupo abeliano.*

Demostración. La propiedad asociativa se cumple por el Corolario 1.12. Las demás propiedades fueron demostradas en la Proposición 1.8. Como $P + Q = (P * Q) * \mathcal{O}$, la observación en la Definición 1.6 nos muestra que $E(K)$ es un subgrupo de E. Por tanto, $E(K)$ es un grupo abeliano con la operación $+$. □

1.4. Teorema de Mordell-Weil

Antes de pasar a puntos de orden finito, enunciamos el Teorema de Mordell-Weil, un importante resultado de teoría de curvas elípticas que no podemos ignorar. El Teorema de Mordell-Weil nos dice que el grupo de puntos racionales de la curva es finitamente generado, es decir, podemos obtener todo punto racional de la curva mediante la suma que hemos definido partiendo de un conjunto finito de puntos iniciales.

Teorema de Mordell-Weil. *Sea $(E, \mathcal{O})$ una curva elíptica definida sobre un cuerpo K. Entonces $(E(K), +)$ es un grupo abeliano finitamente generado.*

La demostración de este resultado se sale del alcance de este documento. Cabe mencionar que no se conoce un método general para encontrar un conjunto generador para cualquier curva.

En particular, a partir del Teorema de Mordell, tenemos que el Teorema Fundamental de grupos abelianos finitamente generados dice que $E(K) \simeq E(K)_{tors} \oplus \mathbb{Z}^r$, donde $E(K)_{tors}$ es el subgrupo de puntos de orden finito y $r = rango(E(K)) \in \mathbb{Z}^+$. Esto nos prueba que $E(K)_{tors}$ es finito, pero daremos una demostración alternativa en el Capítulo 3.

CAPÍTULO 2
Curvas elípticas sobre $\mathbb{C}$

Antes de tratar los puntos racionales de orden finito, nos detendremos brevemente para observar algunas propiedades de curvas elípticas sobre los complejos. Notablemente, toda curva elíptica sobre $\mathbb{C}$ es isomorfa a un toro. Estas propiedades serán importantes para la sección 3.3. Nótese que las demostraciones más largas se han movido al Apéndice C para reducir la densidad de esta sección.

2.1. Retículos y la función $\wp$ de Weierstrass

Definición 2.1. Sean $\omega_1, \omega_2 \in \mathbb{C}$ linealmente independientes sobre $\mathbb{R}$. Un retículo es un conjunto

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\}.$$

$\mathbb{C}/L$ forma una superficie llamada toro, y veremos que es isomorfo al grupo de puntos complejos de una curva elíptica.

Definición 2.2. El conjunto

$$F = \{a_1\omega_1 + a_2\omega_2 \mid 0 \leq a_1, a_2 < 1\}$$

es un paralelogramo fundamental de L. Nota que F depende de la base ω_1, ω_2.

Definición 2.3. Una función meromorfa es una función en $\mathbb{C}$ holomorfa excepto en un conjunto de puntos aislados.

Proposición 2.4. *Toda función meromorfa es el cociente entre dos funciones holomorfas donde el denominador no es la función constante 0.*

Demostración. Ver [1, p. 196]. □

Definición 2.5. Una función doblemente periódica es una función meromorfa tal que $f(z + w) = f(z)$ para todo $z \in \mathbb{C}, w \in L$. Los $w \in L$ se llaman periodos de f.

Una función doblemente periódica se puede ver como una función en $\mathbb{C}/L$.

Recordamos que el divisor de una función es

$$div(f) = \sum_{w \in F} ord_w(f)(w).$$

Es fácil ver que si f es doblemente periódica, entonces $ord_{w+\omega}(f) = ord_w(f)$. Recordamos algunas propiedades;

Proposición 2.6. *Dada f una función doblemente periódica en un retículo L, F un parelelogramo fundamental de L. Entonces,*

a) Si f no tiene polos, es constante.

b) Si $f \neq 0, deg(div(f)) = 0$.

c) Si $f \neq 0, \sum_{w \in F} w \cdot ord_w(f) \in L$.

d) Si f no es constante, es sobreyectiva.

e) La ecuación $f(z) = z_0$ (con $z_0 \in \mathbb{C}$) tiene n soluciones, donde n es el número de polos de f (contando multiplicidad).

f) Si f tiene un único polo en F, no es un polo simple.

Demostración. *a*), *b*) y *d*) se demuestran en Apéndice A. *c*) se obtiene similarmente a *b*), con la diferencia de que la función obtenida no es doblemente periódica. *e*) se obtiene viendo que la función $f(z) - z_0$ es doblemente periódica con los mismos polos que $f(z)$, así que tiene n ceros. *f*) se demuestra en Proposición A.40. □

Ahora introducimos una función doblemente periódica muy importante: la función $\wp$ de Weierstrass:

Definición 2.7. Dado un retículo L, se define la función $\wp$ de Weierstrass como

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq \omega \in L} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Teorema 2.8. *Dado un retículo L, se tiene:*

a) La suma que define $\wp(z)$ converge absolutamente y uniformemente en conjuntos compactos sin elementos de L.

b) $\wp$ es meromorfa en $\mathbb{C}$ y tiene un polo doble en cada $\omega \in L$.

c) $\wp$ es par.

d) $\wp$ es doblemente periódica (en L).

e) Toda función doblemente periódica (en L) es una función racional de $\wp$ y de $\wp'$, la derivada de $\wp$.

Demostración. Ver Apéndice C. □

Ahora que hemos establecido estos conceptos, podemos empezar a ver la relación entre retículos y curvas elípticas.

2.2. Un toro es una curva elíptica

El objetivo de esta sección es probar que un toro $\mathbb{C}/L$ es isomorfo a los puntos complejos de una curva elíptica.

Definición 2.9. Dado un entero $k \geq 3$, la serie de Eisenstein es

$$G_k = \sum_{0 \neq \omega \in L} \omega^{-k}.$$

La suma converge para $k \geq 3$. Si k es impar, los términos para ω y $-\omega$ se cancelan, así que $G_k = 0$.

Proposición 2.10. *Para* $0 < |z| < \text{mín}_{0 \neq \omega \in L}(|\omega|)$,

$$\wp(z) = \frac{1}{z^2} + \sum_{j=1}^{\infty} (2j+1) G_{2j+2} z^{2j}.$$

Demostración. Cuando $|z| < |\omega|$ tenemos que

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \omega^{-2} \left(\frac{1}{(1-(z/\omega))^2} \right) = \omega^{-2} \left(\sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^n} \right).$$

Entonces

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \neq 0} \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^{n+2}}.$$

Sumando sobre ω obtenemos

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1)_{n+2} z^n.$$

Como $G_k = 0$ para k impar, podemos eliminar los términos con n par, de forma que tomamos solo los términos $n = 2j$. Así, obtenemos el resultado buscado. □

Teorema 2.11. *Sea* $\wp(z)$ *la función* $\wp$ *de Weierstrass para un retículo* L. *Entonces*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Demostración. Ver Apéndice C. □

Notación estándar: $\begin{cases} g_2 = 60G_4, \\ g_3 = 140G_6. \end{cases}$

Este teorema nos dice que los puntos $(\wp(z), \wp'(z))$ están en la curva

$$E : y^2 = 4x^3 - g_2 x - g_3.$$

El discriminante del polinomio de la derecha es $16(g_2^3 - 27g_3^2)$.

Proposición 2.12. $\Delta = g_2^3 - 27g_3^2 \neq 0$.

Demostración. $\wp'$ es doblemente periódica, así que $\wp'(\omega_i/2) = \wp'(-\omega_i/2)$. Como $\wp'(-z) = -\wp'(z)$ (se obtiene directamente de que $\wp$ es par), tenemos que $\wp'(\omega_i/2) = 0$ (para $i = 1, 2, 3$). Por tanto, cada $\wp(\omega_i/2)$ es una raíz del polinomio $4x^3 - g_2x - g_3$. Si estas raíces son distintas, entonces su discriminante debe ser distinto de 0.

Ahora sea $h_i(z) = \wp(z) - \wp(\omega_i/2)$. Entonces $h_i(\omega_i/2) = h_i'(\omega_i/2) = 0$, así que h_i tiene un cero de orden al menos 2 en $\omega_i/2$. Ya que solo tiene un polo en F, el doble polo en 0, $\omega_i/2$ es el único cero. Esto nos dice que $h_i(\omega_j/2) \neq 0$ si $j \neq i$, es decir, que las raíces $\wp(\omega_i/2)$ son distintas. □

Esta proposición nos dice que la curva E es una curva elíptica[1]. Los puntos $(\wp(z), \wp'(z))$ solo dependen de z mod L. Así, obtenemos una función de $\mathbb{C}/L$ a $E(\mathbb{C})$.

Teorema 2.13. *Sea L un retículo y $E : y^2 = 4x^3 - g_2x - g_3$ con $\Delta = g_2^3 - 27g_3^2 \neq 0$. Entonces la función*

$$\begin{aligned} \Phi : \mathbb{C}/L &\longrightarrow E(\mathbb{C}) \\ z &\longmapsto (\wp(z), \wp'(z)) \\ 0 &\longmapsto \infty \end{aligned}$$

es un isomorfismo de grupos.

Demostración. Ver Apéndice C. □

2.3. Toda curva elíptica es un toro

Hemos visto que existe un isomorfismo entre toros y sus curvas asociadas. Nuestro próximo objetivo es demostrar que toda curva elíptica está asociada a un retículo.

Dado un retículo $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, sea $\tau = \omega_1/\omega_2$. Como ω_1 y ω_2 son linealmente independientes sobre $\mathbb{R}$, $Im(\tau) \neq 0$, y podemos suponer que $Im(\tau) > 0$ intercambiando ω_1 con ω_2 si fuera necesario. Así, asumimos que $\tau \in \mathcal{H} = \{x + iy \in \mathbb{C} | y > 0\}$.

El retículo $L_\tau = \mathbb{Z}\tau + \mathbb{Z}$ es homotético a L, es decir, existe $\lambda \in \mathbb{C}^*$ tal que $L = \lambda L_\tau$.

Definición 2.14.

$$G_k(\tau) = G_k(L_\tau) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m\tau + n)^k}.$$

$$g_2(\tau) = g_2(L_\tau), \;\; g_3(\tau) = g_3(L_\tau).$$

Tenemos que $G_k(\tau) = \omega_2^k G_k(L)$, donde $G_k(L)$ es la serie de Eisenstein definida para L. A partir de ahora, sea $q = e^{2\pi i\tau}$.

[1] A partir de la información que tenemos, no es inmediato ver que la curva tiene género 1. Para verlo, transformamos la ecuación en la forma $y^2 = (x-e_1)(x-e_2)(x-e_3)$ y utilizamos la Proposición A.40.

Definición 2.15.

$$j(L) = 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2},$$
$$j(\tau) = j(L_\tau).$$

Las definiciones de G_4 y G_6 implican que $g_2(\lambda L) = \lambda^{-4}g_2(L)$ y $g_3(\lambda L) = \lambda^{-6}g_3(L)$. Por tanto vemos que $j(\lambda L) = j(L)$. Así, $j(\tau) = j(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$.

Tenemos que $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$ actúa sobre $\mathcal{H}$ mediante

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

Proposición 2.16. *Sea* $\tau \in \mathcal{H}$ *y* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. *Entonces*

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau).$$

Demostración. Ver Apéndice C. □

Sea $\mathcal{F}$ el subconjunto de $\mathcal{H}$ tal que

$$|z| \geq 1, -1/2 \leq Re(z) < 1/2, z \neq e^{i\theta} \text{ para } \pi/3 < \theta < \pi/2.$$

y sea $\rho = e^{2\pi i/3}$.

Proposición 2.17. *Dado* $\tau \in \mathcal{H}$, *existe* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ *tal que* $\frac{a\tau+b}{c\tau+d} = z \in \mathcal{F}$. *Además,* $z \in \mathcal{F}$ *es determinado de forma única por* τ.

Demostración. Ver [6, VII.1.2]. □

Corolario 2.18. *Sea un retículo* L. *Existe una base* $\{\omega_1, \omega_2\}$ *de* L *con* $\omega_1/\omega_2 \in \mathcal{F}$. *Es decir,* $L = (\lambda)(\mathbb{Z}\tau + \mathbb{Z})$ *para algún* $\lambda \in \mathbb{C}^*$ *y un* $\tau \in \mathcal{F}$ *determinado de forma única.*

Demostración. Sea una base $\{\alpha, \beta\}$ de L y $\tau_0 = \alpha/\beta$. Cambiando el signo de α si es necesario, suponemos que $\tau_0 \in \mathcal{H}$. Entonces existe un $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ tal que $\frac{a\tau_0+b}{c\tau_0+d} = \tau \in \mathcal{F}$. Sean $\omega_1 = a\alpha + b\beta$ y $\omega_2 = c\alpha + d\beta$. Entonces vemos que

$$L = \mathbb{Z}\alpha + \mathbb{Z}\beta = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = (\omega_2)(\mathbb{Z}\tau + \mathbb{Z}).$$

□

Definición 2.19. Dada una función f, y suponemos que $f(\tau) = a_n q^n + a_{n+1}q^{n+1} + \cdots$, con $n \in \mathbb{Z}$ y $a_n \neq 0$. Asume que la serie converge para todo q cercano a 0 (con $q \neq 0$ cuando $n < 0$). Entonces definimos el orden de f en $i\infty$ como $ord_{i\infty}(f) = n$.

Nótese que $q \to 0$ cuando $\tau \to i\infty$, así que el orden en $i\infty$ expresa el comportamiento de la función en ese caso.

Proposición 2.20. *Sea $f \neq 0$ función meromorfa en $\mathcal{H}$ y tal que*

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = f(\tau) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Entonces

$$ord_{i\infty}(f) + \frac{1}{3}ord_{\rho}(f) + \frac{1}{2}ord_{i}(f) + \sum_{z \neq i, i\infty, \rho} ord_z(f) = 0$$

Demostración. Ver [10, 9.16]. □

Corolario 2.21. *Si $z \in \mathbb{C}$, entonces existe un único $\tau \in \mathcal{F}$ tal que $j(\tau) = z$.*

Demostración. Ver Apéndice C. □

Corolario 2.22. *Sean retículos $L_1, L_2 \subset \mathbb{C}$. Entonces $j(L_1) = j(L_2)$ si y solo si existe $0 \neq \lambda \in \mathbb{C}$ tal que $\lambda L_1 = L_2$.*

Demostración. Hemos visto ya que $j(L_1) = j(\lambda L_1) = j(L_2)$. Veamos el otro caso. Suponemos $j(L_1) = j(L_2)$. Escribe $L_i = (\lambda_i)(\mathbb{Z}\tau_i + \mathbb{Z})$ con $\tau_i \in \mathcal{F}$ para $i = 1, 2$. Entonces $j(\tau_1) = j(L_1) = j(L_2) = j(\tau_2)$, por lo que el corolario anterior nos dice que $\tau_1 = \tau_2$. Tomando $\lambda = \lambda_2/\lambda_1$ tenemos que $\lambda L_1 = L_2$. □

Finalmente podemos probar que toda curva elíptica sobre $\mathbb{C}$ tiene un retículo asociado.

Teorema 2.23. *Sea $E : y^2 = 4x^3 - Ax - B$ una curva elíptica sobre $\mathbb{C}$. Entonces existe un retículo L tal que $g_2(L) = A$ y $g_3(L) = B$.*

Por Teorema 2.13, hay un isomorfismo de grupos entre $\mathbb{C}/L$ y $E(\mathbb{C})$.

Demostración. Ver Apéndice C. □

Con esto, damos por terminada esta sección sobre curvas elípticas sobre los complejos. Nuestro próximo objeto de interés son los puntos de orden finito, aquellos que sumados a sí mismos un número finito de veces dan el punto base $\mathcal{O}$. Además, nos centraremos en los puntos racionales que cumplen tal condición.

CAPÍTULO 3
Puntos racionales de orden finito

Los puntos de orden finito, o puntos de torsión, son aquellos puntos que sumados a sí mismos una cantidad finita de veces dan el punto base $\mathcal{O}$. En este apartado veremos diversos métodos para obtener estos puntos en una curva elíptica, con especial interés en el caso de puntos racionales en curvas elípticas definidas sobre $\mathbb{Q}$.

En particular, buscamos demostrar que el conjunto $E(\mathbb{Q})_{tors}$, que recordamos que es el subgrupo de puntos de orden finito, es un conjunto finito. Para ello demostraremos el Teorema de Nagell-Lutz, un resultado que nos da una condición sobre los puntos de orden finito que nos permitirá reducirnos a una cantidad finita de posibilidades.

Adicionalmente, veremos el concepto de polinomios de división, y veremos cómo utilizarlos para obtener las coordenadas de nP a partir de un punto P dado.

Nótese que toda curva con coeficientes racionales puede darse con coeficientes enteros. Esto es porque el cambio de variables $X = d^2x, Y = d^3y$ transforma la ecuación de $y^2 = x^3 + ax^2 + bx + c$ a $Y^2 = X^3 + d^2ax^2 + d^4bx + d^6c$. De esta forma, tomando un d suficientemente grande, podemos eliminar los denominadores de los coeficientes. Por tanto, podremos asumir que una ecuación en forma de Weierstrass con coeficientes racionales tiene coeficientes enteros.

Denotamos los puntos de n-torsión de una curva elíptica E sobre un cuerpo K como:

$$E[n] = \{P \in E(\overline{K}) | nP = \mathcal{O}\}.$$

3.1. Puntos racionales de orden finito. El Teorema de Nagell-Lutz

Dada una curva elíptica E definida sobre $\mathbb{Q}$, el Teorema de Nagell-Lutz nos da una condición necesaria sobre las coordenadas de un punto de $E(\mathbb{Q})$ para que sea de orden finito. Utilizando este resultado, podremos demostrar que el subgrupo de torsión es finito. Para llegar a este resultado, utilizaremos propiedades de divisibilidad por primos para obtener subgrupos de $E(\mathbb{Q})$, y trabajando sobre ellos obtendremos que todo punto en $E(\mathbb{Q})_{tors}$ tiene coordenadas enteras.

Definición 3.1. Sea $q \in \mathbb{Q}$, con $q \neq 0$. Escribimos $q = p^r a/b$, donde p es un primo y $p \nmid ab$. Definimos la valoración p-ádica de q como

$$v_p(q) = r.$$

Fijamos $v_p(0) = +\infty$. Esto es para que $v_p(0) > n$ para todo $n \in \mathbb{Z}$.

Definición 3.2. Sea E una curva elíptica sobre $\mathbb{Q}$ dada por una ecuación $y^2 = x^3 + Ax + B$, con $A, B \in \mathbb{Z}$. Sea r entero positivo. Definimos:

$$E_{p,r} = \{(x, y) \in E(\mathbb{Q}) \mid v_p(x) \leq 2r, v_p(y) \leq 3r\} \cup \{\mathcal{O}\}.$$

Estos son los puntos en los que x tiene al menos p^{2r} en el denominador e y tiene al menos p^{3r}. La idea es que estos puntos son cercanos "p-ádicamente" a $\mathcal{O}$. A partir de aquí escribimos $p \mid z$ ó $z \equiv 0 \pmod{p}$ para indicar que p divide el numerador de z.

Lema 3.3. *a)* $(x, y) \in E_{p,r}$ *si y solo si* $p^{3r} \mid s$.

b) Si $p^{3r} \mid s$, *entonces* $p^r \mid t$.

Demostración. a) Si $(x, y) \in E_{p,r}$, entonces $p^3 r$ divide el denominador de y, así que divide el numerador de $s = 1/y$. En el sentido contrario, si $p^{3r} \mid s$ es inmediato que p^{3r} divide el denominador de y, y por 2) tenemos que p^{2r} divide el denominador de x, por lo que $(x, y) \in E_{p,r}$.

b) Si $p^{3r} \mid s$, entonces tenemos que la potencia exacta que divide el denominador de y es p^{3k} con $k \geq r$. Por 2) tenemos que la que divide el denominador de x es p^{2k}, y por tanto la que divide $t = x/y$ es p^k. Como $k \geq r$, tenemos que $p^r \mid t$.

□

Lema 3.4. *Una recta* $t = c$ *con* $c \in \mathbb{Q}, c \equiv 0$ *(mod p) interseca la curva* $s = t^3 + Ats^2 + Bs^3$ *en como mucho un punto* (s, t) *con* $s \equiv 0$ *(mod p). La recta no es tangente a la curva en este punto.*

Demostración. Supongamos que tenemos dos puntos que lo cumplen, y que sus coordenadas s son s_1 y s_2. Sabemos que $s_1 \equiv s_2 \equiv 0 \pmod{p}$, y suponemos que $s_1 \equiv s_2 \equiv 0 \pmod{p^k}$ para algún $k \geq 1$. Escribimos $s_i' = ps_i$, y tenemos que $s_1' \equiv s_2' \equiv 0 \pmod{p^{k-1}}$. Así, ${s_1'}^2 \equiv {s_2'}^2 \equiv 0 \pmod{p^{k-1}}$, y de ahí sacamos que $s_1^2 = p^2 {s_1'}^2 \equiv p^2 {s_2'}^2 = s_2^2 \pmod{p^{k+1}}$. Usando un procedimiento similar, tenemos que $s_1^3 \equiv s_2^3 \pmod{p^{k+2}}$. Por tanto tenemos que

$$s_1 = c^3 + Acs_1^2 + Bs_1^3 \equiv c^3 + Acs_2^2 + Bs_2^3 = s_2 \pmod{p^{k+1}}.$$

Por inducción, obtenemos que $s_1 \equiv s_2 \equiv 0 \pmod{p^k}$ para todo k. Concluimos que $s_1 = s_2$, así que hay como mucho un punto que cumple $s \equiv 0 \pmod{p}$.

Mediante diferenciación implícita obtenemos la pendiente de la recta tangente:

$$\frac{ds}{dt} = 3t^2 + As^2 + 2Ast\frac{ds}{dt} + 3Bs^2\frac{ds}{dt} = \frac{3t^2 + As^2}{1 - 2Ast - 3Bs^2}$$

Si la recta $t = c$ es tangente a la curva, entonces $1 - 2Ast - 3Bs^2 = 0$. Pero $s \equiv 0 \pmod{p}$ nos da que $t \equiv 0 \pmod{p}$, lo que implica que $1 - 2Ast - 3Bs^2 \equiv 1 \not\equiv 0 \pmod{p}$.

Por tanto, $t = c$ no es tangente a la curva en ese punto. □

Teorema 3.5. *Sea E una curva elíptica dada por una ecuación $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$, p un primo y $r \in \mathbb{Z}^+$. Entonces:*

a) $E_{p,r}$ es subgrupo de $E(\mathbb{Q})$.

b) Si $(x, y) \in E(\mathbb{Q})$, entonces $v_p(x) < 0$ si y solo si $v_p(y) < 0$. Es ese caso, existe un entero positivo r tal que $v_p(x) = -2r$ y $v_p(y) = -3r$.

c) La aplicación

$$\begin{aligned} \lambda_{p,r} : E_{p,r}/E_{p,5r} &\to \mathbb{Z}_{p^4 r} \\ (x, y) &\mapsto p^{-r} x/y (mod\ p^4 r) \\ \mathcal{O} &\mapsto 0 \end{aligned}$$

es un homomorfismo inyectivo, con $\mathbb{Z}_{p^4 r}$ como grupo aditivo.

d) Si $(x, y) \in E_{p,r}$ pero $(x, y) \notin E_{p,r+1}$, entonces $\lambda_{p,r} \not\equiv 0$ (mod p).

Demostración. a) Ver la demostración de c).

b) El denominador de y^2 es igual al denominador de $x^3 + Ax + B$. Es inmediato que el denominador de x es divisible por p si y solo si el denominador de y es divisible por p. Si la potencia exacta que divide el denominador de y es $p^j (j > 0)$, entonces p^{2j} es la potencia exacta en el denominador de y^2. Similarmente, si la potencia exacta que divide el denominador de x es $p^k (k > 0)$, entonces el denominador de $x^3 + Ax + B$ es divisible exactamente por p^{3k}. Por tanto, $2j = 3k$. Concluimos que existe un r tal que $j = 3r$ y $k = 2r$.

c) Si $\lambda_{p,r} \equiv 0 \pmod{p^4 r}$, entonces $v_p(x/y) \geq 5r$, así que $(x, y) \in E_{5r}$. Entonces $\ker \lambda_{p,r} = \{0\}$, así que $\lambda_{p,r}$ es inyectivo.

Para ver que es homomorfismo, sean $t = \frac{x}{y},\ s = \frac{1}{y}$. Dividiendo la ecuación de la curva por y^3 obtenemos

$$s = t^3 + Ats^2 + Bs^3.$$

Nótese que $\lambda_{p,r}(-(x, y)) = \lambda_{p,r}(x, -y)) = -\lambda_{p,r}(x, y)$.

Tomamos tres puntos P_1, P_2, P_3 en la misma recta (es decir, $P_1 + P_2 + P_3 = \mathcal{O}$). Supongamos que la recta es $ax+by+d = 0$, o en coordenadas (s, t): $at+b+ds = 0$. Digamos que $P_i = (x_i, y_i)$ en coordenadas (x, y) y (s_i, t_i) en coordenadas (s, t) para $i = 1, 2, 3$.

Recordamos que utilizando coordenadas proyectivas, podemos ver que el orden de intersección de la recta y la curva no dependen de la elección de coordenadas. Así, utilizaremos coordenadas (s, t) para manejar el grupo.

Si $d = 0$, entonces la recta $at + b + ds = 0$ está en la forma del Lema 3.4. Por tanto, como pasa por (s_1, t_1) y (s_2, t_2), tenemos que $(s_1, t_1) = (s_2, t_2)$ y cambiando de coordenadas tenemos que $P_1 = P_2$. Por la ley de grupo, la recta $ax + by + d = 0$ es tangente en el punto, y cambiando de nuevo de coordenadas vemos que la recta $at + b + ds = 0$ es tangente en el punto, lo que es imposible por el lema. Por tanto, $d \neq 0$.

Ahora, dividiendo entre d tenemos que los puntos están en la recta $s = \alpha t + \beta$ para algún $\alpha, \beta \in \mathbb{Q}$. Vamos a demostrar que

$$\alpha = \frac{t_1^2 + t_1 t_2 + t_2^2 + A s_2^2}{1 - A(s_1 + s_2)t_1 - B(s_1^2 + s_1 s_2 + s_2^2)}.$$

Si $t_1 \neq t_2$, entonces $\alpha = (s_2 - s_1)/(t_2 - t_1)$. Como $s_i = t_i^3 + A t_i s_i^2 + B s_i^3$ vemos que

$$\begin{aligned}
&(s_2 - s_1)(1 - A(s_1 + s_2)t_1 - (s_1^2 + s_1 s_2 + s_2^2)) \\
&= s_2 - s_1 - A(s_2^2 - s_1^2)t_1 - B(s_2^3 - s_1^3) \\
&= (s_2 - A s_2^2 t_2 - B s_2^3) - (s_1 - A s_1^2 t_1 - B s_1^3) + A s_2^2 (t_2 - t_1) \\
&= t_2^3 - t_1^3 + A s_2^2 (t_2 - t_1) \\
&= (t_2 - t_1)(t_1^2 + t_1 t_2 + t_2^2 + A s_2^2).
\end{aligned}$$

Usando esto, vemos que $\alpha = (s_2 - s_1)/(t_2 - t_1)$ es de la forma indicada.

Supongamos ahora que $t_1 = t_2$. Por el Lema 3.4 tenemos que los dos puntos son iguales, es decir, que también se cumple que $s_1 = s_2$. Digamos $s_1 = s_2 = s$ y $t_1 = t_2 = t$. Entonces vemos que

$$\alpha = \frac{3t^2 + As^2}{1 - 2Ast - 3Bs^2}.$$

La recta tangente en ese punto es $s = \alpha t + \beta$, y para obtener la pendiente α derivamos implícitamente $s = t^3 + Ats^2 + Bs^3$ y despejamos ds/dt, obteneniendo el resultado indicado.

Como $s_1 \equiv s_2 \equiv 0 \pmod{p}$, tenemos que

$$1 - A(s_1 + s_2)t_1 - (s_1^2 + s_1 s_2 + s_2^2) \equiv 0 \pmod{p}$$

y como $p^r \mid t_i$, tenemos que

$$t_1^2 + t_1 t_2 + t_2^2 + A s_2^2 \equiv 0 \pmod{p^{2r}}.$$

Con esto y la expresión que hemos obtenido para α, vemos que $\alpha \equiv 0 \pmod{p^{2r}}$, y dado que $p^{3r} \mid s_i$ tenemos que

$$\beta = s_i - \alpha t_i \equiv 0 \pmod{p^{3r}}.$$

Ahora, para encontrar (s_3, t_3) tenemos que encontrar el tercer punto de intersección entre la recta y la curva, así que sustituyendo obtenemos:

$$\alpha t + \beta = t^3 + At(\alpha t + \beta)^2 + B(\alpha t + \beta)^3$$

que reescribimos como

$$0 = t^3 + \frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + A\alpha^2 + B\alpha^3}t^2 + ...$$

La suma de las tres raíces es menos el coeficiente de t^2. Como $p^{2r} \mid \alpha$ y $p^{3r} \mid \beta$, tenemos que

$$t_1 + t_2 + t_3 = -\frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + A\alpha^2 + B\alpha^3} \equiv 0 \pmod{p^{5r}}.$$

Como $t_1 \equiv t_2 \equiv 0 \pmod{p^r}$, tenemos que $t_3 \equiv 0 \pmod{p^r}$. Por tanto, $s_3 = \alpha t_3 + \beta \equiv 0 \pmod{p^{3r}}$, y por el primero de los lemas $P_3 \in E_{p,r}$. Esto demuestra *a*). Además se cumple que

$$\lambda_{p,r}(P_1) + \lambda_{p,r}(P_2) + \lambda_{p,r}(P_3) \equiv p^{-r}(t_1 + t_2 + t_3) \equiv 0 \pmod{p^{4r}}.$$

Esto nos muestra que

$$\lambda_{p,r}(P_1 + P_2) = \lambda_{p,r}(-P_3) = -\lambda_{p,r}(P_3) = \lambda_{p,r}(P_1) + \lambda_{p,r}(P_2),$$

lo que prueba que $\lambda_{p,r}$ es un homomorfismo.

d) Vemos que el conjunto de puntos en $E_{p,r}$ pero no en $E_{p,r+1}$ es

$$\{(x,y) \in E_{p,r} \mid v_p(x) = -2r, v_p(y) = -3r\} = \{(x,y) \in E_{p,r} \mid v_p(x/y) = r\}.$$

Entonces $p^{-r}x/y = x_1/y_1$ con $p \nmid x_1y_1$. Así, $\lambda_{p,r} \not\equiv 0 \pmod{p}$.

□

Corolario 3.6. *Siguiendo la notación del Teorema 3.5. Si $n > 1$ y n no es potencia de p, entonces $E_{p,1}$ no contiene puntos de orden exactamente n.*

Demostración. Supongamos que $P \in E_p, 1$ tiene orden n. Como n no es potencia de p, podemos multiplicar P por la mayor potencia de p que divida a n y obtener así un punto distinto de $\mathcal{O}$ cuyo orden es coprimo con p. Por tanto podemos asumir que P tiene orden n con $p \nmid n$. Sea r el mayor entero tal que $P \in E_{p,r}$. Entonces:

$$n\lambda_{p,r}(P) = \lambda_{p,r}(nP) = \lambda_{p,r}(\mathcal{O}) \equiv 0 \pmod{p^{4r}}.$$

Como $p \nmid n$, esto nos dice que $\lambda_{p,r}(P) \equiv 0 \pmod{p^{4r}}$, así que $P \in E_{5r}$. Esto contradice la elección de r. Por tanto, P no existe. □

Teorema de Nagell-Lutz. *Sea E curva elíptica dada por $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$. Sea $P = (x_0, y_0) \in E(\mathbb{Q})$ punto de orden finito. Entonces*

a) $x_0, y_0 \in \mathbb{Z}$.

b) *Si $y_0 \neq 0$, entonces $y_0^2 \mid 4A^3 + 27B^2$.*

Demostración. a) Suponemos que x_0 ó $y_0 \notin \mathbb{Z}$. Entonces uno de ellos tiene algún primo p dividiendo su denominador. Por Teorema 3.5 tenemos que $P \in E_{p,r}$ para algún $r \geq 1$.

Ahora sea n el orden de P y $l \mid n$ un primo. Entonces $Q = (n/l)P$ es un punto de orden l. Supongamos que l no es p. Entonces Corolario 3.6 nos dice que $E_{p,1}$ no contiene a Q, y por tanto tampoco $E_{p,r}$. Pero $E_{p,r}$ es un subgrupo de $E(\mathbb{Q})$ y contiene a P, así que debe contener a $(n/l)P = Q$. Por tanto l debe ser potencia de p, y como es primo, $l = p$.

Escogemos j tal que $Q \in E_{p,j}, Q \notin E_{p,j+1}$. Por Teorema 3.5, $\lambda_{p,j}(Q) \not\equiv 0 \pmod{p}$, y

$$p\lambda_{p,j}(Q) = \lambda_{p,j}(pQ) \equiv 0 \pmod{p^{4j}}$$

De esto concluimos que $\lambda_{p,j}(Q) \equiv 0 \pmod{p^{4j-1}}$. Pero esto se contradice con $\lambda_{p,j}(Q) \not\equiv 0 \pmod{p}$. Por tanto, $x_0, y_0 \in \mathbb{Z}$.

b) Asumimos que $y_0 \neq 0$. Entonces $2P = (x_2, y_2) \neq \mathcal{O}$. $2P$ tiene orden finito, por lo que $x_2, y_2 \in \mathbb{Z}$. Mediante la fórmula de duplicación (véase Apéndice B) tenemos

$$x_2 = \frac{x_0^4 - 2Ax_0^2 - 8Bx_0 + A^2}{4y_0^2}.$$

Como $x_2 \in \mathbb{Z}$, esto implica que $y_0^2 \mid x_0^4 - 2Ax_0^2 - 8Bx_0 + A^2$. Ahora hacemos un cálculo sencillo para ver que

$$(3x_0^2+4A)(x_0^4-2Ax_0^2-8Bx_0+A^2)-(3x_0^3-5Ax_0-27B)(x_0^3+Ax_0+B) = 4A^3+27B^2.$$

Vemos que y_0^2 divide a los dos términos de la izquierda. Por tanto, $y_0^2 \mid 4A^3 + 27B^2$.

□

Corolario 3.7. *Sea E una curva elíptica sobre $\mathbb{Q}$. Entonces $E(\mathbb{Q})_{tors}$ es finito.*

Demostración. Hemos visto que toda curva elíptica puede darse con una ecuación de Weierstrass. Recordamos que además, toda curva elíptica sobre $\mathbb{Q}$ puede darse con coeficientes enteros. Por el Teorema de Nagell-Lutz, solo hay una cantidad finita de posibilidades para las coordenadas de los puntos de torsión de una curva elíptica tal. Por tanto, el subgrupo de torsión debe ser finito. □

3.2. Reducción módulo p

Otra técnica para determinar el subgrupo de torsión es utilizar reducción módulo p, para un primo p. El resultado que utilizaremos nos dice que la reducción módulo p sobre los puntos racionales de la curva es una aplicación inyectiva, siempre que la curva resultante no sea singular. Esto nos permite reducir las opciones para el grupo de puntos racionales a partir del orden del grupo de puntos módulo p, y repetir el proceso con otros primos hasta reducir las posibilidades de grupo todo lo posible.

Este resultado dice:

Teorema 3.8. *Sea E curva elíptica dada por una ecuación $y^2 = x^3 + Ax + B$, con $A, B \in \mathbb{Z}$. Sea p un primo impar tal que $p \nmid 4A^3 + 27B^2$, y E_p la curva obtenida reduciendo módulo p los coeficientes de E. Sea*

$$\rho_p : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p)$$

la aplicación reducción módulo p. Sea $P \in E(\mathbb{Q})$ de orden finito con $\rho_p(P) = \mathcal{O}$. Entonces $P = \mathcal{O}$. Es decir, $E(\mathbb{Q})_{tors} \longrightarrow E_p(\mathbb{F}_p)$ es inyectiva.

Demostración. Por el Teorema de Nagell-Lutz, los puntos de torsión tienen coordenadas enteras excepto por $\mathcal{O}$. Los puntos con coordenadas enteras se reducen a puntos bien definidos módulo p. Por tanto, $\mathcal{O}$ es el único punto que se reduce a $\mathcal{O}$ (mod p). □

Este resultado complementa al Teorema de Nagell-Lutz, reduciendo aún más las posibilidades de $E(\mathbb{Q})_{tors}$, o en casos en los que factorizar $4A^3+27B^2$ es difícil. Nótese que ρ_p es de hecho un homomorfismo de grupos. La demostración de este resultado se sale del alcance de este documento.

3.3. Polinomios de división

Para generalizar, empezamos con A, B variables. Definimos los polinomios de división $\psi_m \in \mathbb{Z}[x, y, A, B]$ como:

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ para } m \geq 2 \\
\psi_{2m} &= (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ para } m \geq 3.
\end{aligned}$$

Lema 3.9. *Si n es impar, ψ_n es un polinomio en $\mathbb{Z}[x, y^2, A, B]$. Si n es par, ψ_n es un polinomio en $2y\mathbb{Z}[x, y^2, A, B]$.*

Demostración. El resultado se cumple para los $n \leq 4$. Asumimos que se cumple para todo $n < 2m$. Usamos inducción para probar el caso general: podemos asumir que $2m > 4$, así que $m > 2$ y entonces $2m > m + 2$, por lo que los polinomios en la definición de ψ_{2m} y ψ_{2m+1} cumplen la hipótesis inductiva.

Si m es par, entonces $\psi_m, \psi_{m+2}, \psi_{m-2}$ están en $2y\mathbb{Z}[x, y^2, A, B]$, lo que prueba que ψ_{2m} cumple el lema. Si m es impar, entonces ψ_{m-1}, ψ_{m+1} están en $2y\mathbb{Z}[x, y^2, A, B]$, y por tanto ψ_{2m} cumple el lema. Por tanto el lema se cumple para $n = 2m$.

Si m es par, entonces ψ_m, ψ_{m+2} están en $2y\mathbb{Z}[x, y^2, A, B]$, y por tanto $\psi_{m+2}\psi_m^3$ está en $\mathbb{Z}[x, y^2, A, B]$. Si m es impar, entonces ψ_{m-1}, ψ_{m+1} están en $2y\mathbb{Z}[x, y^2, A, B]$ y así $\psi_{m-1}\psi_{m+1}^3$ está en $\mathbb{Z}[x, y^2, A, B]$. Por tanto el lema se cumple para $n = 2m+1$. □

Ahora definimos:

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \tag{3.1}$$

$$\omega_m = (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2). \tag{3.2}$$

Lema 3.10. *$\phi_n \in \mathbb{Z}[x, y^2, A, B]$ para todo n. Si n es impar, $\omega_n \in y\mathbb{Z}[x, y^2, A, B]$. Si n es par, $\omega_n \in \mathbb{Z}[x, y^2, A, B]$.*

Demostración. Ver [10, 3.4]. □

A partir de ahora consideramos la curva elíptica $E : y^2 = x^3 + Ax + B$ con $4A^3+27B^2 \neq 0$. Así, podemos considerar los polinomios anteriores como polinomios en $\mathbb{Z}[x, A, B]$. Escribimos $\phi_n(x)$ y $\psi_n^2(x)$ (nota que $\psi_n(x)$ no es necesariamente polinomio en solo x).

Lema 3.11.

$$\phi_n(x) = x^{n^2} + \text{ términos de menor grado}$$
$$\psi_n^2(x) = n^2x^{n^2-1} + \text{ términos de menor grado}$$

Demostración. En particular, decimos que ψ_n es de esta forma:

$$\psi_n(x) = \begin{cases} y(nx^{(n^2-4)/2} + ...) & \text{si } n \text{ par} \\ nx^{(n^2-1)/2} + ... & \text{si } n \text{ impar.} \end{cases}$$

Para probar esto, utilizamos inducción. Los casos $n \leq 4$ se ven directamente.

- m par, $n = 2m + 1$. El término principal de $\psi_{m+2}\psi_m^3$ es

  $$(m + 2)m^3y^4x^{\frac{(m+2)^2-4}{2}+\frac{3m^2-12}{2}}$$

  y usando $y^2 = x^3 + Ax + B$ vemos que es $(m + 2)m^3x^{\frac{(2m+1)^2-1}{2}}$.

  De la misma forma, el término principal de $\psi_{m-1}\psi_{m+1}^3$ es $(m-1)(m+1)^3x^{\frac{(2m+1)^2-1}{2}}$.

  Simplificando obtenemos que el término principal de ψ_n es $(2m + 1)x^{\frac{(2m+1)^2-1}{2}}$ y sustituyendo $n = 2m + 1$ vemos que se cumple el lema.

- m par, $n = 2m$. De la misma forma que el caso anterior, el término principal de ψ_n es

  $$(2y)^{-1}[ymx^{\frac{m^2-4}{2}}][y((m + 2)(m - 1)^2 - (m - 2)(m + 1)^2)x^{3m^2/2}].$$

  Simplificando la última expresión, obtenemos $\frac{m}{2}x^{\frac{m^2-4}{2}}[4yx^{\frac{3m^2}{2}}]$ y simplificando esto, obtenemos $y(2m)x^{\frac{(2m)^2-4}{2}}$ que sustituyendo $n = 2m$ es lo que dice el lema.

Los casos con m impar se demuestran similarmente.

Habiendo demostrado que ψ_n es de la forma dicha, obtener el resultado para ψ_n^2 se hace elevando al cuadrado la expresión obtenida, y en el caso n par, usando $y^2 = x^3 + Ax + B$. El resultado para ϕ_n se obtiene a partir de que $x\psi_n^2$ y $\psi_{n-1}\psi_{n+1}$ tienen un término principal x^{n^2} con coeficientes n^2 y $n^2 - 1$ respectivamente. □

Ahora que tenemos definidos los polinomios de división, vamos a demostrar la relación entre ellos y la multiplicación de puntos en la curva. Para ello utilizaremos propiedades de curvas sobre complejos.

Sea $E : y^2 = x^3 + Ax + B$ una curva elíptica sobre $\mathbb{Q}$. Todas las ecuaciones de la ley de grupo están definidas sobre $\mathbb{Q}(A, B)$, y es fácil ver que se puede considerar $\mathbb{Q}(A, B)$ como subcuerpo de $\mathbb{C}$. Por tanto consideramos E como curva elíptica sobre $\mathbb{C}$, y por Teorema 2.23 hay un retículo L que corresponde a E. Sea $\wp(z)$ la función $\wp$ de Weierstrass asociada. Tenemos que $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$, con $g_2 = -4A, g_3 = -4B$. A partir de aquí derivaremos fórmulas para $\wp(nz)$ y $\wp'(nz)$, y obtendremos fórmulas para $n(x, y)$ utilizando que $x = \wp(z), y = \wp'(z)/2$.

Lema 3.12. *Hay una función doblemente periódica $f_n(z)$ tal que*

$$f_n(z)^2 = n^2 \prod_{0 \neq u \in (\mathbb{C}/L)[n]} (\wp(z) - \wp(u)).$$

El signo de $f_n(z)$ se puede escoger para que

a) Si n es par, $f_n = P_n(\wp)$ donde $P_n(X)$ es un polinomio de grado $(n^2 - 1)/2$ y coeficiente principal n.

b) Si n es impar, $f_n = \wp' P_n(\wp)$ donde $P_n(X)$ es un polinomio de grado $(n^2 - 4)/2$ y coeficiente principal $n/2$.

Los ceros de f_n son los puntos $0 \neq u \in (\mathbb{C}/L)[n]$ y son ceros simples.

Demostración. Como $\wp(u) = \wp(-u)$, los factores u y $-u$ en el producto son iguales. Si n es impar, entonces u no es congruente a $-u$ módulo L en ningún caso, así que todos los factores están dos veces. Por tanto podemos tomar f_n como $n\prod(\wp(z)-\wp(u))$ tomando solo un miembro de cada par $(u, -u)$. Como hay n^2-1 factores en el producto inicial, tenemos un polinomio de grado $(n^2-1)/2$ sobre $\wp(z)$ y de coeficiente principal n.

Si n es par, los únicos u congruentes a $-u$ módulo L son $u = \omega_j/2$ para $j = 1, 2, 3$. Como $(\wp')^2 = 4\prod(\wp - \wp(\omega_j/2))$, estos factores contribuyen $\wp'/2$ a f_n. Los demás factores se agrupan igual que en el otro caso, obteniendo un polinomio de grado $(n^2-4)/2$ y de coeficiente principal n. Combinando los dos resultados obtenemos que f_n tiene la forma buscada.

Está claro que f_n tiene ceros en cada $0 \neq u \in (\mathbb{C}/L)[n]$, y hay $n^2 - 1$ puntos de esta forma. El único polo (mod L) de f_n es en $z = 0$, de orden $n^2 - 1$, tenemos que estos son todos los ceros y son ceros simples. □

Lema 3.13. *Sea $n \geq 2$. Entonces*

$$\wp(nz) = \wp(z) - \frac{f_{n-1}(z)f_{n+1}(z)}{f_n(z)^2}.$$

Demostración. Sea $g(z) = \wp(nz) - \wp(z)$. Vamos a probar que g y $f_{n-1}f_{n+1}/f_n^2$ tienen el mismo divisor:

- $g(z)$ tiene un polo doble en cada $0 \neq u \in (\mathbb{C}/L)[n]$ y por su expansión en $z = 0$, también tiene un polo doble en 0. En total, contando multiplicidad, g tiene $2n^2$ polos.
- $g(z)$ tiene un cero en los puntos con $nz \equiv \pm z \pmod{L}$. Para esos puntos

$$\frac{d}{dz}g(z) = n\wp'(nz) - \wp'(z) = \pm n\wp'(z) - \wp'(z) = (\pm n + 1)\wp'(z).$$

Como los ceros de $\wp'$ son $\omega_j/2$, tenemos que $g'(z) \neq 0$ para $z \neq \omega_j/2$, así que son ceros simples. Cuando n es impar, $n(\omega_j) = \omega_j$, así que esos puntos son al menos ceros dobles.

Si $nz \equiv z \pmod{L}$, entonces $(n-1)z \equiv 0$. Si n es par, tenemos $(n-1)^2 - 1$ puntos con $(n-1)z = 0$ con $z \neq 0, \omega_j/2$. Similarmente, tenemos $(n+1)^2 - 1$ puntos con $(n+1)z = 0$ con $z \neq 0, \omega_j/2$. Por tanto tenemos $2n^2$ ceros, así que hemos encontrado todos los ceros. Si n es impar, tenemos 3 ceros menos en cada una de las cuentas, pero al menos 6 ceros (con multiplicidad) en los puntos $\omega_j/2$, así que hemos encontrado todos los ceros también.

Ahora pasamos a $f_{n-1}f_{n+1}/f_n^2$. Esta función tiene un polo doble en cada uno de los ceros de f_n. Si $z \neq 0$ y $(n \pm 1)z \equiv 0$, entonces $f_{n\pm1}$ tiene un cero simple en z. Los únicos puntos con $(n+1)z \equiv 0$ y $(n-1)z \equiv 0$ son los que cumplen $2z \equiv 0$, es decir, los $z = \omega_j/2$. Por tanto, $f_{n-1}f_{n+1}$ tiene un cero doble en esos puntos y un cero simple en otro caso.

Por su expansión en 0, la función tiene un polo doble en 0, así que su divisor es idéntico al de g. Por tanto las dos funciones son múltiplos (por constante). Como sus expansiones en 0 tienen el mismo coeficiente principal, deben ser iguales. □

Lema 3.14. $f_{2n+1} = f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1}$

Demostración. Vemos que

$$\wp((n+1)z) - \wp(nz) = -\frac{f_{2n+1}}{f_{n+1}^2 f_n^2},$$

ya que tienen el mismo divisor y sus expansiones en 0 tienen el mismo coeficiente principal. Por Lema 3.13 vemos que

$$\wp((n+1)z) - \wp(nz) = (\wp((n+1)z) - \wp(z)) - (\wp(nz) - \wp(z)) = -\frac{f_n f_{n+2}}{f_{n+1}^2} + \frac{f_{n-1}f_{n+1}}{f_n^2}.$$

Igualando ambas expresiones y despejando obtenemos el resultado buscado. □

Lema 3.15. $\wp' f_{2n} = (f_n)(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2)$.

Demostración. Ver [10, 9.30]. □

Lema 3.16. *a)* $\wp(2z_1) = \frac{1}{4}\left(\frac{6\wp(z_1)^2 - g_2/2}{\wp'(z_1)}\right)^2 - 2\wp(z_1)$.

b) $2\wp'' = (12\wp^2 - g_2)$.

c) $\wp(z_1+z_2) = \frac{1}{4}\left(\frac{\wp'(z_2)-\wp'(z_1)}{\wp(z_2)-\wp(z_1)}\right)^2 - \wp(z_1) - \wp(z_2)$.

Demostración. Ver las ecuaciones 9.10, 9.8 y 9.7 en [10, 9.10]. □

Lema 3.17. *Para todo $n \geq 1$,*

$$f_n(z) = \psi_n\left(\wp(z), \frac{1}{2}\wp'(z)\right).$$

Demostración. Ver que se cumple para $\psi_1 = 1$ es trivial. Los puntos en $(\mathbb{C}/L)[2]$ son 0 y los $\omega_j/2$, y como hemos visto que $(\wp')^2 = 4\prod(\wp - \wp(\omega_j/2))$ obtenemos que se cumple para $\psi_2 = 2y$. Para el caso $n = 3$ usamos Lema 3.13 y Lema 3.16*a*) y *b*) para ver que

$$\begin{aligned} -\frac{f_3}{(\wp')^2} &= -\frac{f_3}{f_2^2} = \wp(2z) - \wp(z) \\ &= \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 - 2\wp(z) - \wp(z) = -\frac{3\wp^4 - (3/2)g_2\wp^2 - 3g_3\wp - (1/16)g_2^2}{(\wp')^2}. \end{aligned}$$

Por tanto $f_3 = 3\wp^4 - (3/2)g_2\wp^2 - 3g_3\wp - (1/16)g_2^2 = 3\wp^4 + 6A\wp^2 - 12B\wp - A^2 = \psi_3(\wp)$. Para el caso $n = 4$ utilizamos Lema 3.16c para ver que

$$\wp(2z+z) = \frac{1}{4}\left(\frac{\wp'(2z) - \wp'(z)}{\wp(2z) - \wp(z)}\right)^2 - \wp(2z) - \wp(z)$$

y

$$\wp(2z-z) = \frac{1}{4}\left(\frac{\wp'(2z) + \wp'(z)}{\wp(2z) - \wp(z)}\right)^2 - \wp(2z) - \wp(z).$$

Utilizando esto vemos que

$$\begin{aligned} -\frac{f_4 f_2}{f_3^2} &= \wp(3z) - \wp(z) = \\ &= \frac{1}{4}\left(\frac{\wp'(2z) - \wp'(z)}{\wp(2z) - \wp(z)}\right)^2 - \frac{1}{4}\left(\frac{\wp'(2z) + \wp'(z)}{\wp(2z) - \wp(z)}\right)^2 \\ &= -\frac{\wp'(2z)\wp'(z)}{(\wp(2z) - \wp(z))^2} = -\frac{\wp'(2z)\wp'(z)}{(-f_3/\wp'(z)^2)^2} \\ &= -\frac{\wp'(2z)\wp'(z)^5}{-f_3^2}. \end{aligned}$$

Por tanto $f_4 f_2 = \wp'(2z)\wp'(z)^5$. $(1/2)\wp'(2z)$ es la coordenada y de $2(\wp(z), (1/2)\wp'(z))$, así que por las fórmulas de la ley de grupo (véase Apéndice B), obtenemos que $\wp'(2z) = -\lambda^3 + 2\lambda\wp(z) - \nu$, con $\lambda = \frac{3\wp(z)^2+A}{2\wp'}$ y $\nu = \frac{-\wp^3+A\wp+2B}{2\wp'}$. Sustituyendo esto y usando que $f_2 = \wp'(z)$ obtenemos que $f_4 = \psi_4(\wp, (1/2)\wp')$, que es el resultado buscado.

Como las f_n satisfacen las mismas relaciones de recurrencia que las ψ_n, obtenemos por inducción que el lema se cumple para toda n. □

Lema 3.18. $\wp'(nz) = f_{2n}/f_n^4$.

Demostración. La función $\wp'(nz)$ tiene polos triples en cada punto de $(\mathbb{C}/L)[n]$. En total, tiene $3n^2$ polos. Como los ceros de $\wp'$ son los puntos de $(\mathbb{C}/L)[2]$ que no son 0, tenemos que los ceros de $\wp'(nz)$ son los puntos de $(\mathbb{C}/L)[2n]$ que no están en $(\mathbb{C}/L)[n]$. Hay $3n^2$ puntos, y como el número de polos es igual al de ceros, deben ser ceros simples.

La función f_{2n}/f_n^4 tiene efectivamente ceros simples en los puntos de $(\mathbb{C}/L)[2n]$ y polos en los puntos de $(\mathbb{C}/L)[n]$. Vemos que los puntos en $(\mathbb{C}/L)[n]$ están en $(\mathbb{C}/L)[2n]$, así que el orden del polo es de $4 - 1 = 3$, por lo que son polos triples. Por tanto los divisores coinciden.

Utilizando las expansiones en $z = 0$, concluimos que ambas funciones son iguales. □

Teorema 3.19. *Sea $P = (x, y)$ un punto en una curva elíptica $E : y^2 = x^3 + Ax + B$ definida sobre $\mathbb{Q}$ y n entero positivo. Entonces*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3} \right).$$

Demostración. La curva E está definida sobre $\mathbb{Q}$, así que podemos asumir que está definido sobre $\mathbb{C}$. Tenemos que

$$(x, y) = \left(\wp(z), \frac{1}{2}\wp'(z) \right), \; n(x, y) = \left(\wp(nz), \frac{1}{2}\wp'(nz) \right)$$

para algún z. Por tanto,

$$\wp(nz) = \wp(z) - \frac{f_{n-1}f_{n+1}}{f_n^2} = \frac{\wp f_n^2 - f_{n-1}f_{n+1}}{f_n^2} = \frac{x\psi_n^2 - \psi_{n-1}\psi_{n+1}}{\psi_n^2} = \frac{\phi_n}{\psi_n^2}.$$

Esto prueba la fórmula para la coordenada x. Para la coordenada y, basta observar que $\omega_n = \frac{1}{2}\frac{\psi_{2n}}{\psi_n}$ y por tanto

$$\frac{1}{2}\wp'(nz) = \frac{1}{2}\frac{\psi_{2n}}{\psi_n^4} = \frac{\omega_n}{\psi_n^3}.$$

□

Corolario 3.20. *Sea E curva elíptica. El endomorfismo de E dado por la multiplicación por n tiene grado n^2.*

Demostración. Por Lema 3.11 tenemos que el grado del endomorfismo $\frac{\phi_n(x)}{\psi_n^2(x)}$ es n^2 siempre que $\phi_n(x)$ y $\psi_n^2(x)$ no tengan raíces comunes. Suponemos que no es así, y sea n el menor índice para el que existe una raíz común. Suponemos que $n = 2m$ es par. Vemos que

$$\phi_2(x) = x^4 - 2Ax^2 - 8Bx + A^2.$$

Computamos la coordenada de $2m(x, y)$ multiplicando por m y después por 2, y como $\psi_2^2 = 4y^2 = 4(x^3 + Ax + B)$ obtenemos

$$\frac{\phi_{2m}}{\psi_{2m}^2} = \frac{\phi_2(\phi_m/\psi_m^2)}{\psi_2^2(\phi_m/\psi_m^2)} = \frac{\phi_m^4 - 2A\phi_m^2\psi_m^4 - 8B\phi_m\psi_m^6 + A^2\psi_m^8}{(4\psi_m^2)(\phi_m^3 + A\phi_m\psi_m^4 + B\psi_m^6)} := \frac{U}{V}$$

Podemos encontrar polinomios f_1, f_2, g_1, g_2[1]tales que

$$U \cdot f_1(\phi_m, \psi_m^2) - V \cdot g_1(\phi_m, \psi_m^2) = 4\psi_m^{14}\Delta$$
$$U \cdot f_2(\phi_m, \psi_m^2) + V \cdot g_2(\phi_m, \psi_m^2) = 4\phi_m^7\Delta.$$

Por tanto, si U y V tienen una raíz común, también la tienen ϕ_m y ψ_m^2. Pero $n = 2m$ era el menor índice para el cual hay una raíz común, así que no es posible.

Por último, hemos visto que ϕ_{2m} y ψ_{2m}^2 son múltiplos de U y V respectivamente. Con Lema 3.11 vemos que el término principal de U es x^{4m^2} y por el mismo lema tiene que ser $U = \phi_{2m}$. Se sigue que $V = \psi_{2m}^2$, y hemos demostrado lo que buscábamos.

Ahora veamos el caso de que $n = 2m + 1$ es impar. Sea r una raíz común. Por la definición de ϕ_n obtenemos que r es raíz de $\psi_{n+1}\psi_{n-1}$. Tenemos entonces que $\psi_{n\pm1}^2$ son polinomios en x cuyo producto se anula en r, así que uno de ellos tiene a r como raíz. Digamos $\psi_{n+\delta}^2(r) = 0$ con $\delta = 1$ ó -1.

Como n es impar, ψ_n y $\psi_{n+2\delta}$ son polinomios en x y $(\psi_n\psi_{n+2\delta})^2 = \psi_n^2\psi_{n+2\delta}^2$ se anula en r. Por tanto $\psi_n\psi_{n+2\delta}$ se anula en r y como $\phi_{n+\delta} = x\psi_{n+\delta}^2 - \psi_n\psi_{n+2\delta}$ tenemos que $\phi_{n+\delta}(r) = 0$. Por tanto $\phi_{n+\delta}$ y $\psi_{n+\delta}^2$ tienen una raíz común, y $n + \delta$ es par.

Como vimos en el caso anterior, si ϕ_{2m} y ψ_{2m}^2 tienen una raíz común, también lo tienen ϕ_m y ψ_m^2. Aplicamos esto a $2m = n + \delta$, y como n es el menor índice en el que hay una raíz común, tenemos que $(n+\delta)/2 \geq n$. Esto implica que $n = 1$. Pero $\phi_1 = x$ y $\psi_1^2 = 1$ que claramente no tienen raíces comunes.

Por tanto, ϕ_n y ψ_n^2 no tienen raíces comunes, lo que demuestra que la multiplicación por n tiene grado n^2. □

A partir de esto podemos probar este teorema:

Teorema 3.21. *Sea E curva elíptica sobre $\mathbb{Q}$ y n entero positivo. Entonces*

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

[1]Tomando U, V como polinomios sobre ϕ_m, ψ_m^2, el algoritmo de Euclides seguido de transformaciones sencillas encuentra los polinomios que cumplen esta relación. Véase [10, Lemma 3.8] para más detalles.

Demostración. El numerador de la derivada de $\phi_n(x)/\psi_n^2(x)$ es $n^2x^{2n^2-2} \neq 0$ (ya que la característica es 0). Esto prueba que el endomorfismo de multiplicación por n es separable. Por tanto, $E[n]$ tiene orden n^2. El teorema de estructura de grupos abelianos finitos nos dice que $E[n]$ es isomorfo a $\mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$ para algunos enteros $n_1, ..., n_k$ con $n_i \mid n_{i+1}$ para todo i. Sea l un primo que divide a n_1. Entonces $l \mid n_i$ para todo i. Por tanto $E[l] \subset E[n]$ tiene orden l^k, y como hemos probado que tiene orden l^2, tenemos que $k = 2$.

La multiplicación por n anula $E[n] \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$, así que $n_2 \mid n$. Como $\#E[n] = n^2 = n_1n_2$, tenemos que $n_1 = n_2 = n$. Por tanto, tenemos que

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

□

3.4. Teorema de Mazur

Para cerrar este documento, mencionamos un importante resultado reciente. La demostración de este resultado se sale del alcance de este trabajo. No obstante, la importancia del resultado hace que sea necesario mencionarlo.

Teorema de Mazur. *Sea E curva elíptica definida sobre $\mathbb{Q}$. Entonces su subgrupo de torsión es o bien $\mathbb{Z}/n\mathbb{Z}$ para $1 \leq n \leq 10$ ó $n = 12$, o bien $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ para $1 \leq n \leq 4$.*

A partir de este resultado, la computación de puntos de orden finito se vuelve más sencilla, debido a que tenemos una cota superior para el orden de un punto de torsión.

APÉNDICE A

Nociones básicas de geometría algebraica de curvas

En esta sección definimos los conceptos básicos que damos por conocidos en el cuerpo del documento. También introduciremos algunos conceptos más avanzados, como divisores y diferenciales, con el objetivo de enunciar el Teorema de Riemann-Roch.

A.1. Variedades

Comenzamos estableciendo algunos conceptos de variedades afines y proyectivas. Dado que una curva es una variedad de dimensión 1, tenemos que definir dichos conceptos.

Definición A.1. Dado un ideal $I \subset \overline{K}[X]$, asociamos un conjunto de puntos

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \ \ \forall f \in I\}.$$

Llamamos conjunto algebraico (afin) a cualquier conjunto $V \subset \mathbb{A}^n$ tal que existe $I \subset \overline{K}[X]$ con $V = V_I$. Dado un conjunto algebraico V, definimos el ideal de V como

$$I(V) = \{f \in \overline{K}[X] : f(P) = 0 \ \ \forall P \in V\}.$$

Un conjunto algebraico V se dice definido sobre K si $I(V)$ es generado por polinomios con coeficientes en K. Esto se denota V/K. Si V/K, entonces el conjunto de puntos K-racionales de V es

$$V(K) = V \cap \mathbb{A}^n.$$

Equivalentemente, $V(K) = \{P \in V : P^\sigma = P \ \ \forall \sigma \in G_{\overline{K}/K}\}$.

Una variedad algebraica (afin) V es un conjunto algebraico cuyo $I(V)$ es un ideal primo en $\overline{K}[X]$.

Ahora veamos el caso proyectivo. Debido a la relación de equivalencia en la definición del espacio proyectivo, no es posible usar ideales de polinomios arbitrarios, así que necesitamos esta definición.

Definición A.2. Un polinomio $f \in \overline{K}[X]$ es homogéneo de grado d si $f(\lambda X_0, ..., \lambda X_n) = \lambda^d f(X_0, ..., X_n)$ para todo $\lambda \in \overline{K}$. Un ideal $I \subset \overline{K}[X]$ es homogéneo si es generado por polinomios homogéneos.

Vemos que esta condición es necesaria para poder definir bien la evaluación a 0 de un polinomio en un punto del espacio proyectivo. Por tanto, ahora podemos definir:

Definición A.3. Dado un ideal homogéneo $I \subset \overline{K}[X]$, asociamos un conjunto de puntos

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0 \ \ \forall f \text{ homogéneo} \in I\}.$$

Llamamos conjunto algebraico (proyectivo) a cualquier conjunto $V \subset \mathbb{P}^n$ tal que existe $I \subset \overline{K}[X]$ con $V = V_I$. Dado un conjunto algebraico V, definimos el ideal de V como

$$I(V) = \{f \in \overline{K}[X] : f \text{ homogéneo}, f(P) = 0 \ \ \forall P \in V\}.$$

Un conjunto algebraico proyectivo V se dice definido sobre K, denotado V/K, si $I(V)$ es generado por polinomios homogéneos con coeficientes en K. Si V/K, entonces el conjunto de puntos K-racionales de V es

$$V(K) = V \cap \mathbb{P}^n.$$

Igual que en el caso afín, se cumple que $V(K) = \{P \in V : P^\sigma = P \ \ \forall \sigma \in G_{\overline{K}/K}\}$.

Una variedad algebraica (proyectiva) V es un conjunto algebraico cuyo $I(V)$ es un ideal primo en $\overline{K}[X]$. Existe una relación entre variedades afines y proyectivas que nos permitirá manejarlas similarmente. Para verlo, llamemos f^* a la homogenización de f respecto a una variable arbitraria X_i. Entonces, dada una variedad afin V, definimos la clausura proyectiva de V como $\overline{V} = \{f^*(X) : f \in I(V)\}$. No entraremos en detalles sobre (de)homogenización, pero véase [8, p. 9].

Proposición A.4. *a) Sea V una variedad afín. Entonces $\overline{V}$ es una variedad proyectiva y*

$$V = \overline{V} \cap \mathbb{A}^n.$$

b) Sea V una variedad proyectiva. Entonces $V \cap \mathbb{A}^n$ es una variedad afín y

$$V \cap \mathbb{A}^n = \emptyset \qquad \text{ó} \qquad V = \overline{V \cap \mathbb{A}^n}$$

c) Si una variedad afín (resp. proyectiva) V está definida sobre K, entonces $\overline{V}$ (resp. $V \cap \mathbb{A}^n$) también está definida sobre K.

Demostración. Ver [2, I.2.3]. □

De esta forma, podemos definir importantes propiedades de una variedad proyectiva a partir de su variedad afín asociada.

Sea ahora una variedad afín V/K. El anillo de coordenadas afín se define como:

$$K[V] = \frac{K[X]}{I(V) \cap K[X]},$$

$$\overline{K}[V] = \frac{\overline{K}[X]}{I(V)},$$

sobre K y sobre $\overline{K}$ respectivamente. Estos anillos son dominios de integridad, y su cuerpo de fracciones se denomina $K(V)$ (y $\overline{K}(V)$ respectivamente) y se llama cuerpo de funciones de V. El cuerpo de funciones de una variedad proyectiva $\overline{V}$, denotado por $K(\overline{V})$, es el cuerpo de funciones de $\overline{V} \cap \mathbb{A}^n$ y equivalentemente con $\overline{K}(\overline{V})$.

Si V/K, podemos extender la acción de $G_{\overline{K}/K}$ a $\overline{K}[V]$ y $\overline{K}(V)$. Entonces $K[V]$ y $K(V)$ son los subconjuntos de $\overline{K}[V]$ y $\overline{K}(V)$, respectivamente, fijados por $G_{\overline{K}/K}$.

Definición A.5. La dimensión de una variedad afín V, denotada por $dim(V)$, es el grado de trascendencia de $\overline{K}(V)$ sobre $\overline{K}$.
La dimensión de una variedad proyectiva $\overline{V}$, denotada por $dim(\overline{V})$, es la dimensión de su variedad afín asociada $\overline{V} \cap \mathbb{A}^n$ (nota que se debe escoger la dehomogenización adecuada para que $\overline{V} \cap \mathbb{A}^n \neq \emptyset$).

Definición A.6. Sea V variedad afín, $P \in V$ y f_1, ..., $f_m \in \overline{K}[X]$ generadores de $I(V)$. Entonces V es suave en P si la matriz

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{\substack{1\leq i\leq m \\ 1\leq j\leq n}}$$

tiene rango $n - dim(V)$. Se dice que V es suave si lo es en todo punto.

Sea una variedad proyectiva $\overline{V}$, $P \in \overline{V}$ y escogemos la dehomogenización tal que $P \in \mathbb{A}^n$. Entonces $\overline{V}$ es suave en P si $\overline{V} \cap \mathbb{A}^n$ es suave en P.

Definición A.7. El anillo local de una variedad afín V en P es

$$\overline{K}[V]_P = \{f/g : f, g \in \overline{K}[V], g(P) \neq 0\} \subset \overline{K}(V).$$

Las funciones en $\overline{K}[V]_P$ se dicen regulares (o definidas) en P.

El anillo local de una variedad proyectiva $\overline{V}$ en P, denotado $\overline{K}[\overline{V}]_P$, es el anillo local de $\overline{V} \cap \mathbb{A}^n$ en P. Una función $F \in \overline{K}(\overline{V})$ es regular en P si pertenece a $\overline{K}[\overline{V}]_P$.

A.2. Aplicaciones racionales

En esta sección, veremos las propiedades de aplicaciones entre variedades y la relación entre las funciones de una curva y las aplicaciones que salen de ella.

Definición A.8. Sean V_1, $V_2 \subset \mathbb{P}^n$ variedades. Una aplicación racional de V_1 a V_2 es una aplicación de la forma

$$\phi : V_1 \longrightarrow V_2,\ \phi = [f_0, ..., f_n],$$

donde $f_0, ..., f_n \in \overline{K}(V_1)$ cumplen que para todo $P \in V_1$ donde todas las f están definidas,

$$\phi(P) = [f_0(P), ..., f_n(P)] \in V_2.$$

Si V_1/K y V_2/K, entonces $G_{\overline{K}/K}$ actúa en ϕ de la forma obvia

$$\phi^\sigma(P) = [f_0^\sigma(P), ..., f_n^\sigma(P)].$$

Así, si V_1/K y V_2/K y además existe un $\lambda \in \overline{K}^*$ tal que $\lambda f_0, ..., \lambda f_n \in K(V_1)$, entonces se dice que ϕ está definido sobre K. Como es usual, ϕ está definido sobre K si y solo si $\phi^\sigma = \phi$ para todo $\sigma \in G_{\overline{K}/K}$.

Nota que dada esta definición, una aplicación racional no es necesariamente una función bien definida en todo punto de V_1. Sin embargo, es posible evaluar $\phi(P)$ en puntos donde alguna f_i no es regular mediante una transformación:

Definición A.9. Una aplicación racional

$$\phi : V_1 \longrightarrow V_2,\ \phi = [f_0, ..., f_n]$$

es regular (o definida) en $P \in V_1$ si existe un $g \in \overline{K}(V_1)$ tal que

a) gf_i es regular para todo i;

b) $(gf_i)(P) \neq 0$ para algún i.

Si existe tal g, entonces fijamos

$$\phi(P) = [(gf_0)(P), ..., (gf_n)(P)].$$

Una aplicación racional regular en todo punto se llama morfismo.

Definición A.10. Sean variedades V_1, V_2. Decimos que V_1 y V_2 son isomorfas, escrito $V_1 \cong V_2$, si existen **morfismos** $\phi : V_1 \longrightarrow V_2$ y $\psi : V_2 \longrightarrow V_1$ tales que $\psi \circ \phi$ y $\phi \circ \psi$ son las aplicaciones identidad en V_1 y V_2 respectivamente. Si ambas variedades y ambos morfismos se definen sobre K, decimos que V_1 y V_2 son isomorfas sobre K.

A partir de aquí nos centraremos en curvas. Antes de nada, definimos el concepto.

Definición A.11. Una curva es una variedad proyectiva de dimensión 1.

Nota que en general, trataremos una curva mediante una ecuación afín, usando la relación entre la variedad proyectiva y su variedad afín asociada de forma implícita. En primer lugar, definimos un ideal maximal de $\overline{K}[V]$ para cada punto, que será importante para definiciones posteriores.

Proposición A.12. *Sea V variedad, $P \in V$. Entonces*

$$M_P = \{f \in \overline{K}[V] : f(P) = 0\}$$

es un ideal maximal de $\overline{K}[V]$.

Demostración. Ver que es ideal es trivial. Para ver que es efectivamente maximal, vemos que

$$\overline{K}[V]/M_P \longrightarrow \overline{K},\ f \longmapsto f(P)$$

es un isomorfismo. Por tanto $\overline{K}[V]/M_P$ es un cuerpo, así que M_P es maximal. □

Definición A.13. Sea una curva C y $P \in C$ suave. La valoración (normalizada) de una función f regular en P es:

$$ord_P(f) = sup\{d \in \mathbb{Z} : f \in M_P^d\}$$

Extendemos esta definición a cualquier $f \in \overline{K}(C)$ estableciendo $ord_P(f/g) = ord_P(f) - ord_P(g)$. Decimos que $ord_P(f)$ es el orden de f en P.

Definición A.14. Un uniformizador de C en P es cualquier $t \in \overline{K}(C)$ tal que $ord_P(t) = 1$.

Definición A.15. Dada una función $f \in \overline{K}(C)$,

- f tiene un cero en P si $ord_P(f) > 0$.
- f tiene un polo en P si $ord_P(f) < 0$. En ese caso, escribimos $f(P) = \infty$.
- Si $ord_P(f) \geq 0$, entonces f es regular en P y podemos evaluar $f(P)$.

Proposición A.16. *Sea C curva suave y $f \in \overline{K}(C)$ con $f \neq 0$. Entonces solo hay un número finito de puntos de C en los que f tiene un cero o un polo. Además, si f no tiene polos, entonces $f \in \overline{K}$.*

Demostración. Ver [2, I.6.5], [2, II.6.1] para ver la finitud del número de polos. Para ver los ceros, aplica esto a $1/f$. Para el último enunciado, ver [2, I.3.4a]. □

Ahora vemos que en curvas suaves, una aplicación racional es siempre un morfismo.

Proposición A.17. *Sea C una curva, $P \in C$ suave, una variedad V y $\phi : C \longrightarrow V$ una aplicación racional. Entonces ϕ es regular en P. En particular, si C es suave, entonces ϕ es un morfismo.*

Demostración. Escribe $\phi = [f_0, ..., f_N]$ con $f_i \in \overline{K}(C)$. Tomamos un uniformizador $t \in \overline{K}(C)$ de C en P. Sea $n = \min_{0 \leq i \leq N} ord_P(f_i)$.

Entonces $ord_P(t^{-n} f_i) = ord_P(f_i) - n \geq 0$ para todo i y existe j tal que $ord_P(t^{-n} f_j) = 0$ (porque $ord_P(f_i) = n$), lo que es equivalente a $(t^{-n} f_j)(P) \neq 0$. Por tanto, ϕ es regular en P. □

De esta forma, no debemos preocuparnos por la regularidad de las aplicaciones cuando trabajemos con curvas suaves. De hecho, cuando la variedad destino es también una curva, se puede demostrar una propiedad más fuerte.

Teorema A.18. *Sea $\phi : C_1 \longrightarrow C_2$ un morfismo de curvas. Entonces ϕ es constante o sobreyectivo.*

Demostración. Ver [2, II.6.8]. □

Sean C_1/K y C_2/K curvas y $\phi : C_1 \longrightarrow C_2$ un morfismo no constante definido sobre K. Entonces la composición con ϕ induce una inyección de cuerpos de funciones que deja fijo K,

$$\phi^* : K(C_2) \longrightarrow K(C_1),\ \phi^* f = f \circ \phi.$$

Teorema A.19. *Sean C_1/K y C_2/K curvas.*

a) Sea $\phi : C_1 \longrightarrow C_2$ una aplicación racional no constante definido sobre K. Entonces $K(C_1)$ es una extensión finita de $\phi^*(K(C_2))$.

b) Sea $\iota : K(C_2) \longrightarrow K(C_1)$ una inyección de cuerpos de funciones que deja fijo K. Entonces existe un único $\phi : C_1 \longrightarrow C_2$ aplicación racional no constante definida sobre K tal que $\phi^* = \iota$.

c) Sea $F \subset K(C_1)$ un subgrupo de índice finito que contiene K. Entonces existe una curva suave C'/K (única salvo K-isomorfismo) y una aplicación racional $\phi : C_1 \longrightarrow C'$ no constante definida sobre K, tales que $\phi^* K(C') = F$.

Demostración. a) Ver [2, II.6.8].

b) Sea $C_1 \subset \mathbb{P}^N$ y para cada i (de 1 a n) sea $g_i \in K(C_2)$ la función en C_2 correspondiente a X_i/X_0 (podemos asumir que C_2 no está contenido en el hiperplano $X_0 = 0$.) Entonces

$$\phi = [1, \iota(g_1), ..., \iota(g_N)]$$

da una aplicación $\phi : C_1 \longrightarrow C_2$ con $\phi^* = \iota$. Esta ϕ no es constante, ya que no todas las g_i pueden ser constantes y ι es inyectiva.

Si $\psi = [f_0, ..., f_N]$ es otra aplicación con $\psi^* = \iota$, entonces para cada i, $f_i/f_0 = \psi^* g_i = \phi^* g_i = \iota(g_i)$ lo que demuestra que $\psi = \phi$. Por tanto ϕ es única.

c) Ver [2, II.6.12].

□

Definición A.20. Sea $\phi : C_1 \longrightarrow C_2$ aplicación de curvas definida sobre K. Si ϕ es constante, definimos su grado como 0. En otro caso, decimos que ϕ es una aplicación finita y definimos su grado como

$$deg(\phi) = [K(C_1) : \phi^* K(C_2)].$$

Corolario A.21. *Sean C_1 y C_2 curvas suaves y $\phi : C_1 \longrightarrow C_2$ una aplicación racional de grado 1. Entonces ϕ es un isomorfismo.*

Demostración. Por definición, si $deg(\phi) = 1$ entonces $\phi^* K(C_2) = K(C_1)$ así que ϕ^* es un isomorfismo de cuerpos de funciones. Por tanto hay una aplicación racional $\psi : C_2 \longrightarrow C_1$ tal que $\psi^* = (\phi^*)^{-1}$. Ya que C_2 es suave, ψ es un morfismo. Por tanto, $(\phi \circ \psi)^* = \psi^* \circ \phi^*$ es la identidad en $\overline{K}(C_2)$ y similarmente $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ es la identidad en $\overline{K}(C_1)$. Por el Teorema A.19b eso implica que $\phi \circ \psi$ y $\psi \circ \phi$ son la identidad en C_2 y C_1 respectivamente. Por tanto ϕ (y ψ) son isomorfismos. □

Continuamos con el concepto de ramificación de una aplicación racional:

Definición A.22. Sea $\phi : C_1 \longrightarrow C_2$ aplicación racional no constante de curvas suaves y $P \in C_1$. Sea $t_{\phi(P)} \in K(C_2)$ un uniformizador en $\phi(P)$. El índice de ramificación de ϕ en P es

$$e_\phi(P) = ord_P(\phi^* t_{\phi(P)}).$$

Nota que $e_\phi(P) \geq 1$. Decimos que ϕ es no-ramificado en P si $e_\phi(P) = 1$, y decimos que ϕ es no-ramificado si lo es en todo punto de C_1.

Proposición A.23. *Sea $\phi : C_1 \longrightarrow C_2$ aplicación racional no constante de curvas suaves.*

a) Para todo $Q \in C_2$,

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = deg(\phi).$$

b) Sea $\psi : C_2 \longrightarrow C_3$ otra aplicación racional no constante de curvas suaves. Entonces para todo $P \in C_1$,

$$e_{\psi\circ\phi}(P) = e_\phi(P) e_\psi(\phi(P)).$$

Demostración. a) Ver [7, III §2, Theorem 1].

b) Sean $t_{\phi(P)}$ y $t_{\psi(\phi(P))}$ uniformizadores en los puntos correspondientes.

Por definición, la función $t_{\phi(P)}$ tiene orden 1 en $\phi(P)$, y por tanto $t_{\phi(P)}^{e_\psi(\phi(P))}$ tiene orden $e_\psi(\phi(P))$ en ese punto. También por definición, tenemos que $e_\psi(\phi(P)) = ord_{\phi(P)}(\psi^* t_{\psi(\phi(P))})$. Por tanto, la función $\psi^* t_{\psi(\phi(P))}$ tiene orden $e_\psi(\phi(P))$ en $\phi(P)$. Las dos funciones tienen el mismo orden en ese punto.

Ahora aplicamos ϕ^*. Como tienen el mismo orden en $\phi(P)$, al aplicar ϕ^* tienen el mismo orden en P. Escribiendo esto vemos que

$$ord_P(\phi^* t_{\phi(P)}^{e_\psi(\phi(P))}) = ord_P((\psi\phi)^* t_{\psi(\phi(P))}).$$

Para obtener el resultado deseado, vemos que la expresión a la derecha es la definición de $e_{\psi\circ\phi}(P)$, y en la expresión a la izquierda vemos que

$$\begin{aligned} ord_P(\phi^* t_{\phi(P)}^{e_\psi(\phi(P))}) &= ord_P(\phi^* t_{\phi(P)}^{ord_P(\psi^* t_{\psi(\phi(P))})}) \\ &= ord_P(\phi^* t_{\phi(P)}) * ord_P(\psi^* t_{\psi(\phi(P))}) = e_\phi(P) e_\psi(\phi(P)). \end{aligned}$$

□

Corolario A.24. *Una aplicación $\phi : C_1 \longrightarrow C_2$ es no-ramificada si y solo si*

$$\#\phi^{-1}(Q) = deg(\phi) \quad \forall Q \in C_2$$

Demostración. Por la Proposición A.23a vemos que

$$deg(\phi) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \#\phi^{-1}(Q).$$

Como $e_\phi(P) \geq 1$, esto se cumple si y solo si $e_\phi(P) = 1$ para cada P, es decir, ϕ es no-ramificada. □

Antes de pasar a la siguiente sección, enunciamos el Teorema de Bezout, un resultado que nos permite conocer el número de puntos de intersección entre dos curvas proyectivas.

Teorema de Bezout. *Sean C_1 y C_2 curvas proyectivas sin componentes comunes, de grados d_1 y d_2 respectivamente. Entonces*

$$\#(C_1 \cap C_2) = d_1 d_2.$$

Demostración. Ver [9, Apéndice A.4]. □

A.3. Divisores

El grupo divisor de una curva C, denotado por Div(C), es el grupo abeliano libre generado por los puntos de C. Un divisor, es decir, un elemento $D \in Div(C)$, es una suma formal:

$$D = \sum_{P \in C} n_P(P)$$

donde cada $n_P \in \mathbb{Z}$ y $n_P \neq 0$ en una cantidad finita de puntos.

El grado de D se define como:

$$deg(D) = \sum_{P \in C} n_P.$$

Los divisores de grado 0 forman un subgrupo de $Div(C)$ que denotamos por $Div^0(C)$.

Si C/K, entonces $G_{\overline{K}/K}$ actúa sobre $Div(C)$:

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma).$$

Entonces decimos que D está definido sobre K si $D^\sigma = D$ para todo $\sigma \in G_{\overline{K}/K}$ (nota que esto no es equivalente a que todos los P con $n_P \neq 0$ pertenezcan a $C(K)$, basta con que $G_{\overline{K}/K}$ permute los coeficientes apropiadamente).

Dada una curva C suave y $f \in \overline{K}(C)^*$ una función del cuerpo de funciones de la curva. Asociamos a f el divisor:

$$div(f) = \sum_{P \in C} ord_P(f)(P).$$

Por la Proposición A.16 sabemos que existe un número finito de puntos cuyo orden es distinto de 0, así que $div(f)$ está bien definido.

Definición A.25. Un divisor $D \in Div(C)$ es principal si existe $f \in \overline{K}(C)^*$ tal que $D = div(f)$.

Definición A.26. Dos divisores $D_1, D_2 \in Div(C)$ son linealmente equivalentes, denotado $D_1 \sim D_2$ si $D_1 - D_2$ es un divisor principal.

Proposición A.27. *La relación $\sim$ así definida es una relación de equivalencia.*

Demostración. $\sim$ es relación de equivalencia si cumple las tres propiedades:

- Reflexiva: $D_1 \sim D_1$. Como $D_1 - D_1 = 0 = div(c)$ para cualquier c función constante no cero, el divisor $D_1 - D_1$ es principal.
- Simétrica: $D_1 \sim D_2$ si y solo si $D_2 \sim D_1$. Para ver esto, vemos que si $D_1 - D_2 = div(f)$, entonces $D_2 - D_1 = -div(f) = div(1/f)$.
- Transitiva: Si $D_1 \sim D_2, D_2 \sim D_3$, entonces $D_1 \sim D_3$. Si $D_1 - D_2 = div(f)$ y $D_2 - D_3 = div(g)$, entonces $D_1 - D_3 = div(f) + div(g) = div(fg)$.

Hemos demostrado que $\sim$ es relación de equivalencia. □

Definición A.28. El grupo de clases de divisores (o grupo de Picard) de C es el grupo cociente $Pic(C) = Div(C)/\sim$. Llamamos $Pic_K(C)$ al subgrupo de $Pic(C)$ fijado por $G_{\overline{K}/K}$. Nótese que en general, este no es el cociente de $Div_K(C)$ por el subgrupo de divisores principales.

Proposición A.29. *Sea C una curva suave y $f \in \overline{K}(C)^*$. Entonces:*

a) $div(f) = 0$ si y solo si $f \in \overline{K}^*$.

b) $deg(div(f)) = 0$, es decir, los divisores principales forman un subgrupo de $Div^0(C)$.

Demostración. a) Si $div(f) = 0$, entonces f no tiene polos, por lo que la aplicación asociada $f : C \longrightarrow \mathbb{P}^1$ no es sobreyectiva. Por tanto, es constante, es decir, $f \in \overline{K}^*$. El inverso es inmediato: una función constante no 0 no tiene ceros ni polos.

b) Ver [2, II.6.10].

□

Definición A.30. La parte de grado 0 del grupo de clase de divisores de una curva suave C es $Pic^0(C) = Div^0(C)/\sim$. Llamamos $Pic^0_K(C)$ al subgrupo de $Pic^0(C)$ fijado por $G_{\overline{K}/K}$.

Finalmente introducimos un concepto que será importante cuando veamos el Teorema de Riemann-Roch:

Definición A.31. Un divisor $D = \sum n_P(P)$ es positivo, denotado $D \geq 0$, si $n_P \geq 0$ para todo $P \in C$.
Similarmente, decimos $D_1 \geq D_2$ para indicar que $D_1 - D_2$ es positivo.

Definición A.32. Sea $D \in Div(C)$. Asociamos a D el conjunto de funciones:

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^* : div(f) \geq -D\} \cup \{0\}.$$

Proposición A.33. *Sea $D \in Div(C)$.*

a) $\mathcal{L}(D)$ es un $\overline{K}$-espacio vectorial de dimensión finita. Denotamos su dimensión:

$$l(D) = dim_{\overline{K}}\mathcal{L}(D).$$

b) Si $deg(D) < 0$, entonces $\mathcal{L}(D) = \{0\}$ y $l(D) = 0$.

c) Si $D \sim D' \in Div(C)$ entonces $\mathcal{L}(D) \cong \mathcal{L}(D')$ y por tanto $l(D) = l(D')$.

Demostración. a) Ver [2, II.5.19].

b) Sea $f \in \mathcal{L}(D)$ con $f \neq 0$. Entonces:

$$deg(div(f)) = 0 \geq deg(-D) = -deg(D).$$

Por tanto $deg(D) \geq 0$. De esta forma, si $deg(D) < 0$ ninguna función $f \neq 0$ puede estar en $\mathcal{L}(D)$, así que en ese caso $\mathcal{L}(D) = \{0\}$.

c) Si $D \sim D'$, entonces $D = D' + div(g)$ para algún $g \in \overline{K}(C)$. Entonces la aplicación

$$\mathcal{L}(D) \longrightarrow \mathcal{L}(D'),\ f \longmapsto fg$$

es un isomorfismo.

□

La dimensión de este espacio vectorial tiene una estrecha relación con el concepto de género de una curva, como veremos en el Teorema de Riemann-Roch. No obstante, antes de poder enunciar el teorema, debemos introducir el concepto de divisor canónico, relacionado con los diferenciales de la curva.

A.4. Diferenciales

Definición A.34. Sea C una curva. El espacio de formas diferenciales en C, denotado Ω_C es el $\overline{K}$-espacio vectorial generado por símbolos de la forma dx para $x \in \overline{K}(C)$, sujetos a las relaciones usuales:

a) $d(x + y) = dx + dy$ para todo $x, y \in \overline{K}(C)$.

b) $d(xy) = xdy + ydx$ para todo $x, y \in \overline{K}(C)$.

c) $da = 0$ para todo $a \in \overline{K}$.

Proposición A.35. *Sea C una curva. Entonces Ω_C es un $\overline{K}(C)$-espacio vectorial 1-dimensional.*

Demostración. Ver [4, 27.A,B], [5, II.3.4] o [7, III § 4, Theorem 3]. □

Proposición A.36. *Sea C una curva, $P \in C$, $t \in \overline{K}(C)$ un uniformizador en P.*

a) Para todo $\omega \in \Omega_C$ existe un $g \in \overline{K}(C)$ (que depende de ω y de t) que satisface

$$\omega = g\ dt.$$

Denotamos g como ω/dt.

b) Sea $f \in \overline{K}(C)$ regular en P. Entonces df/dt es regular en P.

c) Sea $\omega \in \Omega_C, \omega \neq 0$. Entonces $ord_P(\omega/dt)$ solo depende de ω y de P, y no de la elección de t. Llamamos a este valor el orden de ω en P y lo denotamos $ord_P(\omega)$.

d) Sean $f, x \in \overline{K}(C)$ con $x(P) = 0$. Entonces

$$ord_P(f\ dx) = ord_P(f) + ord_P(x) - 1$$

e) Sea $\omega \in \Omega_C, \omega \neq 0$. Entonces solo un número finito de $P \in C$ cumple que $ord_P(\omega) \neq 0$.

Demostración. a) Ver [8, II.4.3a].

b) Ver [2, comentario siguiente a IV.2.1].

c) Sea t' otro uniformizador en P. Por b), tenemos que dt/dt' y dt'/dt son regulares en P, por tanto $ord_P(dt'/dt) = 0$. Entonces tenemos que

$$\omega = g\ dt = g(dt'/dt)dt.$$

lo que nos da el resultado buscado.

d) Escribimos $x = ut^n$ con $n = ord_P(x) \geq 1$ y por tanto $ord_P(u) = 0$. Entonces

$$dx = [nut^{n-1} + (du/dt)t^n]\ dt.$$

Por b) sabemos que du/dt es regular en P. Por tanto, si $n \neq 0$ el primer término es dominante, lo que nos da

$$ord_P(f\ dx) = ord_P(fnut^{n-1}\ dt) = ord_P(f) + n - 1.$$

e) Escoge una $x \in \overline{K}(C)$ tal que $\overline{K}(C)/\overline{K}(x)$ es separable y escribe $\omega = f\ dx$. Por [2, IV.2.2a], la aplicación $x : C \longrightarrow \mathbb{P}^1$ ramifica en un número finito de puntos de C. De esta forma, podemos restringirnos a puntos $P \in C$ que cumplen

$$f(P) \neq 0, (P) \neq \infty, x(P) \neq \infty$$

y en los que la aplicación x sea no-ramificada en P. Así, hemos descartado un número finito de puntos.

Las condiciones sobre x implican que $x - x(P)$ es uniformizador en P, por lo que

$$ord_P(\omega) = ord_P(f\ d(x - x(P))) = 0.$$

Por tanto $ord_P(\omega) = 0$ para todos estos puntos. Así, solo puede cumplirse $ord_P(\omega) \neq 0$ en un número finito de $P \in C$.

□

Definición A.37. Sea $\omega \in \Omega_C$. El divisor asociado a ω es

$$div(\omega) = \sum_{P \in C} ord_P(\omega)(P) \in Div(C)$$

El diferencial $\omega \in \Omega_C$ es regular (o holomorfo) si $div(\omega) \geq 0$, es decir, $ord_P(\omega) \geq 0$ para todo $P \in C$. Es no nulo si $div(\omega) \leq 0$.

Definición A.38. La clase de divisores canónicos es la imagen en $Pic(C)$ de $div(\omega)$ para cualquier $\omega \in \Omega_C$. Cualquier divisor en esta clase se llama divisor canónico.

La definición de divisor canónico tiene sentido: ya que Ω_C es un espacio vectorial unidimensional, tenemos que para cualquier par de diferenciales ω_1, ω_2 distintos de 0, hay una función $f \in \overline{K}(C)^*$ tal que $\omega_1 = f\omega_2$, y por tanto $div(\omega_1) = div(f) + div(\omega_2)$.

Ya hemos visto todo lo que necesitamos para enunciar el Teorema de Riemann-Roch.

A.5. El Teorema de Riemann-Roch

Teorema de Riemann-Roch. *Sea C una curva suave y K_C un divisor canónico en C. Entonces existe un entero $g \geq 0$, llamado el* ***género*** *de C, tal que para todo $D \in Div(C)$,*

$$l(D) - l(K_C - D) = deg(D) - g + 1.$$

Demostración. La demostración se sale del alcance de nuestro trabajo, pero véase [2, IV §1] o [3, Chapter 1]. □

Corolario A.39. *a)* $l(K_C) = g$.

b) $deg(K_C) = 2g - 2$.

c) Si $deg(D) > 2g - 2$ *entonces*

$$l(D) = deg(D) - g + 1.$$

Demostración. a) Inmediato a partir del Teorema de Riemann-Roch con $D = 0$. Nótese que $\mathcal{L}(0) = \overline{K}$ y por tanto $l(0) = 1$.

b) Inmediato a partir de *a)* y del Teorema de Riemann-Roch con $D = K_C$.

c) Por b) tenemos que $deg(K_C - D) < 0$, y por tanto $l(K_C - D) = 0$. A partir de esto, el Teorema de Riemann-Roch nos da el resultado.

□

Proposición A.40. *Sea C la curva*

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

donde $e_1, e_2, e_3 \in \overline{K}$ son distintos. Entonces:

a) La curva es suave y tiene un único punto en el infinito, que denotamos $\mathcal{O}$.

b) C tiene género 1.

c) No hay funciones en C con un solo polo simple.

Demostración. a) Dada una curva por una ecuación $f(x, y) = 0$, es suave si

$$\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0.$$

Por tanto ponemos la ecuación como $f(x, y) = y^2 - (x - e_1)(x - e_2)(x - e_3) = 0$. Vemos que $\frac{\partial f}{\partial y} = 0$ si y solo si $y = 0$. Por tanto $x = e_i$ para algún $i = 1, 2, 3$. Pero $\frac{\partial f}{\partial x} = -(x - e_2)(x - e_3) - (x - e_1)(x - e_3) - (x - e_1)(x - e_2) \neq 0$ para los tres casos. Por tanto C es suave en todo punto.

Homogenizando con $x = X/Z, y = Y/Z$ y tomando $Z = 0$ llegamos a que $X^3 = 0$. Por tanto hay un único punto en el infinito $\mathcal{O} = [0, 1, 0]$.

b) Tomamos $P_i = (e_i, 0)$. La función $x - e_i$, o en forma homogénea $\frac{X - e_i Z}{Z}$ tiene orden cero en todos los puntos distintos de P_i y $\mathcal{O}$. Como y es uniformizador en P_i y

$$x - e_i = y^2 \prod_{\substack{j=1,2,3 \\ j \neq i}} (x - e_j)^{-1},$$

tenemos que $ord_{P_i}(x - e_i) = 2$. Finalmente, para ver el orden en $\mathcal{O}$, homogeneizando la ecuación y dividiendo entre Y^3 vemos que

$$\frac{Z}{Y} = (\frac{X}{Y} - e_1\frac{Z}{Y})(\frac{X}{Y} - e_2\frac{Z}{Y})(\frac{X}{Y} - e_3\frac{Z}{Y}).$$

$\frac{Z}{Y}$ tiene un cero en $\mathcal{O}$ y $t = \frac{X}{Y}$ es uniformizador en $\mathcal{O}$. Por tanto,

$$\frac{Z}{Y} = t^3 f \text{ con } f \in \overline{K}[C]_{\mathcal{O}}, f(\mathcal{O}) \neq 0.$$

A partir de esto, llegamos a que

$$\frac{X - e_i Z}{Z} = \frac{\frac{X}{Z} - e_i\frac{Z}{Y}}{\frac{Z}{Y}} = \frac{t - e_i t^3 f}{t^3 f} = \frac{1}{t^2} g, \text{ con } g \in \overline{K}[C]_{\mathcal{O}}, g(\mathcal{O}) \neq 0.$$

Por tanto $ord_{\mathcal{O}}(x - e_i) = -2$. Juntando todo tenemos que

$$div(x - e_i) = 2(P_i) - 2(\mathcal{O}).$$

Vemos que el grado es efectivamente 0.

Para ver el divisor de y, primero observamos que el orden en puntos distintos de P_i y $\mathcal{O}$ es de nuevo 0. Además, y es uniformizador en P_i, así que $ord_{P_i}(y) = 1$. Solo queda ver el orden en $\mathcal{O}$. Vemos que $\frac{Y}{Z} = (\frac{Z}{Y})^{-1} = t^{-3}f^{-1} = t^{-3}h$, con $h \in \overline{K}[C]_{\mathcal{O}}, h(\mathcal{O}) \neq 0$. Por tanto, $ord_{\mathcal{O}}(y) = -3$, y tenemos:

$$div(y) = (P_1) + (P_2) + (P_3) - 3(\mathcal{O}).$$

Ahora pasamos a ver el divisor de dx. Para puntos $P = (\alpha, \beta) \neq P_i$, tenemos que $x - \alpha$ es uniformizador en P y como $dx = d(x - \alpha)$ tenemos que el orden de dx en P es 0. Para P_i, y es uniformizador, y a partir de $y^2 = (x - e_1)(x - e_2)(x - e_3) = f(x)$ obtenemos $2ydy = f'(x)dx$, y despejando $dx = 2\frac{ydy}{f'(x)}$. Como P_i no es singular, $f'(e_i) \neq 0$ y por tanto $ord_{P_i}(dx) = 1$. Finalmente, para ver el orden en $\mathcal{O}$ usamos que $dx = d(X/Z) = d(\frac{X/Y}{Z/Y}) = \frac{Z/Yd(X/Y) - X/Yd(Z/Y)}{(Z/Y)^2} = \frac{t^3(-2f - tf')dt}{t^6 f^2} = t^{-3}ldt$, con $l \in \overline{K}[C]_{\mathcal{O}}, l(\mathcal{O}) \neq 0$. Por tanto $ord_{\mathcal{O}}(dx) = -3$. Juntando todo, vemos que $div(dx) = (P_1) + (P_2) + (P_3) - 3(\mathcal{O})$.

Como $div(dx/y) = 0$, la clase del divisor canónico es trivial. Por tanto, podemos tomar $K_C = 0$, y aplicando Corolario A.39c vemos que $g = 1$.

c) Por Corolario A.39c vemos que si $deg(D) \geq 1$,

$$l(D) = deg(D).$$

Sea $P \in C$. Entonces $l((P)) = 1$. Pero $\mathcal{L}((P))$ claramente contiene las funciones constantes, que no tienen polos. Por tanto, no hay funciones en C con un solo polo simple.

□

Terminamos enunciando que si C y D están definidos sobre K, entonces $\mathcal{L}(D)$ también.

Proposición A.41. *Sea C/K curva suave y $D \in Div_K(C)$. Entonces $\mathcal{L}(D)$ tiene una base que consiste en funciones en $K(C)$.*

Demostración. Ver [8, II.5.8]. □

Con estos resultados, damos por terminada esta introducción. A partir de ahora nos centraremos en curvas elípticas y construiremos el grupo de puntos racionales de la curva, demostrando sus propiedades con ayuda de los resultados que hemos demostrado hasta ahora.

APÉNDICE B

Fórmulas explícitas de la ley de grupo

Suponemos que $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ es una curva elíptica dada por una ecuación de Weierstrass. Recordamos que la transformación $y \longmapsto \frac{1}{2}(y - a_1x - a_3)$ pone la ecuación en la forma $y^2 = 4x^3 + b_2x^2 + b_4x + b_6$. Los coeficientes de esta transformación son:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

La transformación adicional $(x, y) \longmapsto (\frac{x-3b_2}{36}, \frac{y}{108})$ pone la ecuación como $y^2 = x^3 + Ax + B$. Los coeficientes de esta ecuación son

$$\begin{aligned} A &= 27(24b_4 - b_2^2), \\ B &= 54(b_2^3 - 36b_2b_4 + 216b_6). \end{aligned}$$

Dada la ecuación en la forma más general. Entonces:

- Sea $P = (x, y)$. El punto $-P$ es el otro punto de intersección en la recta vertical que pasa por P. Utilizando esto, obtenemos que $-P = (x, -y - a_1x - a_3)$.
- Sean $P_1 = (x, y_1), P_2 = (x, y_2)$ con $y_1+y_2+a_1x+a_3 = 0$. Utilizando la propiedad anterior, vemos que $P_1 = -P_2$. Entonces $P_1 + P_2 = \mathcal{O}$.
- Sean $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = (x_3, y_3)$ con $P_1 + P_2 = P_3$. Empezamos viendo la ecuación de la recta que los une $y = \lambda x + \nu$. De momento, suponemos que $P_1 \neq \pm P_2$. Entonces $\lambda = \frac{y_2-y_1}{x_2-x_1}$ es la pendiente de esta recta. Para obtener ν, sustituimos el punto $P_1 = (x_1, y_1)$ en la ecuación de la recta, obteniendo $\nu = \frac{y_1x_2-y_2x_1}{x_2-x_1}$.

  Finalmente, para obtener x_3 sustituimos $y = \lambda x+\nu$ en la ecuación de la curva y despejamos para obtener $x^3+(a_2-\lambda^2-a_1\lambda)x^2+(a_4-2\lambda\nu-a_1\nu-a_3\lambda)x+a_6-$

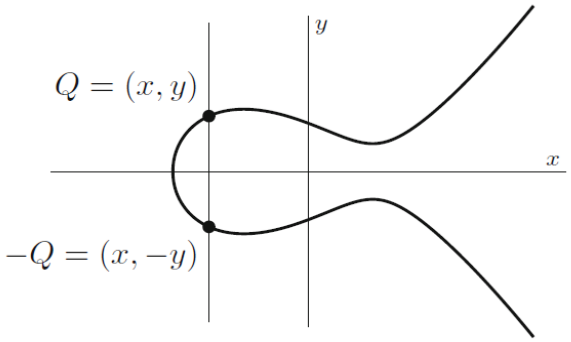

Figura B.1: El inverso de un punto

$\nu^2 - a_3\lambda\nu = 0$. Tenemos que las tres raíces de este polinomio son las coordenadas x de los tres puntos de intersección x_1, x_2, x_3. Igualando los coefientes en x^2 de este polinomio con los de $(x-x_1)(x-x_2)(x-x_3)$ llegamos a que $x_1+x_2+x_3 = \lambda^2 - a_1\lambda - a_2$. Despejando x_3 obtenemos:

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2.$$

Sustituyendo en $y = \lambda x + \nu$ obtenemos que la coordenada y de $P_1 * P_2$ es $(\lambda + a_1)x_3 + \nu + a_3$. Como $P_1 + P_2 = -(P_1 * P_2)$, obtenemos que

$$y_3 = -((\lambda + a_1)x_3 + \nu + a_3).$$

Ahora vemos el caso $P_1 = P_2$. En este caso, la recta en la ley de grupo es la recta tangente, cuya pendiente es $\lambda = \left.\frac{\partial y}{\partial x}\right|_{P_1} = \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}$. Entonces $\nu = \frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}$. A partir de las coordenadas de la recta, obtenemos x_3 e y_3 de la misma forma.

Juntando todo tenemos que:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},\ \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \text{ si } x_1 \neq x_2,$$
$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3},\ \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \text{ si } x_1 = x_2,$$

y a partir de eso,

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

Como casos particulares especiales, distinguimos:

- Si $P_1 \neq \pm P_2$, entonces

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2.$$

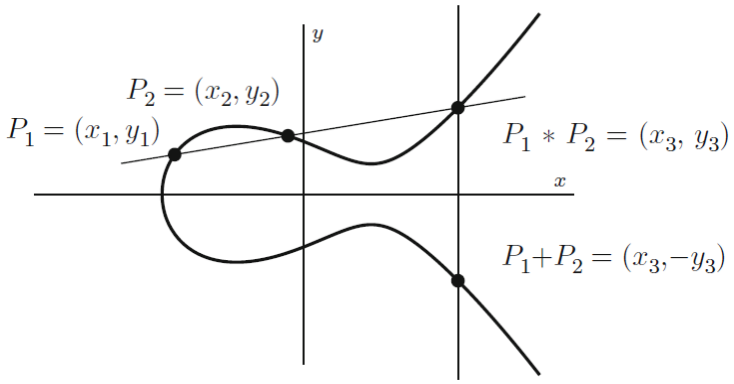

Figura B.2: Ley de grupo explícita. La recta es $y = \lambda x + \nu$.

Este caso es en realidad la coordenada x del caso $P_1 + P_2 = P_3 \neq \mathcal{O}$ con $x_1 \neq x_2$. No obstante, es un caso particular que conviene tener accesible debido a su utilidad en casos comunes.

- La fórmula de duplicación (para $P = (x, y)$):

$$x(2P) = \frac{x^4 + b_4 x^2 - 2b_6 x - b_8}{4x^3 + b_2 x^2 + 2b_4 x + b_6},$$

donde los coeficientes están dados al principio de este Apéndice.

Este resultado nos permite expresar la coordenada x de $2P$ en función de la coordenada x de P. Este resultado tiene multitud de aplicaciones, por ejemplo en computación de puntos de orden finito.

APÉNDICE C
Demostraciones del capítulo 2

En este apéndice se incluyen las demostraciones del capítulo 2 más largas. Para simplificar la notación, denotamos $\omega_3 = \omega_1 + \omega_2$.

Teorema 2.8. *Dado un retículo L, se tiene:*

a) La suma que define $\wp(z)$ converge absolutamente y uniformemente en conjuntos compactos sin elementos de L.

b) $\wp$ es meromorfa en $\mathbb{C}$ y tiene un polo doble en cada $\omega \in L$.

c) $\wp$ es par.

d) $\wp$ es doblemente periódica (en L).

e) Toda función doblemente periódica (en L) es una función racional de $\wp$ y de $\wp'$, la derivada de $\wp$.

Para la demostración necesitaremos un lema:

Lema C.1. *Si $k > 2$ entonces*

$$\sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{|\omega|^k}$$

Demostración del Lema. Ver [10, p. 263]. □

Demostración del Teorema 2.8. a) Dado un conjunto compacto C y $M = \text{máx}\{\|z| : z \in C\}$. Si $z \in C$ y $|\omega| \geq 2M$, entonces $|z - \omega| \geq |\omega|/2$ y $|2\omega - z| \leq 5|\omega|/2$, así que

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{(z-\omega)^2 \omega^2} \right| \leq \frac{M(5|\omega|/2}{|\omega|^4/4} = \frac{10M}{|\omega|^3}.$$

El lema nos prueba que esto converge.

La suma de los términos con $|\omega| \geq 2M$ converge absolutamente y uniformemente para $z \in C$. Como solo hemos omitido una cantidad finita de términos, se cumple para todo C.

b) $\wp(z)$ es analítica para $z \notin L$, ya que es un límite uniforme de funciones analíticas. Si $z \in L$, la suma de los términos $\omega \neq z$ es analítica cerca de z, así que el término $1/(z-\omega)^2$ hace que $\wp$ tenga un polo doble en z.

c) Es fácil ver que $\omega \in L \Leftrightarrow -\omega \in L$. Si tomamos la suma de $\wp(-z)$ sobre $-\omega$, vemos que la suma para $\wp(z)$ es igual a la suma para $\wp(-z)$. Por tanto $\wp(z) = \wp(-z)$, es decir, $\wp$ es una función par.

d) Diferenciando $\wp(z)$ término por término obtenemos

$$\wp'(z) = -2\sum_{\omega \in L} \frac{1}{(z-\omega)^3}$$

Esta serie converge absolutamente si $z \notin L$, y cambiar z por $z+\omega$ desplaza los términos de la serie. Por tanto $\wp'(z+\omega) = \wp'(z)$. Esto implica que existe una constante c_ω tal que $\wp(z+\omega) - \wp(z) = c_\omega$. Escogiendo $z = \omega/2$ tenemos que $c_\omega = \wp(-\omega/2) - \wp(\omega/2)$ que por el punto anterior sabemos que es 0. Por tanto, $\wp(z+\omega) = \wp(z)$.

e) Sea $f(z)$ una función doble periódica. Como $f(z) = \frac{f(z)+f(-z)}{2} + \frac{f(z)-f(-z)}{2}$ es suma de una función par y otra impar, basta probar el resultado para funciones pares e impares. Como $\wp$ es par, $\wp'$ es impar, y por tanto si $f(z)$ es impar tenemos que $f(z)/\wp'(z)$ es par. Por tanto basta probarlo para funciones pares.

Si $f = 0$, ya está. Ahora sea $f \neq 0$. Si fuera necesario, cambiamos f por $(af+b)/(cf+d)$ con a, b, c, d tales que $ad - bc \neq 0$ para que $f(z)$ no tenga ni ceros ni polos en los z tales que $2z \in L$. Si probamos que esto es una función racional de f, podemos despejar f y obtener lo que buscamos.

Como f es par y doble periódica, $f(\omega_3 - z) = f(z)$, así que $ord_{\omega_3 - w}(f) = ord_w(f)$. Por tanto, los elementos en los que f tiene un cero o polo se pueden poner en pares $(w, \omega_3 - w)$ en los que los elementos de cada par son distintos (si $w = x\omega_i$ con $0 < x < 1, i = 1$ ó 2, en su lugar tomamos el par $(x\omega_i, (1-x)\omega_i)$).

Para un w fijo, la función $\wp(z) - \wp(w)$ tiene ceros en $z = w$ y $z = \omega_3 - w$, y como solo hay un polo doble en F, son ceros simples y no hay más ceros en F. Por tanto la función

$$h(z) = \prod_{(w, \omega_3 - w)} (\wp(z) - \wp(w))^{ord_w(f)}$$

tiene ceros y polos del mismo orden que f en w, y ceros del orden de f en w en $\omega_3 - w$. Como la suma de los ordenes de f en los $z \in L$ se anula, los polos en los factores del producto se cancelan. Por tanto $f(z)/h(z)$ no tiene ceros ni polos en F, así que es constante. Como $h(z)$ es una función racional de $\wp(z)$, también lo es $f(z)$.

□

Teorema 2.11. *Sea $\wp(z)$ la función $\wp$ de Weierstrass para un retículo L. Entonces*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Demostración del Teorema 2.11. Por Proposición 2.10 sabemos que

$$\wp(z) = z^{-2} + 3G_4 z^2 + 5G_6 z^4 + ...$$
$$\wp'(z) = -2z^{-3} + 6G_4 z + 20G_6 z^3 + ...$$

Elevando esto al cubo y al cuadrado respectivamente obtenemos:

- El primer término al cubo y cuadrado respectivamente nos da z^{-6} y $4z^{-6}$.
- Multiplicando dos veces el primer término de $\wp(z)^3$ por el segundo y tercer término, obtenemos $3G_4 z^{-2}$ y $5G_6$. Ya que esta combinación está 3 veces, multiplicamos el coeficiente por 3.
- Multiplicando el primer término de $\wp'(z)^2$ por el segundo y tercer término, obtenemos $-12G_4 z^{-2}$ y $-40G_6$. La combinación está 2 veces, así que multiplicamos el coeficiente por 2.

Poniendo todo esto junto, tenemos

$$\wp(z)^3 = z^{-6} + 9G_4 z^{-2} + 15G_6 + ...$$
$$\wp'(z)^2 = 4z^{-6} - 24G_4 z^{-2} - 80G_6 + ...$$

Por tanto,

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 = c_1 z + c_2 z^2 + ...$$

es una serie de potencias sin término constante ni potencias negativas de z. Los únicos polos posibles de f son los polos de $\wp$ y de $\wp'$, es decir, los elementos de L. Pero f es doblemente periódica y no tiene polo en 0, así que por definición no tiene polos en los elementos de L. Por tanto, no tiene polos, y por 2.6a, es constante. Ya que no tiene término constante, $f(0) = 0$ y por tanto $f = 0$. □

Teorema 2.13. *Sea L un retículo y $E : y^2 = 4x^3 - g_2 x - g_3$ con $\Delta = g_2^3 - 27g_3^2 \neq 0$. Entonces la función*

$$\begin{aligned} \Phi : \mathbb{C}/L &\longrightarrow E(\mathbb{C}) \\ z &\longmapsto (\wp(z), \wp'(z)) \\ 0 &\longmapsto \infty \end{aligned}$$

es un isomorfismo de grupos.

Demostración del Teorema 2.13. Vamos a demostrar que Φ es isomorfismo. Para ver que es homomorfismo de grupos, ver [10, 9.10].

- Sobreyectividad: sea $(x, y) \in E(\mathbb{C})$. La función $\wp(z) - x$ tiene un polo doble, así que tiene ceros. Por tanto existe $z \in \mathbb{C}$ tal que $\wp(z) = x$. Por Teorema 2.11 tenemos que $y^2 = \wp'(z)^2$, y por tanto $\wp'(z) = \pm y$. Si $\wp'(z) = y$ ya está. Si $\wp'(z) = -y$ entonces $\wp'(-z) = y$, y como $\wp(-z) = x$ tenemos el punto buscado.

- Inyectividad: sean z_1, z_2 con $\wp(z_1) = \wp(z_2)$ y $\wp'(z_1) = \wp'(z_2)$. Si z_1 es un polo de $\wp$, tiene que cumplirse $z_1 \in L$ y como $\wp(z_1) = \wp(z_2)$, también $z_2 \in L$. Por tanto $z_1 \equiv z_2 \pmod{L}$. Ahora asumimos que z_1 no es polo de $\wp$, así que $z_1 \notin L$. La función $h(z) = \wp(z) - \wp(z_1)$ tiene un polo doble en $z = 0$ como único polo, así que tiene exactamente dos ceros. Suponemos que $z_1 = \omega_i/2$ para algún i. Hemos visto que $\wp'(\omega_i/2) = 0$, por lo que z_i es raíz doble de $h(z)$ y por tanto no hay más raíces. Por tanto debe ser $z_2 = z_1$. Por último, si z_1 no es $\omega_i/2$ para algún i, vemos que $h(z_1) = h(-z_1) = 0$, y como $z_1 \not\equiv -z_1 \pmod{L}$, el único otro cero $\pmod{L}$ de $h(z)$ es $-z_1$ y tenemos que $z_2 \equiv -z_1$. Pero $y = \wp'(z_2) = \wp'(-z_1) = -\wp'(z_1) = -y$, así que $\wp'(z_1) = y = 0$. $\wp'(z)$ tiene un polo triple, así que tiene tres ceros en F, y sabemos que son los puntos $\omega_i/2$. Pero hemos supuesto que z_1 no es $\omega_i/2$. Contradicción. Por tanto debe ser $z_1 = z_2$.

□

Proposición 2.16. *Sea $\tau \in \mathcal{H}$ y $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Entonces*

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau).$$

Demostración de la Proposición 2.16. Empezamos viendo G_k:

$$G_k\left(\frac{a\tau+b}{c\tau+d}\right) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m\frac{a\tau+b}{c\tau+d} + n)^k} = (c\tau+d)^k \sum_{(m,n)\neq(0,0)} \frac{1}{(m(a\tau+b) + n(c\tau+d))^k}$$
$$= (c\tau+d)^k \sum_{(m,n)\neq(0,0)} \frac{1}{((ma+nc)\tau + (mb+nd))^k}$$

Como la matriz tiene determinante 1, tenemos que su inversa es $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ y por tanto si $(m', n') = (m, n)\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, entonces $(m, n) = (m', n')\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Por tanto, hay una correspondencia 1 a 1 entre los pares (m, n) y los pares $(m', n') = (ma+nc, mb+nd)$. Por tanto tenemos que

$$G_k\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k \sum_{(m',n')\neq(0,0)} \frac{1}{(m'\tau+n')^k} = (c\tau+d)^k G_k(\tau).$$

De la definición de g_2 y g_3 vemos que

$$g_2\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^4 g_2(\tau),\ g_3\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^6 g_3(\tau).$$

Cuando sustituimos las expresiones en la definición de j, todos los factores $(c\tau + d)$ se cancelan, así que queda $j\left(\frac{a\tau+b}{c\tau+d}\right) = j(\tau)$. □

Corolario 2.21. *Si $z \in \mathbb{C}$, entonces existe un único $\tau \in \mathcal{F}$ tal que $j(\tau) = z$.*

Demostración del Corolario 2.21. Empezamos calculando $j(\rho)$ y $j(i)$. Como $\rho^2 = -1-\rho$, vemos que $\rho L_\rho \subset L_\rho$ y por tanto $L_\rho = \rho^3 L_\rho \subset \rho^2 L_\rho \subset \rho L_\rho \subset L_\rho$, así que $\rho L_\rho = L_\rho$. Por tanto $g_2(L_\rho) = g_2(\rho L_\rho) = \rho^{-4} g_2(L_\rho) = \rho^{-1} g_2(L_\rho)$. Como $\rho \neq 1$, $g_2(\rho) = g_2(L_\rho) = 0$. Por tanto, $j(\rho) = 0$.

Similarmente, $iL_i = L_i$ y $g_3(iL_i) = i^{-6} g_3(L_i) = -g_3(L_i)$, así que $g_3(i) = g_3(L_i) = 0$ y por tanto $j(i) = 1728$.

Ahora consideramos otros valores de τ. Sea $h(\tau) = j(\tau) - z$. h tiene un polo de orden 1 en $i\infty$ como único polo. Por tanto tenemos que

$$\frac{1}{3} ord_\rho(h) + \frac{1}{2} ord_i(h) + \sum_{z \neq i, i\infty, \rho} ord_z(h) = 1.$$

Si $z \neq 0, 1728$, entonces h tiene orden 0 en ρ y en i. Por tanto, tiene un único cero en $\mathcal{F}$, así que $j(\tau) = z$ tiene solución única en $\mathcal{F}$. Si $z = 1728$, tenemos que $\frac{1}{2} ord_i(h) > 0$ y es un número entero. Por tanto el orden debe ser 0 para todo $z \neq \rho, i$ (ya que en otro caso la suma sería mayor a 1). Como la única combinación $m/3 + n/2 = 1$ con $m \geq 0, n > 0$ es $m = 0$, tenemos que h tiene un doble cero en i y no más ceros. Esto cubre el caso $z = 1728$. Similarmente, el caso $z = 0$ queda cubierto porque $j(\tau)$ tiene un cero triple en ρ como único cero en $\mathcal{F}$. □

Teorema 2.23. *Sea $E : y^2 = 4x^3 - Ax - B$ una curva elíptica sobre $\mathbb{C}$. Entonces existe un retículo L tal que $g_2(L) = A$ y $g_3(L) = B$.*

Por Teorema 2.13, hay un isomorfismo de grupos entre $\mathbb{C}/L$ y $E(\mathbb{C})$.

Demostración del Teorema 2.23. Sea $j = 1728 \frac{A^3}{A^3 - 27B^2}$. Por Corolario 2.21 existe un retículo $L = \mathbb{Z}\tau + \mathbb{Z}$ tal que $j(\tau) = j(L) = j$.

Primero asumimos que $g_2(L) \neq 0$. Entonces $j = j(L) \neq 0$, por lo que $A \neq 0$. Escogemos $\lambda \in \mathbb{C}^*$ tal que $g_2(\lambda L) = \lambda^{-4} g_2(L) = A$. Como $j = j(L)$, tenemos que $g_3(\lambda L)^2 = B^2$, así que $g_3(\lambda L) = \pm B$. Si es B, ya está. Si es $-B$, vemos que $g_3(i\lambda L) = i^6 g_3(\lambda L) = B$ y $g_2(i\lambda L) = i^4 g_2(\lambda L) = A$. Por tanto, λL o $i\lambda L$ es el retículo buscado.

Ahora suponemos $g_2(L) = 0$. Entonces $A = 0$, y como $A^3 - 27B^2 \neq 0$ tenemos que $B \neq 0$. Como $g_2(L)^3 - 27 g_3(L)^2 \neq 0$, también tenemos que $g_3(L) \neq 0$. Escogemos $\mu \in \mathbb{C}^*$ tal que $g_3(\mu L) = \mu^6 g_3(L) = B$. Como $g_2(\mu L) = \mu^4 g_2(L) = 0 = A$, μL es el retículo buscado. □

Bibliografía

[1] L. Ahlfors: Complex Analysis. An introduction to the theory of analytic functions of one complex variable. *McGraw-Hill, Inc. Third Edition.* (1979).

[2] R. Hartshorne: Algebraic geometry. *Springer-Verlag, New York. Graduate Texts in Mathematics, No. 52.* (1977).

[3] S. Lang: Introduction to algebraic and abelian functions, volume 89 of Graduate Texts in Mathematics. *Springer-Verlag, New York, second edition* (1982).

[4] H. Matsumura: Commutative algebra, volume 56 of Mathematics Lecture Note Series. *Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition,* (1980).

[5] A. Robert: Elliptic curves. *Springer-Verlag, Berlin. Notes from postgraduate lectures given in Lausanne 1971/72, Lecture Notes in Mathematics, Vol. 326.* (1973).

[6] J.-P. Serre: A course in arithmetic. *Springer-Verlag, New York. Translated from the French, Graduate Texts in Mathematics, No. 7.* (1973).

[7] I. R. Shafarevich: Basic algebraic geometry. *Springer-Verlag, Berlin, study edition,* (1977). Traducido del ruso por K. A. Hirsch, Revised printing of Grundlehren der mathematischen Wissenschaften, Vol. 213 (1974).

[8] J.H. Silverman: The arithmethic of elliptic curves. *Second Edition, Springer* (2009).

[9] J.H. Silverman, J.T. Tate: Rational points on elliptic curves. *Second Edition UTM Springer* (2015).

[10] L. C. Washington: Elliptic curves, number theory and cryptography. *Second Edition* (2008).