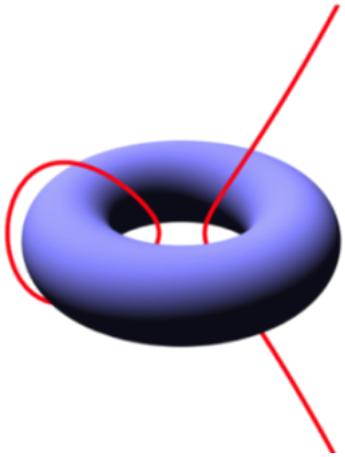
Curvas elípticas

Gonzalo Rodriguez, Leonardo Montoya, Melanie Vargas

Departamento de Matemática, Universidad Técnica Federico Santa María



Resumen

El objetivo de este trabajo es estudiar el concepto de curvas elípticas en el contexto de la geometría algebraica. Para ello será necesario introducir la noción de divisores sobre curvas algebraicas con el objetivo de poder hablar del grupo de Picard, se verá que gracias a una biyección entre este grupo y la curva, podremos definir naturalmente una estructura de grupo para la curva elíptica. Recordaremos además algunas herramientas del análisis complejo para estudiar algunas aplicaciones de curvas elípticas sobre el cuerpo $\mathbb{C}$, en primer lugar la función $\wp$ de Weierstrass que nos permite formar una biyección entre un toro complejo la curva elíptica. En segundo lugar, introducimos las funciones theta y su relación con las curvas elípticas, la cual tiene una gran variedad de aplicaciones a otras áreas de la matemática.

Índice

1. Introducción

La teoría de las ecuaciones diofánticas es esa rama de la teoría de números que se ocupa de la solución de ecuaciones polinomiales en números enteros o números racionales. Existen ecuaciones diofánticas que no son tan fáciles de manipular con métodos elementales, por lo que se suele recurrir a la teoría de curvas elípticas para poder resolverlas.
Una ecuación diofántica bastante conocida vendría siendo el Último Teorema de Fermat, el cual nos dice que no existen x, y, z enteros tales que para $n \geq 3$,

$$x^n + y^n = z^n.$$

Por muchos tiempo se intentó demostrar este teorema con métodos elementales, sin embargo, luego de más de 300 años pudo ser demostrado utilizando curvas elípticas.
Las curvas elípticas sobre cuerpos finitos se usan en algunas aplicaciones en criptografía y también para factorización de números enteros.
Veremos que se puede asociar una ley de grupo para dichas curvas utilizando la teoría de geometría algebraica para obtener cálculos explícitos para la operación de suma. También daremos un enfoque al análisis complejo y unas aplicaciones que pueden servir para otras ramas de la matemática.

Notación

A lo largo de este trabajo, denotaremos por k un cuerpo base fijo.

Entendemos un número complejo como un elemento del conjunto

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}.$$

El símbolo $\mathbb{C}$ denota el cuerpo de números complejos.

Dado $n \in \mathbb{N}$, denotamos el $n-$espacio proyectivo sobre k por $\mathbb{P}^n_k$ o simplemente $\mathbb{P}^n$, el conjunto de todos los subespacios lineales unidimensionales del espacio vectorial k^{n+1}.
Denotamos al conjunto $S(X) = k[x_0, \ldots, x_n]/I(X)$ donde I es el ideal construido en el curso.

2. Preliminares

2.1. Divisores en curvas

Definición 2.1. Sea X una curva suave, proyectiva e irreducible.

1. Un **divisor** en X es una combinación lineal finita $k_1a_1 + \cdots + k_na_n$ de distintos puntos $a_1, \ldots, a_n \in X$ con $k_1, \ldots, k_n \in \mathbb{Z}$ para algún $n \in \mathbb{N}$. Los divisores en X forman un grupo abeliano bajo la suma de coeficientes. Denotamos a los divisores por $\mathrm{Div}X$.

2. Un divisor $D = k_1a_1 + \cdots + k_na_n$ es llamado **efectivo**, denotado por $D \geq 0$, si $k_i \geq 0$ para cada $i = 1, \ldots, n$. Si D_1, D_2 son dos divisores tales que $D_2 - D_1$ es efectivo, escribimos que $D_2 \geq D_1$ o $D_1 \leq D_2$. En otras palabras, tenemos que $D_2 \geq D_1$ si y sólo si cada coeficiente de cada punto en D_2 es mayor o igual a los coeficientes de estos puntos en D_1.

3. El **grado** de un divisor $D = k_1a_1 + \cdots + k_na_n$ es el número $\deg D := k_1 + \cdots + k_n \in \mathbb{Z}$. El grado forma un homomorfismo deg:$\mathrm{Div}X \to \mathbb{Z}$. Su kernel se denota como

$$\mathrm{Div}^0X = \{D \in \mathrm{Div}X : \deg D = 0\}.$$

Construcción de divisiores de polinomios: Sea $X \subset \mathbb{P}^n$ una curva suave e irreducible.

1. Para un polinomio no nulo $f \in S(X)$, el **divisor** de f se define como

$$\mathrm{div}f := \sum_{a \in V_X(f)} \mathrm{mult}_a(f) \cdot a \in \mathrm{Div}X,$$

donde $V_X(f)$ denota los ceros de f en X. En otras palabras, el divisor $\mathrm{div}f$ contiene los datos de los ceros de f junto a sus multiplicidades. Por el Teorema de Bézout, su grado es $\deg(\mathrm{div}f) = \deg X \cdot \deg f$.

2. Si $n = 2$ e $Y \subset \mathbb{P}^2$ es otra curva que no contiene a X, el **divisor de intersección** de X e Y es

$$X \cdot Y := \sum_{a \in X \cap Y} \mathrm{mult}_a(X, Y) \cdot a \in \mathrm{Div}X.$$

Lema 2.1. *Sea X una curva suave, proyectiva e irreducible, y sean $f, g \in S(X)$ polinomios no nulos. Entonces*

$$\mathrm{mult}_a(fg) = \mathrm{mult}_a(f) + \mathrm{mult}_a(g)$$

para todo $a \in X$. En particlar, tenemos que $div(fg) = divf + divg \in DivX$.

Construcción de divisores de funciones racionales: Sea X una curva suave, proyectiva e irreducible, y sea $\varphi \in k(X)^*$ una función racional no nula. Podemos escribir $\varphi = \frac{g}{f}$ dos polinomios homogéneos f y g del mismo grado.

1. Definimos la multiplicidad de φ en un punto $a \in X$ como

$$\mathrm{mult}_a(\varphi) := \mathrm{mult}_a(g) - \mathrm{mult}_a(f) \in \mathbb{Z}.$$

2. Análogamente, por la primera construcción, definimos el divisor de φ como

$$\mathrm{div}\varphi := \sum_{a \in V_X(f) \cap V_X(g)} \mathrm{mult}_a(\varphi) \cdot a = \mathrm{div}g - \mathrm{div}f.$$

Observemos que el Lema 2.1 implica que $\text{mult}_a(\varphi_1\varphi_2) = \text{mult}_a(\varphi_1) + \text{mult}_a(\varphi_2)$ para todo $a \in X$ para φ_1, φ_2 funciones racionales. Además se tiene que $\text{div}(\varphi_1\varphi_2) = \text{div}\varphi_1 + \text{div}\varphi_2$, es decir, el mapeo $\text{div} : k(X)^* \to \text{Div}X$ es un homomorfismo de grupos.
Observemos además que cualquier funcion racional en X es de la forma $\varphi = \frac{g}{f}$ para dos polinomios homogéneos del mismo grado, por la primera construcción, este divisor tiene grado cero:

$$\deg(\text{div}\varphi) = \deg(\text{div}g - \text{div}f) = \deg\text{div}g - \deg\text{div}f = \deg X \cdot \deg g - \deg X \cdot \deg f = 0.$$

Por lo tanto el homomorfismo de la observación anterior puede ser visto como un morfismo $\text{div} : k(X)^* \to \text{Div}^0 X$.

Definición 2.2. Sea X una curva suave, proyectiva e irreducible.

1. Un divisor en X es llamado **principal** si es divisor de una función racional. Denotamos por $\text{Prin}X$ al conjunto de todos los divisores principales. Notemos que $\text{Prin}X$ es la imagen de un divisor por $\text{div} : k(X)^* \to \text{Div}^0 X$ y por lo tanto es subgrupo de $\text{Div}^0 X$ y $\text{Div}X$.

2. El cociente
$$\text{Pic}X := \text{Div}X/\text{Prin}X$$
es llamado el **grupo de Picard** o **grupo de clases divisorias** en X. Restrictos al grado cero, podemos definir $\text{Pic}^0 X := \text{Div}^0 X/\text{Prin}X$. Por abuso de notación, un divisor y su clase en $\text{Pic}X$ lo denotaremos por el mismo símbolo.

Observemos que los grupos $\text{Pic}X$ y $\text{Pic}^0 X$ llevan la misma información en X, como siempre tenemos
$$\text{Pic}X/\text{Pic}^0 X \cong \text{Div}X/\text{Div}^0 X \cong \mathbb{Z}.$$
Curvas cúbicas: Sean a, b dos puntos de $X \subset \mathbb{P}^2$ curva cúbica y suave, no necesariamente iguales. Existe una única recta $L \subset \mathbb{P}^2$ tal que $a + b \leq L \cdot X$ como divisores en X, llamada la recta que pasa por a y b si los puntos son distintos, y la recta tangente de X en $a = b$ en otro caso. Pero $L \cdot X$ es un divisor efectivo de grado 3 en X, y por lo tanto existe un único punto $c \in X$ con $L \cdot X = a + b + c$. En lo siguiente, denotaremos a c por $\psi(a, b)$.
Geométricamente, para $a, b \in X$, el punto $\psi(a, b)$ es el tercer punto de intersección de X con la recta que pasa por a y b. De hecho, uno puede mostrar que el mapeo $\psi : X \times X \to X$, $(a, b) \mapsto \psi(a, b)$ es un morfismo.

Proposición 2.1. *Sea $X \subset \mathbb{P}^2$ una curva cúbica suave. Entonces para todo $a, b \in X$ distintos, tenemos que $a - b \neq 0 \in Pic^0 X$, es decir, no existe una función racional no nula φ en X tal que $div\varphi = a - b$.*

En particular, la proposición 2.1 implica que $\text{Pic}^0 X \neq \{0\}$ para cada superficie cúbica $X \subset \mathbb{P}^2$.

Demostración. Supongamos por contradicción que el enunciado de la proposición es falso. Luego, existe un entero positivo d y polinomios homogéneos $f, g \in S(X)$ de grado d tales que se cumple:

(a) Existen puntos $a_1, \ldots, a_{3d-1}$ y $a \neq b$ en X tal que
$$\text{div}g = a_1 + \cdots + a_{3d-1} \quad \text{y} \quad \text{div}f = a_1 + \cdots + a_{3d-1} + b.$$
(Por lo tanto $\text{div}\varphi = a - b$ para $\varphi = \frac{g}{f}$).

(b) Entre los valores $a_1, \ldots, a_{3d-1}$ hay al menos $2d$ puntos distintos.

Tomamos d minimal con estas dos propiedades.
Si $d = 1$, entonces $\mathrm{div}g = a_i + a_2 + a$ y $\mathrm{div}f = a_1 + a_2 + b$, luego se tiene que $a = b = \psi(a_1, a_2)$, en contradicción a nuestra suposición. Por lo tanto podemos suponer que $d > 1$. Volvamos a considerar los puntos $a_1, \ldots, a_{3d-1}$ tal que $a_2 \neq a_3$, y tal que $a_1 = a_2$ si hay puntos iguales entre los a_i.
Ahora consideramos las combinaciones lineales $\lambda f + \mu g$ para $\lambda, \mu \in k$, no ambos cero. Como los polinomios f y g tienen divisores diferentes, son linealmente independientes en $S(X)$, y por lo tanto $\lambda f + \mu g$ no se anula en X. Luego, se tiene que $a_1 + \cdots + a_{3d-1} \leq \mathrm{div}(\lambda f + \mu g)$ para todo λ y μ, y para cualquier $c \in X$ existen λ y μ con $a_1 + \cdots + a_{3d-1} \leq \mathrm{div}(\lambda f + \mu g)$. Por supuesto, por Teorema de Bézout, se tiene que $\mathrm{div}(\lambda f + \mu g) = a_1 + \cdots + a_{3d-1} + c$.
Escogemos $a = \psi(a_1, a_2)$ y $b = \psi(a_1, a_3)$. Entonces

$$\mathrm{div}g = (a_1 + a_2 + \psi(a_1, a_2)) + a_3 + a_4 + \cdots + a_{3d-1}$$

y

$$\mathrm{div}f = (a_1 + a_3 + \psi(a_1, a_3)) + a_2 + a_4 + \cdots + a_{3d-1}.$$

Pero $a_1 + a_2 + \psi(a_1, a_2)$ y $a_1 + a_3 + \psi(a_1, a_3)$ son divisores de polinomios lineales homogéneos k y l, respectivamente, existen polinomios lineales homogéneos f', g' de grado $d - 1$ con $g = kg'$ y $f = lf'$, y así

$$\mathrm{div}g' = a_4 + \cdots + a_{3d-1} + a_3 \ \mathbf{y} \ \mathrm{div}f' = a_4 + \cdots + a_{3d-1} + a_2.$$

Notemos que estos nuevos polinomios f' y g' satisfacen la primera propiedad para d reemplazado por $d-1$, ya que $a_3 \neq a_2$ por hipótesis. Más aún, f' y g' satisfacen la segunda propiedad porque, si hay puntos iguales entre los a_i, entonces al volver a etiquetarr estos puntos, sólo hay dos puntos distintos entre a_1, a_2, a_3 y por lo que todavía debe haber al menos $2d - 2$ puntos distintos entre $a_4, \ldots, a_{3d-1}$.
Esto contradice la minimalidad de d, y por lo tanto se prueba la proposición. □

2.2. Funciones holomorfas y meromorfas

Definición 2.3. Sea $U \subset \mathbb{C}$ un abierto en la topología usual. Una función $f : U \to \mathbb{C}$ se dice *holomorfa* si es diferenciable, en el sentido complejo, para todo punto $z_0 \in U$, esto es, el límite

$$f'(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

existe para todo $z_0 \in U$.
Una función $f : U \to \mathbb{C} \cup \{\infty\}$ se dice *meromorfa* si es que es holomorfa en todo $z_0 \in \mathbb{C}$ excepto en algunas singularidades aisladas, las cuáles son polos, esto es, si para todo $z_0 \in U$ existe un número $n \in \mathbb{Z}$ y una función holomorfa $\tilde{f}$, definida en una vecindad $V \subset U$ de z_0, tal que

$$f(z) = (z - z_0)^n \tilde{f}(z)$$

para todo $z \in V$. Si la función f no es identicamente nula en una vecindad de z_0, podemos considerar $\tilde{f}(z_0) \neq 0$ en esta representación; en este caso el número n está únicamente determinado y lo llamamos el *orden* de f en z_0 y lo denotamos por $\mu_{z_0}(f)$. Si $n > 0$ decimos que f tiene un *cero* de orden n en z_0, si $n < 0$ decimos que f tiene un *polo* de orden $-n$ en este punto. Una función meromofa es holomorfa al rededor del punto z_0 si y solo si tiene orden no negativo en este punto.

Observación 2.1. Por supuesto, cualquier función regular (respectivamente racional) sobre un abierto de Zariski de la recta afín $\mathbb{A}^1_{\mathbb{C}} = \mathbb{C}$ es holomorfa y una función racional será meromorfa. Sin embargo, existen muchas funciones holomorfas que no son regulares y muchas funciones meromorfas que no son racionales, por ejemplo,

$$f : \mathbb{C} \to \mathbb{C}, \quad z \mapsto e^z.$$

2.2.1. Propiedades de funciones holomorfas

A pesar de que la definición de función holomorfa, es decir función diferenciable en el sentido complejo, es formalmente igual a la definición de función real diferenciable, el comportamiento en el caso complejo es totalmente diferente al caso real. Las diferencias más notables son:

(a) Toda función holomorfa es automáticamente infinitamente diferenciable, es decir, toda las derivadas de orden superior $f^{(k)}$ para $k \in \mathbb{N}$ existen y son nuevamente holomorfas.

(b) Toda función holomorfa f es analítica, es decir, se puede representar localmente al rededor de cualquier punto z_0 por su serie de Taylor. El radio de convergencia es "tan grande como puede ser", es decir, si f es holomorfa en una bola abierta U al rededor de z_0, entonces la serie de Taylor de f en z_0 converge y representa f al menos sobre U. En consecuencia, una función meromorfa f de orden n en z_0 puede ser expandida en una serie de Laurent como

$$f(z) = \sum_{k=n} c_k (z - z_0)^k.$$

El coeficiente c_{-1} de la serie se llama *residuo* de f en z_0 y se denota $\mathrm{res}_{z_0} f$.

Los residuos se relacionan con los órdenes de una función meromorfa de la siguiente manera: si $f(z) = (z - z_0)^n \tilde{f}(z)$ se tiene que

$$\mathrm{res}_{z_0} \frac{f'(z)}{f(z)} = \mathrm{res}_{z_0} \left(\frac{n}{z - z_0} + \frac{\tilde{f}'(z)}{\tilde{f}(z)} \right) = n = \mu_{z_0}(f).$$

(c) (Teorema de los residuos) Si γ es un contorno cerrado, orientado positivamente y f es una función meromorfa en una vecindad de γ y su interior, que no tiene polos sobre γ, entonces

$$\int_\gamma f(z)\, dz = 2\pi i \sum_{z_0} \mathrm{res}_{z_0} f,$$

donde la suma se toma sobre todos los z_0 al interior de γ donde f tiene polos. En particular si f es holomorfa al interior de γ, esta integral se anula.

(d) (Teorema Liouville) Toda función que es holomorfa y acotada sobre todo el plano complejo $\mathbb{C}$ es constante.

3. Curvas elípticas

Definición 3.1. Una **curva elíptica** es una curva cúbica suave en $\mathbb{P}^2$.

Veremos que las curvas elípticas se pueden dotar naturalmente de una estructura de grupo.

Proposición 3.1. *Sea $X \subset \mathbb{P}^2$ una curva elíptica, y sea $a_0 \in X$ un punto. Entonces el mapeo*

$$\Phi : X \to Pic^0 X, \quad a \mapsto a - a_0$$

es una biyección.

Demostración. Como $\deg(a - a_0) = 0$, el mapeo Φ es claramente bien definido. Además es inyectivo, si $\Phi(a) = \Phi(b)$ para $a, b \in X$ entonces $a - a_0 = b - a_0$ y por tanto $a - b = 0$, en $\mathrm{Pic}^0 X$. Por proposición 2.1 esto es posible si $a = b$.
Para mostrar que Φ es sobreyectiva, sea D un elemento arbitrario de $\mathrm{Pic}^0 X$, que podemos escribir como

$$D = a_1 + \cdots + a_m - b_1 - \cdots - b_m$$

para algún $m \in \mathbb{N}$ y no necesariamente distintos $a_1, \ldots, a_m, b_1, \ldots, b_m \in X$. Supongamos primero que $m \geq 2$. Luego, existen polinomios lineales homogéneos l, l' en X tal que $\div l = a_1 + a_2 + \psi(a_1, a_2)$ y $\div l' = b_1 + b_2 + \psi(b_1, b_2)$. El cociente de estos polinomios es una función racional en X, cuyo divisor $a_1 + a_2 + \psi(a_1, a_2) - b_1 - b_2 - \psi(b_1, b_2)$ es por tanto cero en $\mathrm{Pic}^0 X$. Se sigue que podemos escribir

$$D = \psi(b_1, b_2) + a_3 + \cdots + a_m - \psi(a_1, a_2) - b_3 - \cdots - b_m \in \mathrm{Pic}^0 X.$$

Hemos reducido entonces el número m de puntos (positivos y negativos) en D por 1. Continuando este proceso, podemos asumir que $m = 1$, es decir, $D = a_1 - b_1$ para algunos $a_1, b_1 \in X$.
De la misma manera, se tiene que

$$a_0 + a_1 + \psi(a_0, a_1) - b_1 - \psi(a_0, a_1) - \psi(b_1, \psi(a_0, a_1)) = 0 \in \mathrm{Pic}^0 X,$$

luego $D = a_1 - b_1 = \psi(b_1, \psi(a_0, a_1)) - a_0 \in \mathrm{Pic}^0 X$. Por lo tanto, $D = \Phi(\psi(b_1, \psi(a_0, a_1)))$, es decir, Φ es sobreyectiva. □

3.1. Ley de grupo en curvas elípticas

Sea $X \subset \mathbb{P}^2$ una curva elíptica. Luego de escoger $a_0 \in X$, la proposición anterior nos da una biyección canónica entre la variedad X y el grupo abeliano $\mathrm{Pic}^0 X$, es decir, dos objetos matemáticos diferentes. Así, podemos usar esta la biyección para dotar a X de una estructura de grupo abeliano, y a $\mathrm{Pic}^0 X$ la estructura de una variedad suave y proyectiva.

De hecho, $\mathrm{Pic}^0 X$ se puede convertir en una variedad (llamada la **variedad de Picard**) para cada curva suave y proyectiva X. Sin embargo, en general no es isomorfa a X. Sólo se puede mostrar que el mapeo $\Phi : X \to \mathrm{Pic}^0 X$ $a \mapsto a - a_0$ de la proposición anterior es inyectivo si X no es isomorfo a $\mathbb{P}^1$, de modo que entonces podemos pensar en X como una subvariedad de Picard.

En contraste, el hecho de que X puede verse como grupo abeliano es especial en curvas elípticas. En lo siguiente exploraremos la estructura de grupo explícitamente.

Construcción de la estructura de grupo en una curva elíptica: Sea a_0 un punto fijo de $X \subset \mathbb{P}^2$. Como se dijo antes, podemos utilizar la biyección de la proposición 2 para definir una estructura

de grupo en X. Más precisamente, si denotamos a esta operación de grupo por $\oplus$ (para distinguir de la adición en Div$X$ o Pic$X$), entonces $a \oplus b$ para $a, b \in X$ debe satisfacer

$$\Phi(a \oplus b) = \Phi(a) + \Phi(b).$$

Para hallar explícitamente $a \oplus b$, notemos que $a + b + \psi(a, b)$ y $a_0 + \psi(a, b) + \psi(a_0, \psi(a, b))$ son divisores de polinomios lineales homogéneos, y por tanto

$$a + b + \psi(a, b) - a_0 - \psi(a, b) - \psi(a_0, \psi(a, b)) = 0 \quad \in \mathrm{Pic}^0 X.$$

Por lo tanto,

$$\begin{aligned} a \oplus b &= \Phi^{-1}(\Phi(a) + \Phi(b)) \\ &= \Phi^{-1}(a - a_0 + b - a_0) \\ &= \Phi^{-1}(\psi(a_0, \psi(a, b)) - a_0) \\ &= \psi(a_0, \psi(a, b)). \end{aligned}$$

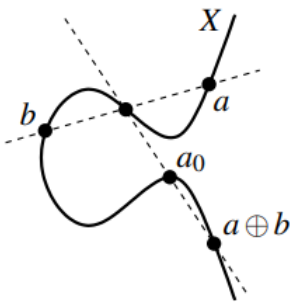
En otras palabras, para construir $a \oplus b$ dibujamos la recta que une a a y b. Luego dibujamos otra recta que pasa por el punto $\psi(a, b)$ y el punto a_0. El tercer punto de intersección de esta segunda recta con X es entonces $a \oplus b$.
Similarmente, para construir la inversa $\ominus a$ de a en esta estructura de grupo, utilizamos la relación

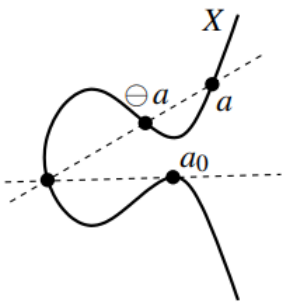
$$a_0 + a_0 + \psi(a_0, a_0) - a - \psi(a_0, a_0) - \psi(a, \psi(a_0, a_0)) = 0 \quad \in \mathrm{Pic}^0 X$$

para obtener

$$\begin{aligned} \ominus a &= \Phi^{-1}(-\Phi(a)) \\ &= \Phi^{-1}(a_0 - a) \\ &= \Phi^{-1}(\psi(a, \psi(a, a_0)) - a_0) \\ &= \psi(a, \psi(a_0, a_0)). \end{aligned}$$

Así, para construir la inversa $\ominus a$ dibujamos la recta tangente que pasa por a_0. Luego dibujamos otra recta que pasa por el punto de intersección $\psi(a_0, a_0)$ de esta tangente con X y el punto a. El tercer punto de intersección de la segunda recta con X es $\ominus a$.





Observemos que, utilizando la descripción geométrica, la operación $\oplus$ puede ser definida completamente elemental, sin hacer referencia a la teoría de divisores. Sin embargo, sería muy difícil demostrar que obtenemos una estructura de grupo, en particular, para probar la asociatividad. Finalmente, el elemento neutro de este grupo es el punto $(0 : 1 : 0) \in \mathbb{P}^2$.

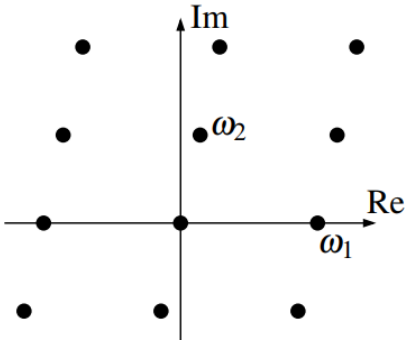
3.2. Aplicaciones de curvas elípticas al análisis complejo

Nos restringimos ahora al cuerpo base de los complejos $\mathbb{C}$, de manera que una curva elíptica es, desde el punto de vista topológico, un toro. Comenzamos dando un resumen de los resultados que necesitaremos de análisis complejo.

Para nuestras aplicaciones en las curvas elípticas necesitaremos un tipo particular de función meromorfa. Para describir su construcción fijemos dos números complejos $w_1, w_2 \in \mathbb{C}$ que sean linealmente independientes sobre $\mathbb{R}$, es decir, que no están sobre la misma línea real en $\mathbb{C}$ a través del origen. Entonces el conjunto

$$\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2 = \{nw_1 + mw_2 : n, m \in \mathbb{Z}\} \subset \mathbb{C}$$

se llama un *reticulado* en $\mathbb{C}$, como se indica en los puntos de la figura siguiente.



Note que Λ es un subgrupo aditivo de $\mathbb{C}$ y que el cociente $\mathbb{C}/\Lambda$ es un toro topológico. Además, las funciones sobre el toro $\mathbb{C}/\Lambda$ corresponden exactamente a las funciones Λ-periódicas sobre $\mathbb{C}$, esto es, funciones sobre $\mathbb{C}$ tal que

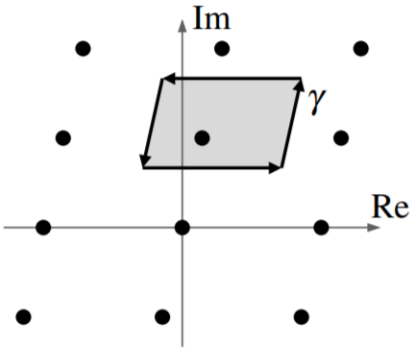
$$f(z + w) = f(z)$$

para todo $z \in \mathbb{C}$ y para todo $w \in \Lambda$. De ahora en adelante, Λ será un reticulado fijo en $\mathbb{C}$ y usaremos de manera indistinta, los conceptos de "función sobre $\mathbb{C}/\Lambda$" y "función Λ-periódica sobre $\mathbb{C}$".
Nuestro objetivo, por ahora, es ver que $\mathbb{C}/\Lambda$ puede ser identificado con una curva elíptica en una manera natural. Comenzamos con un resultado auxiliar que nos indica ya una relación entre álgebra y análisis; específicamente, probaremos que una función meromorfa sobre $\mathbb{C}/\Lambda$ tiene el mismo número de ceros que de polos.

Lema 3.1. *Sea $f : \mathbb{C}/\Lambda \to \mathbb{C} \cup \{\infty\}$ una función meromorfa no nula, entonces*

$$\sum_{z_0 \in \mathbb{C}/\Lambda} \mu_{z_0}(f) = 0.$$

Demostración. Llamamos "paralelogramo de periodicidad" a un paralelogramo cuyos bordes generan Λ. Tomamos un camino γ al rededor de los lados de un paralelogramo de periodicidad, de tal forma que los ceros y polos de f no estén sobre γ. Así se tiene que Λ tiene un solo representante dentro del paralelogramo, como se muestra en la figura siguiente.



Debido a la periodicidad de f, las integrales a lados opuestos del paralelogramo se anulan mutuamente, se sigue que

$$\int_\gamma \frac{f'(z)}{f(z)}\,dz = 0.$$

Ahora calculemos la misma integral usando el teorema de los residuos: sea z_0 un punto con $\mu_{z_0}(F) = n$, entonces se sigue

$$\operatorname{res}_{z_0} \frac{f'(z)}{f(z)} = \operatorname{res}_{z_0} \left(\frac{n}{z - z_0} + \frac{\tilde{f}'(z)}{\tilde{f}(z)} \right) = n = \mu_{z_0}(f),$$

usando el teorema de los residuos tenemos

$$\int_\gamma \frac{f'(z)}{f(z)}\,dz = 2\pi i \sum_{z_0} \operatorname{res}_{z_0} \frac{f'(z)}{f(z)} = 2\pi i \sum_{z_0} \operatorname{res}_{z_0} \mu_{z_0}(f).$$

De donde, junto con la primera igualdad

$$\begin{aligned} 2\pi i \sum_{z_0} \operatorname{res}_{z_0} \mu_{z_0}(f) &= 0 \\ \Rightarrow \sum_{z_0} \operatorname{res}_{z_0} \mu_{z_0}(f) &= 0. \end{aligned}$$

□

3.2.1. Función $\wp$ de Weierstrass

Proposición 3.2. *(y definición). Sea $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ un reticulado en $\mathbb{C}$. Existe una función $\wp$ meromorfa sobre $\mathbb{C}$, llamada la función $\wp$ de Weierstrass, definida por*

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

Esta función posee polos de orden 2 exactamente en los puntos del reticulado.

Demostración. Es sabido que la suma (infinita) de funciones holomorfas, es holomorfa en z_0 dado que la suma converge uniformemente en una vecindad de z_0.
Daremos una idea de la demostración de la convergencia: Sea $z_0 \in \mathbb{C} \setminus \Lambda$ un punto fijo que no pertenece al reticulado. Entonces todo sumando es una función holomorfa en una vecindad de z_0. Las expansiones de estos sumandos para ω grande son

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{\left(1 - \frac{z}{\omega}\right)^2} - 1 \right) = \frac{2z}{\omega^3} + \left(\textit{términos de orden superior} \frac{1}{\omega^4} \right)$$

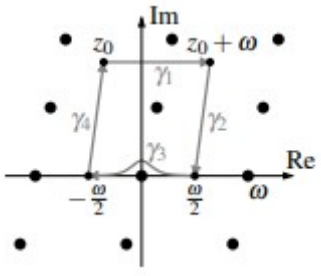
Así, los sumandos crecen como ω^3. Sumamos estos valores de acuerdo al valor absoluto de ω. Note que el número de puntos del reticulado con un valor absoluto dado aproximadamente igual a $n \in \mathbb{N}$ es proporcional al área del anillo de radio interior $n - \frac{1}{2}$ y radio exterior $n + \frac{1}{2}$, la cual crece linealmente con n. Por lo tanto, la suma final es del orden de $\sum_{n=1}^{\infty} n\frac{1}{n^3} = \sum_{n=1}^{\infty} \frac{1}{n^2}$, la cual es convergente. Note que la suma no sería convergente si no se resta la constante $\frac{1}{\omega^2}$ en cada sumando, ya que cada término crecería como $\frac{1}{\omega^2}$, y por lo tanto la suma sería del orden de $\sum_{n=1}^{\infty} \frac{1}{n}$, la cual es divergente.
Finalmente, los polos de orden 2 en los puntos de Λ son claramente visibles. □

Observación 3.1. (Propiedades de la función $\wp$). Es conocido que en una serie absolutamente convergente, como la anterior, toda manipulación (reordenamiento de sumandos, diferenciación término a término) se pueden realizar sin ningún problema. En particular, las siguientes propiedades de la función $\wp$ son obvias:

(a) La función $\wp$ es una función par, es decir, $\wp(z) = \wp(-z)$ para todo $z \in \mathbb{C}$. Así, su serie de Laurent en 0 contiene solo exponentes pares.

(b) Su derivada es $\wp'(z) = \sum_{\omega \in \Lambda} \frac{-2}{(z-\omega)^3}$. La cual es una función impar, es decir, $\wp'(-z) = -\wp'(z)$ para todo z. Así su serie de Laurent en 0 contiene solo exponentes impares. Tiene polos de orden 3 exactamente en los puntos del reticulado.

(c) La función $\wp$ es doblemente periodica con respecto a Λ, es decir, $\wp(z_0) = \wp(z_0+\omega)$ para todo $z_0 \in \mathbb{C}$ y $\omega \in \Lambda$. Para probar esto, primero note que es obvio por (b) que $\wp'(z_0) = \wp'(z_0+\omega)$. Ahora, integre $\wp'(z)$ sobre el contorno cerrado $\gamma = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4$ mostrado en la imagen



El resultado es 0, ya que $\wp$ es una integral de $\wp'$. Pero también, la integral a través de γ_2 cancela a la integral sobre γ_4 ya que $\wp'(z)$ es periodica. La integral sobre γ_3 es igual a $\wp(-\frac{\omega}{2}) - \wp(\frac{\omega}{2})$, la cual se anula pues $\wp$ es una función par.
Se concluye que

$$0 = \int_{\gamma_1} \wp'(z)dz = \wp(z_0 + \omega) - \wp(z_0)$$

es decir, $\wp$ es periodica con respecto a Λ.

Lema 3.2. *La función $\wp$ asociada a un reticulado Λ satisface una ecuación diferencial*

$$\wp'(z)^2 = c_3\wp(z)^3 + c_2\wp(z)^2 + c_1\wp(z) + c_0, \quad \textit{para todo } z \in \mathbb{C}$$

para algunas constantes $c_0, c_1, c_2, c_3 \in \mathbb{C}$(dependen de Λ).

Demostración. Por la observación anterior, sabemos que $(\wp')^2$ es una función par con un polo de orden 6 en el origen. Por lo tanto su serie de Laurent centrada en 0 es de la forma

$$\wp'(z)^2 = \frac{a_{-6}}{z^6} + \frac{a_{-4}}{z^4} + \frac{a_{-2}}{z^2} + a_0(\textit{ términos de orden superior})$$

para algunas constantes $a_{-6}, a_{-4}, a_{-2}, a_0 \in \mathbb{C}$. Las funciones $\wp^3, \wp^2, \wp$ y 1 también son funciones pares y tienen polos en el origen de orden $6, 4, 2$, y 0, respectivamente. Luego existen constantes $c_3, c_2, c_1, c_0 \in \mathbb{C}$ tales que la serie de Laurent de la combinación lineal

$$f(z) := \wp'(z)^2 - c_3\wp(z)^3 - c_2\wp(z)^2 - c_1\wp(z) - c_0$$

posee solo potencias positivas de z. Por lo tanto, f es holomorfa en una vecindad del origen y se anula en 0.
Pero $\wp, \wp'$ son $\Lambda - periodicas$, por lo tanto f lo es. Así, f es holomorfa alrededor de cada punto del reticulado. Pero f es también holomorfa alrededor de todos los otros puntos, ya que $\wp, \wp'$ lo son. En otras palabras, f es holomorfa sobre todo $\mathbb{C}$.
Mas aún, por la periodicidad, todo valor tomado por f es asumido sobre el paralelogramo $\{x\omega_1 + y\omega_2 : x, y \in [0, 1]\}$. Como f es continua, su imagen sobre este paralelogramo compacto, y por tanto sobre todo $\mathbb{C}$ es acotada. Por el teorema de Liouville, f debe ser constante. Pero f se anula en 0, por lo que f debe ser la función nula, el cual es justamente el enunciado del Lema. □

Observación 3.2. Por un calculo explícito, uno puede probar que los coeficientes c_3, c_2, c_1, c_0 en el Lema (3.2) están dados por

$$c_3 = 4, \quad c_2 = 0, \quad c_1 = -60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4}, \quad c_0 = -140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}$$

La prueba del Lema (3.2) nos muestra lo poderoso que pueden ser los métodos del análisis complejo, para probar la ecuación diferencial, fue suficiente comparar solo cuatro coeficientes de sus series de Laurent centradas en el origen, el resto fue completamente teoría general.
Note además que la ecuación diferencial del Lema (3.2) es una ecuación cúbica (no-homogenea) en las dos funciones $\wp, \wp'$, las cuales son $\Lambda - periodicas$ y por tanto bien definidas sobre el cociente $\mathbb{C}/\Lambda$. Por lo tanto, podemos usarla para obtener una aplicación desde $\mathbb{C}/\Lambda$ a una curva elíptica, como sigue:

Proposición 3.3. *Sea $\Lambda \subset \mathbb{C}$ un reticulado fijo, y sea $X \subset \mathbb{P}^2_{\mathbb{C}}$ una curva cubica*

$$X = \{(x_0 : x_1 : x_2) | x_2^2 x_0 = c_3 x_1^3 + c_2 x_1^2 x_0 + c_1 x_1 x_0^2 + c_0 x_0^3\}$$

para las constantes $c_3, c_2, c_1, c_0 \in \mathbb{C}$ del Lema (3.2). Entonces existe una biyección

$$\Psi : \mathbb{C}/\Lambda \to X, \quad z \mapsto (1 : \wp(z) : \wp'(z))$$

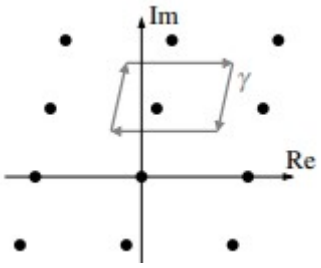
Demostración. Como $\wp$ y $\wp'$ son periodicas con respecto a Λ y satisfacen la ecuación diferencial del Lema (3.2), es claro que Ψ esta bien definido como aplicación sobre X (Hablando estrictamente, para $z = 0$ debemos notar que $\wp$ y $\wp'$ tienen polos de orden 2 y 3, respectivamente, así la expresión dada por $\Psi(0)$ formalmente se ve como $(1 : \infty : \infty)$. Pero como $\wp(z), \wp'(z)$ son funciones meromorfas, podemos escribir $\wp(z) = \frac{f(z)}{z^2}$ y $\wp'(z) = \frac{g(z)}{z^3}$ localmente, alrededor del origen, para algunas funciones f, g que no se anulan en 0, y así debemos interpretar la expresión para Ψ como

$$\Psi(0) = \lim_{z\to 0}(1 : \wp(z) : \wp'(z)) = \lim_{z\to 0}(z^3 : zf(z) : g(z)) = (0 : 0 : 1)$$

es decir, $\Psi(z)$ esta bien definida para $z = 0$).
Ahora, sea $(x_0 : x_1 : x_2) \in X$ un punto dado, vamos a probar que su imagen inversa bajo Ψ es exactamente un punto. Por lo anterior, esto es claro para el punto al infinito $(0 : 0 : 1)$, así que podemos asumir que tomamos un punto distinto a este, así podemos pasar a coordenadas no homogeneas donde $x_0 = 1$.
Primero, buscamos un $z \in \mathbb{C}$ tal que $\wp(z) = x_1$. Para esto, consideramos la integral

$$\int_\gamma \frac{\wp'(z)}{\wp(z) - x_1} dz$$

sobre el borde de cualquier "paralelogramo de periodicidad" (esto es, que no contiene a los ceros y polos de la función $z \mapsto \wp(z) - x_1$), como en la siguiente figura:



La integral se anula en los lados opuestos del paralelogramo por la periodicidad de $\wp$ y $\wp'$. Así, la integral debe ser 0. Luego, por 2.2.1 (b) y (c) se tiene,

$$0 = \sum_{z_0\in\mathbb{C}/\Lambda} res_{z_0} \frac{\wp'(z)}{\wp(z) - x_1} = \sum_{z_0\in\mathbb{C}/\Lambda} ord_{z_0}(\wp(z) - x_1).$$

En otras palabras, la función $z \mapsto \wp(z) - x_1$ tiene tantos ceros como polos en $\mathbb{C}/\Lambda$, contados con multiplicidad. Como $\wp$ tiene un polo de orden 2 en los puntos del reticulado, se tiene entonces que existen exactamente dos puntos en $\wp^{-1}(x_1)$, contados con multiplicidad.
Para tal punto z con $\wp(z) = x_1$, tenemos por el lema (3.2)

$$\wp'(z)^2 = c_3\wp(z)^3 + c_2\wp(z)^2 + c_1\wp(z) + c_0 = c_3x_1^3 + c_2x_1^2 + c_1x_1 + c_0 = x_2^2$$

Como $(1 : x_1 : x_2) \in X$. Entonces, existen dos posibilidades:

i.- Si $\wp'(z) = 0$, entonces $x_2 = 0$ también, y así, z es un doble cero(es decir, el único cero) de la función $z \mapsto \wp(z) - x_1$. Por lo tanto, existe exactamente un $z \in \mathbb{C}/\Lambda$ con $\Psi(z) = (1 : \wp(z) : \wp'(z)) = (1 : x_1 : x_2)$.

ii.- Si $\wp'(z) \neq 0$, entonces z es un cero simple de $z \mapsto \wp(z) - x_1$. Como $\wp$ es par y $\wp'$ impar por la observación (3.1), vemos que $-z$ debe ser el otro cero, y satisface $\wp'(-z) = -\wp'(z)$. Por lo tanto, exactamente una de las ecuaciones $\wp'(z) = x_2$ y $\wp'(-z) = x_2$ se cumple, y el correspondiente punto es la única imagen inversa de $(1 : x_1 : x_2)$ bajo Ψ.

Por lo tanto, se concluye que Ψ es biyectiva. $\square$

Observación 3.3. De hecho, la aplicación Ψ no es solo una biyección: Ambos $\mathbb{C}/\Lambda$ y X son variedades complejas de dimensión 1, y Ψ es incluso un isomorfismo entre estas dos variedades.

Observación 3.4. Con la proposición (3.3), nos encontramos en una situación similar a la de la proposición (3.1), tenemos una biyección entre $\mathbb{C}/\Lambda$ y una variedad X. Así, la aplicación Ψ de la proposición anterior puede ser usada para construir una estructura de grupo sobre X, de hecho esta estructura de grupo es la misma que la obtenida por la aplicación φ de la proposición (3.1) usando divisores. Pero, las propiedades algebraicas de esta estructura de grupos es mucho mas obvia, por ejemplo, es facil ver que los puntos de orden n son los n^2 puntos de la forma

$$\frac{1}{n}\left(i\omega_1 + j\omega_2\right), \quad para\ 0 \leq i, j < n.$$

3.2.2. Funciones theta y divisores

Existen al menos dos formas de abordar el problema de construir una inmersión holomorfa de una curva elíptica, o más generalmente de un toro complejo $\mathbb{C}/\Lambda$, en el espacio proyectivo $\mathbb{P}^n$. La primera manera consiste en buscar n funciones Λ-periódicas meromorfas $f_1, f_2, \ldots, f_n$ y tratar de extender la aplicación meromorfa

$$u : \mathbb{C}/\Lambda \to \mathbb{P}^n, \quad u(x) = (f_1(x), f_2(x), \ldots, f_n(x))$$

a una aplicación holomorfa. La segunda manera consiste en buscar funciones holomorfas $\tilde{u}_0, \tilde{u}_1, \ldots, \tilde{u}_n$ sobre $\mathbb{C}$, que no tengan un ceros comunes, de manera que la aplicación holomorfa

$$(\tilde{u}_0, \tilde{u}_1, \ldots, \tilde{u}_n) : \mathbb{C} \to \mathbb{C}^{n+1}$$

induce, por paso a cociente, una aplicación $\mathbb{C}/\Lambda \to \mathbb{P}^n$. Para esto, se requiere que, para cada $\lambda \in \Lambda$, exista una función $f_\lambda : \mathbb{C} \to \mathbb{C}^*$ tal que

$$\tilde{u}_j(z + \lambda) = f_\lambda(z)\tilde{u}_j(z)$$

para todo $j \in \{0, \ldots, n\}$. Esto motiva la definición siguiente, en la cuál nos enfocamos en el caso de dimensión igual a 1, fijamos nuevamente un reticulado Λ y llamamos E la curva elíptica asociada.

Definición 3.2. Llamamos *función theta* asociada a Λ a toda función θ entera sobre $\mathbb{C}$, no idénticamente nula, tal que para cada $\lambda \in \Lambda$ existen constantes a_λ, b_λ que satisfacen

$$\theta(z + \lambda) = e^{2\pi i(a_\lambda z + b_\lambda)}\theta(z)$$

para todo $z \in \mathbb{C}$. La familia $(a_\lambda, b_\lambda)_{\lambda\in\Lambda}$ es llamada el *tipo* de θ.

La ecuación anterior es equivalente a

$$\frac{\theta'}{\theta}(z + \lambda) = 2\pi i a_\lambda + \frac{\theta'}{\theta}(z).$$

En otras palabras, las funciones theta son funciones enteras, no idénticamente nulas, para las que $\left(\frac{\theta'}{\theta}\right)'$ es una función elíptica. Una familia $\theta_0, \ldots \theta_n$ del mismo tipo, sin ceros comunes, definen una aplicación holomorfa de E en $\mathbb{P}$.

Ejemplo 3.1.

1. Toda función
$$z \mapsto e^{2\pi i(az^2+bz+c)}$$
es una función theta. Estas son llamadas las funciones theta triviales y obviamente, no se anulan entre sí.

2. **La función σ de Weierstrass**, definida por el producto infinito
$$\sigma(z) = z \prod_{\lambda\in\Lambda} \left(1 - \frac{z}{\lambda}\right) e^{\frac{z}{\lambda} + \frac{z^2}{2\lambda^2}},$$
es una función theta, pues la derivada de $\frac{\sigma'}{\sigma}$ es $-\wp$.

3. **Las funciones theta de Riemann** se definen para cada par (a, b) de reales por

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau) = \sum_{m \in \mathbb{Z}} e^{i\pi(\tau(m+a)^2 + 2(m+a)(z+b))}.$$

Estas funciones verifican, para todo par de enteros p, q

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z + \tau p + q) = e^{i\pi(-2pz - p^2\tau + 2pb - 2aq)} \theta \begin{bmatrix} a \\ b \end{bmatrix} (z),$$

por lo que son funciones theta para el reticulado Λ_τ.

A una función meromorfa f no nula sobre E, se le puede asociar un divisor

$$div(f) = \sum_{x \in E} \mu_x(f) \cdot x,$$

el cuál es de orden par debido a 3.1. A pesar de que una función θ no define una función sobre E, sus "divisores sobre $\mathbb{C}$" son invariantes por traslación de Λ; podemos así definir el divisor $div(\theta)$ de θ sobre E. Ya que θ es holomorfa, este divisor es efectivo.

Ejemplo 3.2. 1. El divisor de σ es 0.

2. El divisor de $\theta \begin{bmatrix} a \\ b \end{bmatrix}$ es la traslación de $\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ por $\tau a + b$.

Proposición 3.4. *Sean (λ_1, λ_2) una base de Λ y θ una función theta. Entonces se tiene que*

$$a_{\lambda_1}\lambda_2 - a_{\lambda_2}\lambda_1 = deg(div(\theta)).$$

Demostración. (Idea) Es suficiente integrar la función $\frac{\theta'}{\theta}$ sobre el paralelogramo de lados λ_1, λ_2, de tal manera que no contenga ningún cero de θ y utilizar el hecho de que

$$\frac{\theta'}{\theta}(z + \lambda_j) = 2\pi i a_{\lambda_j} + \frac{\theta'}{\theta}(z).$$

□

Ejemplo 3.3. Para toda función θ de Riemann, se tiene $a_{\tau m+n} = -m$, de donde sus divisores son de grado 1. Ya que $\theta \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}$ es impar y no tiene polos, su divisor es 0 y del ejemplo 3.2, se tiene

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} = \tau(a + 1/2) + (b + 1/2).$$

Las funciones theta de Riemann, también nos permiten ver una curva elíptica como una plana cúbica. Nombramos

$$\theta_{00} = \theta \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \theta_{10} = \theta \begin{bmatrix} 1/2 \\ 0 \end{bmatrix}, \quad \theta_{01} = \theta \begin{bmatrix} 0 \\ 1/2 \end{bmatrix}, \quad \theta_{11} = \theta \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}.$$

Se puede probar que que θ_{00}, θ_{10} y θ_{01} son pares, mientras que θ_{11} es impar.

Proposición 3.5. *La aplicación holomorfa $u : E \to \mathbb{P}^2$ definida por*

$$z \mapsto (\theta_{00}(z)\theta_{11}(z)^2, \theta_{10}(z)\theta_{01}(z)\theta_{11}(z), \theta_{00}(z)^3)$$

induce un isomorfismo de E hacia la cúbica lisa de ecuación

$$Y^2Z = X(\beta Z + \alpha X)(\alpha Z - \beta X),$$

donde

$$\alpha = \frac{\theta_{10}(z)^2}{\theta_{00}(z)^2}, \quad \beta = \frac{\theta_{01}(z)^2}{\theta_{00}(z)^2}.$$

El cuerpo de funciones meromorfas de una curva elíptica es generado, sobre $\mathbb{C}$, por $\wp$ y $\wp'$, y su grado de trascendencia es 1. Además, toda función meromorfa definida sobre una curva elíptica, es un cociente de dos funciones theta del mismo tipo.

Las funciones theta son importantes en diversas áreas, incluidas las teorías de variedades abelianas y espacios módulo, y de las formas cuadráticas. Se utilizan para generalizar a un álgebra de Grassmann, aparecen en teoría cuántica de campos, en particular en la teoría de cuerdas y D-branas.

Referencias

[1] Debarre, O(2000). Tores et variétés abéliennes complexes.

[2] Gathmann, A(2018). Algebraic geometry.

[3] Silverman, J(2015). Rational points on Elliptic Curves.