Trabajo monográfico

Formas Modulares

Camilo Gallardo

Abril 2022

Orientador:

Gonzalo Tornaría

Licenciatura en Matemática
Universidad de la República
Montevideo, Uruguay

Introducción

El objetivo de este trabajo es entender las curvas modulares como espacios de módu-li. Para llegar a formalizar esta noción vamos a cubrir primero la teoría básica necesaria sobre superficies de Riemann, curvas elípticas y formas modulares. Las referencias principales son [Mil17] para los primeros tres capítulos y [DS05] especialmente para el último.

La teoria de las formas modulares es una de las herramientas más poderosas de la teoría de números. Sus aplicaciones son inmensas y se extienden a muchas otras áreas, incluida la física. En particular, las formas modulares se relacionan estrechamente con las curvas elípticas a través del teorema de modularidad, el cual permite probar resultados profundos como el Último Teorema de Fermat.

Por otro lado, los espacios de móduli nos darán un ejemplo de intercambio entre objetos algebraicos (curvas elípticas) y objetos analíticos (superficies de Riemann). Un resultado sorprendente en esta línea es que toda curva elíptica en los complejos es isomorfa a un toro, preservando la estructura de grupos. Esto se prueba en el capítulo 2. Los capítulos 3 y 4 generalizan sucesivamente las ideas anteriores hasta llegar al concepto de espacio de móduli de curvas elípticas. El principio guía es que los puntos de una superficie pueden codificar información acerca de un conjunto de objetos algebraicos.

El punto de partida serán las superficies que surgen de la acción de cierto grupo de transfomaciones en el semiplano complejo, dando lugar a las curvas modulares. El capítulo 2 comienza introduciendo la noción de curva elíptica en el plano proyectivo. Luego se estudian resultados de análisis en superficies de Riemann compactas, los cuales permiten comprender el cuerpo de las funciones doblemente periódicas y su papel crucial en la parametrización de curvas elípticas. El capítulo 3 vuelve sobre la estructura compleja de las curvas modulares para dar una interpretación geométrica de las formas modulares como formas diferenciales. Para ilustrar la utilidad de esta idea se calcula la dimensión de los espacios de formas modulares a partir de resultados de geometría algebraica. Finalmente, la información sobre los ceros de las formas modulares nos permitirá probar que el j-invariante define un isomorfismo entre la curva modular $Y(1)$ y la esfera de Riemann. El último capítulo se vale del material anterior para explicitar cómo las clases de isomorfismo de curvas elípticas, junto a cierta información sobre la N-torsión, están determinadas por los puntos en la curva modular de cierto subgrupo de congruencia de nivel N.

Como comentario final, si bien el contenido se limita al cuerpo de los números complejos, hay una teoría profunda y rica que resulta de considerar las curvas modulares como curvas algebraicas en $\mathbb{Q}$, o en cuerpos intermedios, lo cual sería una posible área de estudio a seguir en el futuro.

Índice general

Capítulo 1

Curvas modulares

1. Acciones de grupos en $\mathbb{H}$

Recordemos primero el grupo general lineal $\mathrm{GL}_n(\mathbb{C})$ de las matrices $n \times n$ invertibles con coeficientes en $\mathbb{C}$. En particular nos va a interesar la acción de $\mathrm{GL}_2(\mathbb{C})$ en $\mathbb{C}^2$, dada por

$$\alpha \cdot (z, w) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} z \\ w \end{pmatrix} = \begin{pmatrix} az + bw \\ cz + dw \end{pmatrix}.$$

Definición 1.1. *El **espacio proyectivo complejo** de dimensión n se define informalmente como el conjunto de las rectas en $\mathbb{C}^{n+1}$ que pasan por el origen y, formalmente, como el cociente de $\mathbb{C}^{n+1}$ menos el origen identificando vectores colineales,*

$$\mathbb{P}^n(\mathbb{C}) = \left(\mathbb{C}^{n+1} - \{0\}\right) / \sim \qquad v \sim w \iff \exists \lambda \in \mathbb{C} - \{0\} : w = \lambda v$$

Proposición 1.1. *El espacio proyectivo $\mathbb{P}^n(\mathbb{C})$ es compacto.*

Prueba. La esfera de dimensión n compleja, $S^n = \{(z_i) \in \mathbb{C}^{n+1} : \sum |z_i|^2 = 1\}$ es compacta. Su imagen por la proyección al cociente $\mathbb{C}^{n+1} - \{0\} \to \mathbb{P}^n(\mathbb{C})$ es sobreyectiva. □

Definimos el *subespacio afín* como todos los puntos de $\mathbb{P}^n(\mathbb{C})$ cuya última coordenada es distinta de cero. Este conjunto se identifica con $\mathbb{C}^n$ tomando representantes cuya última coordenada es 1. El complemento del subespacio afín se identifica con $\mathbb{P}^{n-1}(\mathbb{C})$. Por lo tanto podemos escribir

$$\mathbb{P}^n(\mathbb{C}) = \mathbb{C}^n \cup \mathbb{P}^{n-1}(\mathbb{C}).$$

Por ejemplo, cuando $n = 1$, la recta con dirección (z, w) se puede representar por el vector $(z/w, 1)$ si $w \neq 0$. Abusando un poco la terminología, llamemos al número $z/w \in \mathbb{C}$, la "clase de equivalencia"de (z, w). Hay una sola dirección en $\mathbb{C}^2 - \{(0, 0)\}$ con $w = 0$, representada por el vector $(1, 0)$. En este caso definimos $z/w = \infty$, y decimos que $(1, 0) \in \mathbb{P}^1(\mathbb{C})$ es el *punto en el infinito*. Con esta notación, $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$.

Definición 1.2. *El espacio $\mathbb{C} \cup \{\infty\}$ es compacto con la siguiente topología: en $\mathbb{C}$ es la topología usual, y se definen los entornos de ∞ como los abiertos de $\mathbb{C}$ con complemento compacto. Topológicamente, este espacio es una esfera, y se llama la **esfera de Riemann**. De hecho se puede ver lo siguiente:*

Proposición 1.2. *El espacio proyectivo $\mathbb{P}^1(\mathbb{C})$ es homeomorfo a la esfera de Riemann.*

PRUEBA. El mapa $\phi : \mathbb{C}^2 - \{0\} \to \mathbb{C} \cup \{\infty\}$ que lleva el punto (z, w) en su clase de equivalencia z/w es continuo y abierto, y define un mapa continuo y biyectivo $\tilde{\phi} : \mathbb{P}^1(\mathbb{C}) \to \mathbb{C} \cup \{\infty\}$ tal que el siguiente diagrama conmuta.

$$\begin{array}{ccc} \mathbb{C}^2 - \{0\} & & \\ \Big\downarrow p & \searrow^{\phi} & \\ \mathbb{P}^1(\mathbb{C}) & \xrightarrow{\tilde{\phi}} & \mathbb{C} \cup \{\infty\} \end{array}$$

El mapa $\tilde{\phi}$ es abierto porque ϕ es abierto y p es continuo.

□

Para todo $\alpha \in \mathrm{GL}_2(\mathbb{C})$, el mapa $(z, w) \mapsto \alpha \cdot (z, w)$ es lineal, luego lleva rectas en rectas. Se deduce que la acción de $\mathrm{GL}_2(\mathbb{C})$ en $\mathbb{C}^2 - \{(0, 0)\}$ define una acción en $\mathbb{P}^1(\mathbb{C})$,

$$\alpha \cdot (z/w) = \frac{az + bw}{cz + dw} = \frac{a(z/w) + b}{c(z/w) + d},$$

de forma tal que actuar por $\mathrm{GL}_2(\mathbb{C})$ conmuta con la proyección $\mathbb{C}^2 - \{0\} \to \mathbb{P}^1(\mathbb{C})$.

$$\begin{array}{ccc} \mathbb{C}^2 - \{0\} & \xrightarrow{\alpha \cdot z} & \mathbb{C}^2 - \{0\} \\ \Big\downarrow & & \Big\downarrow \\ \mathbb{P}^1(\mathbb{C}) & \xrightarrow{\alpha \cdot z} & \mathbb{P}^1(\mathbb{C}) \end{array}$$

Explícitamente,

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \alpha \cdot z = \begin{cases} \frac{az+b}{cz+d} & cz + d \neq 0 \\ \infty & cz + d = 0 \end{cases} \qquad \alpha \cdot \infty = \begin{cases} \frac{a}{c} & c \neq 0 \\ \infty & c = 0 \end{cases} \tag{1}$$

Nos va a interesar restringir la acción al semiplano superior $\mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$. Si α es una matriz con coeficientes reales y $z \in \mathbb{H}$, entonces $cz + d$ es distinto de cero porque c y d son reales pero z no, y $\alpha(z) \neq \infty$. Por otro lado, la parte imaginaria de $\alpha(z)$ está dada por

$$\Im(\alpha \cdot z) = \frac{\Im(z)}{\mid cz + d \mid^2} \det(\alpha).$$

De esta ecuación se deduce que α preserva $\mathbb{H}$ si y solo si tiene determinante positivo. Para todo tal α podemos asumir que tiene determinante 1 ya que multiplicar la matriz por un escalar real deja invariante la transformación en (1) y no cambia el signo del determinante.

DEFINICIÓN 1.3. *Llamamos* $\mathrm{SL}_2(\mathbb{R})$ *al grupo de las matrices* 2×2 *con determinante* 1 *y coeficientes reales. La acción en* $\mathbb{H}$ *de* $\mathrm{SL}_2(\mathbb{R})$ *es la dada por* (1).

Una observación interesante es que, de hecho, todos los automorfismos en $\mathbb{H}$ provienen de la acción de una matriz en $\mathrm{SL}_2(\mathbb{R})$, la cual es única a menos de un factor ± 1.

PROPOSICIÓN 1.3. *Sea* $\mathrm{Aut}(\mathbb{H})$ *el grupo de automorfismos biholomorfos (holomorfo y con inversa holomorfa) de* $\mathbb{H}$. *Entonces* $\mathrm{Aut}(\mathbb{H}) \cong \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$.

La demostración es sencilla pero se difiere hasta la sección 3 de este capítulo.

2. Cocientes de $\mathbb{H}$

Sea Γ un grupo que actúa continuamente en un espacio topológico X. Definimos $\Gamma\backslash X$ como el espacio de las órbitas de X por Γ. Si p es la proyección $x \mapsto \Gamma x$, entonces los subconjuntos abiertos de $\Gamma\backslash X$ son todos aquellos cuya preimagen por p es abierta.

Nos interesa darle una estructura de variedad diferenciable al espacio $\Gamma\backslash\mathbb{H}$, para lo cual queremos que sea Hausdorff. El objetivo de esta sección es probar esta propiedad cuando Γ es un subgrupo discreto de $\mathrm{SL}_2(\mathbb{R})$.

LEMA 1.1. *Sea* G *un grupo topológico localmente compacto Hausdorff que actúa transitivamente sobre un espacio* X, *tal que el estabilizador* K *de un punto* x_0 *(y de cualquier punto) es compacto. Suponer también que el mapa* $G/K \to X$: $gK \mapsto g \cdot x_0$ *es un homeomorfismo. Entonces son equivalentes, para* Γ *subgrupo de* G:

1. *Para todos* A, B *compactos en* X, $\{\gamma \in \Gamma : A \cap \gamma B \neq \emptyset\}$ *es finito.*
2. Γ *es discreto.*

PRUEBA.

(2) $\Rightarrow$ (1): Sea p la proyección $G \to G/K$. Veamos que para A compacto en G/K, su preimagen $p^{-1}(A)$ es compacta en G. Sea $G = \bigcup_i V_i$ para una familia de abiertos. Como G es localmente compacto podemos suponer que la clausura $\bar{V}_i$ es compacta para cada V_i. Como A es compacto y p es abierta podemos tomar finitos V_i tales que $A \subseteq \bigcup_i p(V_i)$, luego A está contenido en la unión finita de los compactos $p(\bar{V}_i)$, y

$$p^{-1}(A) = AK \subseteq \bigcup_{i=1}^{n} \bar{V}_i K\,.$$

Cada $\bar{V}_i K$ es compacto en G por ser producto de compactos. Por otro lado, A es cerrado por ser compacto en un espacio Hausdorff, y entonces $p^{-1}(A)$ es un cerrado, contenido en un compacto.

Ahora sean A, B compactos en G/K. El conjunto $\{\gamma \in \Gamma : A \cap \gamma B \neq \emptyset\}$ es igual a la intersección de Γ con $\big(p^{-1}(A)\big) \cdot \big(p^{-1}(B)\big)^{-1}$, esto es la intersección de un conjunto discreto con un compacto y por lo tanto debe ser finito.

(1) $\Rightarrow$ (2): Sea V un abierto de G con clausura compacta. Por la parte (1) aplicada a los compactos $\overline{V} \cdot x_0$ y $\{x_0\}$ en X, existen finitos $\gamma \in \Gamma$ tales que $\gamma \cdot x_0 \in \overline{V} \cdot x_0$. En particular $\Gamma \cap \overline{V}$ es finito.

□

A partir del lema se puede probar lo siguiente:

PROPOSICIÓN 1.4. *Sean* G, K, X *y* Γ *como antes, con* Γ *discreto.*

1. *Para todo* $x \in X$, $\{\gamma \in \Gamma : x = \gamma x\}$ *es finito.*

2. *Para todo $x \in X$ existe un entorno U de x tal que $U \cap \gamma U \neq \emptyset$ solo si $x = \gamma x$.*
3. *Para todos $x \neq y \in X$ no en la misma órbita por G existen entornos U, V de x e y respectivamente tales que $\gamma U \cap V = \emptyset$ para todo $\gamma \in \Gamma$.*

Observación 1.1. *La parte (1) es inmediata y se deduce solo del hecho de que K es compacto y Γ discreto. La parte (2) implica que, en el caso en que Γ actúa libremente en X, la proyección $p : X \to \Gamma\backslash X$ es un homeomorfismo restringido a cada uno de los trasladados γU, los cuales son disjuntos. Esto significa que (X, p) es un* ***espacio de cubrimiento*** *de $\Gamma\backslash X$. En particular, cuando X es simplemente conexo, por ejemplo si $X = \mathbb{H}$, entonces X es el* ***cubrimiento universal*** *de $\Gamma\backslash X$. La parte (3) dice que el espacio $\Gamma\backslash X$ es Hausdorff.*

Lema 1.2. *Sea G un grupo que actúa continua y transitivamente sobre X. Si G y X son localmente compactos y existe una base numerable para la topología de G, entonces el mapa*

$$gK \mapsto g \cdot x_0$$

es un homeomorfismo $G/K \cong X$.

Para una demostración del lema anterior ver [Mil17, Capítulo 1].

Corolario 1.1. *Sea Γ un subgrupo discreto de $\mathrm{SL}_2(\mathbb{R})$. El espacio $\Gamma\backslash\mathbb{H}$ es Hausdorff.*

Prueba. Alcanza con mostrar que se verifican las hipótesis del lema y la proposición anteriores. Verificamos que:

- El grupo $\mathrm{SL}_2(\mathbb{R})$ actúa transitivamente sobre $\mathbb{H}$: tomar $z = x + yi \in \mathbb{H}$ con x, y reales, $y > 0$. La transformación $\alpha = \frac{1}{\sqrt{y}} \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ lleva i en z.
- El estabilizador de i en $\mathrm{SL}_2(\mathbb{R})$ es compacto: las matrices en $\mathrm{SL}_2(\mathbb{R})$ que fijan i son aquellas cuyos coeficientes a, b, c, d satisfacen

$$\frac{ai + b}{ci + d} = i, \qquad ad - bc = 1,$$

que es equivalente a

$$\begin{aligned} a &= d, \\ b &= -c, \end{aligned} \qquad a^2 + b^2 = 1,$$

lo que define el grupo especial ortogonal

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} : \theta \in \mathbb{R} \right\} \cong \mathbb{R}/\mathbb{Z}.$$

Este grupo es compacto.

□

3. Estructura compleja

DEFINICIÓN 1.4. *Una superficie de Riemann es un espacio Hausdorff X junto con:*

1. *Una familia de abiertos U_α que cubren X.*
2. *Para cada α, un homeomorfismo $\psi_\alpha : U_\alpha \to \tilde{U}_\alpha$ donde $\tilde{U}_\alpha$ es un abierto de $\mathbb{C}$. Los ψ_α deben cumplir que, si $\tilde{U}_\alpha \cap \tilde{U}_\beta \neq \emptyset$, entonces el mapa $\psi_\alpha \circ \psi_\beta^{-1}$ es holomorfo en su dominio de definición, en cuyo caso ψ_α y ψ_β se dicen compatibles.*

Los pares (ψ_α, U_α) se llaman cartas de X. Una función $f : V \to \mathbb{C}$ en una superficie de Riemann es holomorfa si $f \circ \psi_\alpha^{-1} : \psi_\alpha(U_\alpha \cap V) \to \mathbb{C}$ lo es para todo ψ_α.

EJEMPLO 1.1. *La Esfera de Riemann (definición 1.2), $\mathbb{C} \cup \{\infty\}$, admite una estructura compleja dada por:*

1. *Dos abiertos,*

$$U_1 = \mathbb{C}, \qquad U_2 = \mathbb{C} \cup \{\infty\} - \{0\}.$$

2. *Dos homeomorfismos,*

$$\begin{aligned} \psi_1 : U_1 \to \mathbb{C}, & \qquad \psi_2 : U_2 \to \mathbb{C}, \\ \psi_1(z) = z, & \qquad \psi_2(z) = 1/z. \end{aligned}$$

Los mapas ψ_1 y ψ_2 son compatibles, ya que $\psi_1 \circ \psi_2^{-1}$ y $\psi_2 \circ \psi_1^{-1}$ son ambos iguales a $1/z$ en su dominio de definición, $\mathbb{C} - \{0\}$.

Las funciones holomorfas en la esfera de Riemann son las constantes, por el teorema de Liouville. Para una función f, ser holomorfa en el infinito significa que $f(1/z)$ es holomorfa en un entorno del cero, y en particular implica que f es acotada en un abierto de complemento compacto.

EJEMPLO 1.2. *Sea Γ un subgrupo discreto de $\mathrm{SL}_2(\mathbb{R})$ que actúa libremente sobre $\mathbb{H}$. El espacio $\Gamma\backslash\mathbb{H}$ es Hausdorff por el corolario 1.1. Como vimos, cada $x \in \mathbb{H}$ tiene un entorno U_x donde la proyección $p : \mathbb{H} \to \Gamma\backslash\mathbb{H}$ es un homeomorfismo. Tomemos los pares $(p|_{U_x}^{-1}, p(U_x))$ como cartas para dar a $\Gamma\backslash\mathbb{H}$ una estructura compleja. Con esta estructura, decir que una función f en $V \subset \Gamma\backslash\mathbb{H}$ sea holomorfa significa que la función $f \circ p$ es holomorfa en $p^{-1}(V) \subset \mathbb{H}$. En conclusión, la composición $f \mapsto f \circ p$ es una biyección entre las funciones holomorfas en V y las funciones holomorfas en $p^{-1}(V)$ invariantes por la acción del grupo.*

Trabajaremos luego con el subgrupo $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{SL}_2(\mathbb{R})$ de matrices con coeficientes enteros. Este grupo no actúa libremente sobre $\mathbb{H}$, pero los resultados recién vistos sobre grupos nos van a permitir eludir este problema.

PROPOSICIÓN 1.5 (Lema de Schwarz). *Sea f una función holomorfa en el disco $\mathbb{D} = \{z : |z| < 1\}$ tal que $f(0) = 0$ y $|f(z)| \leq 1$ para todo z en $\mathbb{D}$.*

1. *Para todo $z \in \mathbb{D}$ se tiene $|f(z)| \leq |z|$.*
2. *Si $|f'(0)| = 1$ o $|f(z)| = |z|$ para un $z \in \mathbb{D}$ entonces existe una constante γ con $|\gamma| = 1$ tal que $f(z) = \gamma z$ para todo $z \in \mathbb{D}$.*

PRUEBA. Sea $F : \mathbb{D} \to \mathbb{C}$ dada por

$$F(z) = \begin{cases} f'(0) & z = 0 \\ f(z)/z & z \neq 0 \end{cases}$$

Entonces F es una función holomorfa en el disco. Sea $D(r) = \{z : |z| \leq r\}$, $r < 1$. Por el principio del máximo para funciones holomorfas sabemos que:

- El valor absoluto de F en $D(r)$ alcanza su máximo en el borde $\{|z| = r\} \subset \mathbb{D}$.
- Si el máximo se alcanza en el interior de $D(r)$ entonces F es constante en $D(r)$.

La primera condición implica que existe z_r con $|z_r| = r$ tal que $|F(z)| \leq |f(z_r)|/|z_r| \leq 1/r$ para todo $z \in D(r)$. Tomando el límite $r \to 1$ se obtiene (1). Si $|f'(0)| = 1$ o $|f(z)| = |z|$ para algún z, significa que $|F|$ alcanza su máximo valor posible en el interior de algún $D(r)$ y deducimos (2).

□

En particular, si tanto f como su inversa son funciones holomorfas del disco, tenemos $|f(z)| \leq |z|$ y $|z| \leq |f(z)|$ para todo $z \in \mathbb{D}$. Luego f debe ser una rotación por (2). Obtenemos lo siguiente:

Corolario 1.2. *Los automorfismos del disco que fijan el origen son las rotaciones por un ángulo fijo.*

Ahora podemos probar la proposición 1.3.

Corolario 1.3. $\mathrm{Aut}(\mathbb{H}) \cong \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$.

Demostración. Sea $f \in \mathrm{Aut}(\mathbb{H})$. De la prueba del corolario 1.1 sabemos que existe $\alpha \in \mathrm{SL}_2(\mathbb{R})$ con $\alpha(i) = f(i)$. Por lo tanto, tomando la composición $\alpha^{-1} \circ f$, podemos asumir que $f(i) = i$. Consideramos el isomorfismo del semiplano superior en el disco,

$$\phi : \mathbb{H} \to \mathbb{D}, \qquad z \mapsto \frac{z - i}{z + i}\,.$$

El mapa $\phi \circ f \circ \phi^{-1}$ es un automorfismo del disco que fija el centro, y por el corolario anterior debe ser de la forma $z \mapsto e^{i\theta} z$, $\theta \in \mathbb{R}$. Entonces tenemos

$$\begin{aligned} f &= \phi^{-1} \circ e^{i\theta} \circ \phi\,, \\ &= \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}^{-1} \begin{pmatrix} e^{i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{pmatrix} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}, \\ &= \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}. \end{aligned}$$

La última matriz pertenece al estabilizador de i en $\mathrm{SL}_2(\mathbb{R})$. Esto prueba que todo automorfismo en $\mathbb{H}$ se escribe como la acción por un elemento de $\mathrm{SL}_2(\mathbb{R})$. Recíprocamente, toda matriz de $\mathrm{SL}_2(\mathbb{R})$ define una única transformación lineal en $\mathbb{C}^2$. La función correspondiente en el plano proyectivo (como función de las rectas que pasan por el origen) está definida a menos de un factor escalar, el cual solo puede ser 1 o -1 si nos restringimos a matrices con determinante igual a 1.

□

OBSERVACIÓN 1.2. *Generalmente nos referimos con cierta ambigüedad a los elementos de* $\mathrm{SL}_2(\mathbb{R})$ *sin distinguir si se trata de matrices o de transformaciones racionales en* $\mathbb{P}^1(\mathbb{C})$. *Sin embargo, estrictamente hablando, las transformaciones se identifican con elementos de* $\mathrm{SL}_2(\mathbb{R})/\{\pm I\}$. *Por ejemplo, la matriz* $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ *tiene orden* 4, *pero en* $\mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ *tiene orden* 2, *correspondiendo a la transformación* $z \mapsto -1/z$.

EJEMPLO 1.3. *Sea* Δ *un grupo finito que actúa sobre el disco unitario* $\mathbb{D}$ *fijando el centro, y tal que la acción por cada elemento de* Δ *es una función holomorfa en* $\mathbb{D}$. *Según el corolario anterior,* Δ *es isomorfo a un subgrupo finito del grupo de rotaciones*

$$\{z \mapsto e^{i\theta} z : \theta \in \mathbb{R}\} \cong \mathbb{R}/\mathbb{Z}.$$

Como los subgrupos finitos de $\mathbb{R}/\mathbb{Z}$ *son cíclicos,* Δ *es cíclico de orden* m *y es generado por* $z \mapsto \zeta z$, *donde* $\zeta^m = 1$. *La función* z^m *es invariante por esta acción y define un homeomorfismo* $\Delta\backslash\mathbb{D} \to \mathbb{D}$. *Usando este mapa como carta, podemos definir una estructura compleja en* $\Delta\backslash\mathbb{D}$. *Para todo abierto* $U \subseteq \Delta\backslash\mathbb{D}$,

$$\mathrm{Hol}(U) := \{f \circ z^m : f \in \mathrm{Hol}(\tilde{U})\}$$

donde $\tilde{U} \subseteq \mathbb{C}$ *es la imagen por* z^m *de* U. *De modo que las funciones holomorfas en* U *son funciones holomorfas de* z^m. *Éstas son precisamente las funciones holomorfas invariantes por* Δ.

Como comentario al margen, el cuerpo de funciones $\mathrm{Hol}(\Delta\backslash\mathbb{D})$ es el cuerpo de las series de potencias en z^m, mientras que $\mathrm{Hol}(\mathbb{D})$ son las series de potencias en z. El último cuerpo es una extensión de grado m del primero, lo que se corresponde con el hecho de que la proyección $\mathbb{D} \to \Delta\backslash\mathbb{D}$ es un mapa "m en 1".

EJEMPLO 1.4. *Sea* $X = \{z \in \mathbb{C} : \Im(z) > t\}$ *para algún* $t > 0$, *y sea* $h \in \mathbb{Z}$. *Definimos una acción de* $\mathbb{Z}$ *en* X *por* $n \cdot z = z + nh$. *Ahora extendemos* X *a un espacio* X^* *agregando un punto "*∞*". La topología es la misma en los puntos de* X, *y una base local en* ∞ *consiste de entornos de la forma* $\{z \in \mathbb{C} : \Im(z) > N\}$. *Entonces se puede extender la acción de* $\mathbb{Z}$ *en* X *a una acción continua en* X^* *imponiendo* $n \cdot \infty = \infty$.

La función

$$q(z) = \begin{cases} e^{2\pi i z/h} & z \in X \\ 0 & z = \infty \end{cases}$$

define un homeomorfismo de $\mathbb{Z}\backslash X^*$ *en el disco abierto de centro* 0 *y radio* $e^{-2\pi t/h}$, *el cual lleva la órbita*

$$\mathbb{Z} \cdot z = \{z + nh : n \in \mathbb{Z}\}$$

en $q(z)$.

Luego define una estructura compleja en $\mathbb{Z}\backslash X^*$.

Con esta estructura, las funciones holomorfas f *en* $\mathbb{Z}\backslash X^*$ *son aquellas que se escriben como* $f(z) = f^*(q(z))$ *donde* f^* *es una función holomorfa de* q. *Que* f *sea holomorfa en* ∞ *significa que* f^* *es holomorfa en* 0. *En particular* f *tiene una expansión de Fourier*

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i z n/h},$$

$$f^*(q) = \sum_{n=0}^{\infty} a_n q^n .$$

Concluimos esta sección enunciando el Teorema de Uniformización, que sirve como motivación del contenido estudiado hasta este punto.

TEOREMA 1.1. *Toda superficie de Riemann X es isomorfa al cociente de su cubrimiento universal $\tilde{X}$ por la acción holomorfa de un grupo discreto. Además, $\tilde{X}$ es isomorfo a una de las tres superficies simplemente conexas:*

1. *El plano complejo $\mathbb{C}$.*
2. *El semiplano superior $\mathbb{H}$.*
3. *La esfera de Riemann $\mathbb{C} \cup \{\infty\}$.*

4. Puntos Ramificados

Se señaló anteriormente que $\mathrm{SL}_2(\mathbb{Z})$ no actúa libremente sobre $\mathbb{H}$. En esta sección investigamos cómo y en qué puntos la acción deja de ser libre.

DEFINICIÓN 1.5. *Sean X un espacio topológico, Γ un grupo actuando en X, y $x \in X$ un punto con estabilizador no trivial en Γ. Decimos que x es un* ***punto ramificado*** *de $\Gamma\backslash X$.*

DEFINICIÓN 1.6. *Sea α una matriz en $\mathrm{SL}_2(\mathbb{R})$ diferente de $\pm I$. Si estudiamos su forma canónica de Jordan se distinguen dos casos:*

$$(i) \quad \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}, \ \lambda \neq \mu, \qquad (ii) \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

La matriz en (i) corresponde a la transformación $z \mapsto (\lambda/\mu)z$. A su vez la matriz en (ii) corresponde a la traslación $z \mapsto z + 1/\lambda$.

Si α es conjugada a una matriz de tipo (i), y $|\lambda/\mu| = 1$, decimos que α es ***elíptica****. Si es conjugada a una matriz de tipo (ii) decimos que es* ***parabólica****. También decimos que α es elíptica o parabólica como transformación racional en $\mathbb{P}^1(\mathbb{C})$ si lo es como matriz.*

DEFINICIÓN 1.7. *Sea Γ un subgrupo discreto de $\mathrm{SL}_2(\mathbb{R})$.*

- *Todo $z \in \mathbb{H}$ es un* ***punto elíptico*** *de Γ si es punto fijo de una transformación elíptica en Γ.*
- *Todo $s \in \{\infty\} \cup \mathbb{R}$ es una* ***cúspide*** *de Γ si es punto fijo de una transformación parabólica en Γ.*

Toda matriz elíptica, siendo diagonalizable y con valores propios distintos, admite un par de vectores propios conjugados $(z, 1)$, $(\bar{z}, 1)$, de modo que z y $\bar{z}$ son puntos fijos en $\mathbb{C}$. Exactamente uno de ellos pertenece a $\mathbb{H}$.

Si α es parabólica, tiene un solo vector propio (a, b) real. Si $b = 0$, ∞ es punto fijo y α es una traslación $z + h$; si $b \neq 0$, $a/b \in \mathbb{R}$ es punto fijo.

Observación 1.3. *Los transformaciones elípticas* ***no*** *son $z \mapsto cz$ para algún c. Esta transformación claramente no tiene puntos fijos en $\mathbb{H}$. Ambas transformaciones sí son conjugadas por matrices en $\mathrm{SL}_2(\mathbb{C})$ pero no por matrices en Γ.*

Observación 1.4. *Hemos visto que el estabilizador en Γ de todo punto es un grupo cíclico finito. Por lo tanto es generado por una transformación α de orden finito. Luego también tiene orden finito como matriz en $\mathrm{SL}_2(\mathbb{Z})$. Los valores propios deben ser raíces de la unidad. Se deduce que* ***los puntos ramificados de*** *$\Gamma\backslash\mathbb{H}$* ***son los puntos elípticos de*** *Γ.*

Ejemplo 1.5. *Sea $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. El estabilizador de i en $\mathrm{SL}_2(\mathbb{R})$ es*

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} : \theta \in \mathbb{R} \right\} \cong \mathbb{R}/\mathbb{Z}\,.$$

Su intersección con Γ es

$$\mathrm{Est}(i,\Gamma) = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}.$$

Es generado por la matriz elíptica $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ (congruentes en $\mathrm{GL}_2(\mathbb{C})$).

Las transformaciones elípticas en Γ son matrices que tienen como valores propios raíces de la unidad. Como los valores propios además son raíces del polinomio característico, viven en una extensión cuadrática de $\mathbb{Q}$. Los únicos números que satisfacen estas condiciones son $1, i, \rho, \rho^2$, donde $\rho = \frac{1}{2} + i\frac{\sqrt{3}}{2}$.

La matriz $\left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ tiene valores propios $\rho, \bar{\rho}$. Como transformación racional (en $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$) tiene orden 3. Los vectores propios son $(\rho, 1)$, $(\bar{\rho}, 1)$, entonces $\rho \in \mathbb{H}$ es punto elíptico.

De hecho, i y ρ son los únicos puntos elípticos para $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, a menos de traslación por elementos de Γ. Vamos a probar esta afirmación como parte de un resultado más general, pero antes introducimos un poco de terminología:

Definición 1.8. *Un* ***dominio fundamental*** *para Γ subgrupo discreto de $\mathrm{SL}_2(\mathbb{Z})$ es un subconjunto D abierto conexo de $\mathbb{H}$ tal que ningún par de puntos en D son Γ-equivalentes, y tal que $\mathbb{H} = \bigcup_{\gamma\in\Gamma} \gamma\bar{D}$. Esto es igual a decir que la proyección $\mathbb{H} \to \Gamma\backslash\mathbb{H}$ es inyectiva restringida a D y sobreyectiva restringida a $\bar{D}$.*

Proposición 1.6. *Sean*

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad Sz = -1/z\,,$$

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad Tz = z + 1\,,$$

$$D = \{z \in \mathbb{H} : \ |z| > 1, \ \ |Re(z)| < 1/2\}\,,$$

$$\rho = \frac{1}{2} + i\frac{\sqrt{3}}{2}\,, \qquad \rho^2 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}\,.$$

1. *El conjunto D es un dominio fundamental para $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. Dos elementos distintos $z, z' \in \bar{D}$ son equivalentes por $\Gamma(1)$ exactamente en alguna de las siguientes condiciones:*
   a) $z' = z \pm 1\,, \qquad \Re(z) = \pm 1/2\,.$
   b) $z' = -1/z\,, \qquad |z| = 1\,.$
2. *Sea $z \in \bar{D}$. Si el estabilizador de z es distinto de $\{\pm I\}$ entonces*
   a) $z = i\,,$ $\mathrm{Est}(z) = \langle S\rangle$ *tiene orden 2 en* $\Gamma(1)/\{\pm I\}$.
   b) $z = \rho\,,$ $\mathrm{Est}(z) = \langle TS\rangle$ *tiene orden 3 en* $\Gamma(1)/\{\pm I\}$.
   c) $z = \rho^2\,,$ $\mathrm{Est}(z) = \langle ST\rangle$ *tiene orden 3 en* $\Gamma(1)/\{\pm I\}$.
3. *El grupo $\Gamma(1)$ es generado por S, T.*

Prueba. Sea Γ' el subgrupo de $\Gamma(1)$ generado por T y S. Sabemos que, para $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma'$ y $z \in \mathbb{H}$, $\Im(\gamma z) = \Im(z)/|cz+d|^2$.

Sea $\gamma \in \Gamma'$ tal que $|cz+d|$ es mínimo, de modo que $\Im(\gamma z)$ es máximo. Llamemos z' a γz. Podemos asumir que $|\Re(z')| \leq 1/2$, ya que siempre podemos garantizar esto aplicando alguna potencia de la transformación T. Además tenemos $|z'| \geq 1$. De lo contrario, $\Im(Sz') = \dfrac{\Im(z')}{|z'|^2} > \Im(z')$ contradice la maximalidad de $\Im(z')$. Se deduce que $\mathbb{H} \subseteq \Gamma' \cdot \bar{D}$.

Ahora sean $z, z' \in \bar{D}$ equivalentes por $\Gamma(1)$, es decir $z' = \gamma z$ para un $\gamma \in \Gamma(1)$. Hay dos posibilidades: $\Im(z) \geq \Im(\gamma z)$, $\Im(z) \leq \Im(\gamma z)$. Supongamos que vale la última desigualdad. Esto implica $|cz+d| \leq 1$. Como $|z| \geq 1$, los únicos valores posibles de c son $-1, 0, 1$.

- $c = 0$:
$$|cz+d| = |d| \leq 1 \Rightarrow d = \pm 1$$
Luego $\gamma = \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ es una traslación. Como $z, z' \in \bar{D}$, $b = \pm 1$ y $\gamma = \pm T$.
- $c = 1$:
$$|z+d| \leq 1 \Rightarrow \begin{cases} d = 0 \\ d = -1, & z = \rho \\ d = 1, & z = \rho^2 \end{cases}$$
En los dos últimos casos, notar que de hecho $|z+d| = 1$, y por lo tanto z y z' tienen igual parte imaginaria. Si $z \neq z'$, la única posibilidad es que $\{z, z'\} = \{\rho, \rho^2\}$, y se satisface la parte (1). Si son iguales, entonces $\gamma \in \mathrm{Est}(\rho)$ o $\gamma \in \mathrm{Est}(\rho^2)$.
Cuando $d = 0$, entonces $\gamma = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} \Rightarrow \gamma z = a - 1/z$. Necesariamente $|z| = 1$. Hay tres posibilidades para a:
$$\begin{cases} a = 0, & |z| = 1, \quad \gamma = S \\ a = 1, & z = \rho = z', \quad \gamma = TS \\ a = -1, & z = \rho^2 = z', \quad \gamma = ST \end{cases}$$
- $c = -1$: Se resuelve de forma similar.

Esto prueba las partes (1) y (2).

Ahora sea $\alpha \in \Gamma(1)$ y $z \in \bar{D}$. Existe $z' \in \bar{D}$ tal que $\alpha z = \gamma z'$, con $\gamma \in \Gamma'$. Notar que z y z' son equivalentes por $\Gamma(1)$:

$$\begin{aligned} z = (\alpha^{-1}\gamma)z' &\Rightarrow \alpha^{-1}\gamma \in \Gamma' \\ &\Rightarrow \alpha \in \Gamma' \end{aligned}$$

□

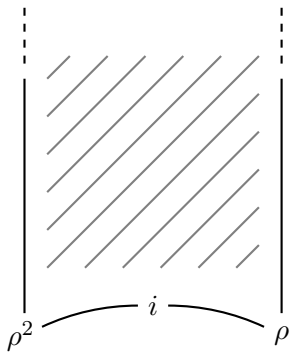


FIGURA 1. Dominio fundamental de $\Gamma(1)$

5. La curva X(1)

Llamemos $\Gamma(1)$ al grupo modular $\mathrm{SL}_2(\mathbb{Z})$. En los puntos donde $\Gamma(1)$ actúa libremente podemos definir una carta como en el ejemplo 1.2. Los únicos puntos de $\mathbb{H}$ con estabilizador no trivial son los puntos elípticos: i, ρ, y sus trasladados por elementos de Γ. Consideremos la transformación racional

$$\phi : \mathbb{H} \to \mathbb{D}, \quad z \mapsto \frac{z-i}{z+i}, \quad i \mapsto 0.$$

El estabilizador de i es generado por $S(z) = -1/z$. Como transformación racional, S tiene orden 2 e induce un automorfismo $\phi \circ S \circ \phi^{-1}$ de orden 2 en el disco $\mathbb{D}$, el cual se deduce que debe ser la rotación de 180 grados $z \mapsto -z$. El siguiente diagrama conmutativo ilustra la situación.

$$\begin{array}{ccc} \mathbb{H} & \xrightarrow{S} & \mathbb{H} \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ \mathbb{D} & \xrightarrow{-z} & \mathbb{D} \end{array}$$

Por la parte (2) de la proposición 1.4, podemos tomar un entorno U de i suficientemente pequeño tal que $\gamma U \cap U \neq \emptyset \iff \gamma \in \{I, S\}$. Es decir que $x, y \in U$ son equivalentes por $\Gamma(1)$ si y solo si $x = S(y)$ o $x = y$. Si llamamos G al grupo $\{I, S\} \cong \mathbb{Z}/2\mathbb{Z}$ entonces en U las órbitas por $\Gamma(1)$ coinciden con las órbitas por G.

Sea p la proyección $\mathbb{H} \to \Gamma(1)\backslash\mathbb{H}$. Mirando el diagrama, el mapa $z^2 \circ \phi$ es invariante por S en U e induce una función continua en el cociente $G\backslash U = \Gamma(1)\backslash U = V$,

$$\Gamma(1)\cdot z \mapsto \left(\frac{z-i}{z+i}\right)^2,$$

la cual es un homeomorfismo sobre un abierto $\tilde{V} \subseteq \mathbb{D}$. Elegimos esta función como carta $V \to \tilde{V}$.

El punto ρ tiene estabilizador de orden 3 y se trata similarmente, obteniendo la carta

$$\Gamma(1)\cdot z \mapsto \left(\frac{z-\rho}{z-\bar{\rho}}\right)^3.$$

La superficie de Riemann obtenida de $\Gamma(1)\backslash\mathbb{H}$ es un ejemplo de una *curva modular* y se llama $Y(1)$. Esta superficie no es compacta, pero se la puede compactificar agregando un punto, la órbita de ∞. Sea $\mathbb{H}^* = \mathbb{H} \cup \{\infty\}$, con la topología definida en el ejemplo 1.4, y consideremos la superficie $X(1) = \Gamma(1)\backslash\mathbb{H}^*$. El estabilizador de ∞ en $\Gamma(1)$ es el subgrupo de matrices con coeficiente c igual a cero:

$$\mathrm{Est}(\infty, \Gamma(1)) = \left\{ \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\} = \left\{ T^b : b \in \mathbb{Z} \right\} \cong \mathbb{Z}\,.$$

A continuación identificamos $\mathrm{Est}(\infty, \Gamma(1))$ con $\mathbb{Z}$. Existe un entorno U de ∞ donde las $\mathbb{Z}$-órbitas son iguales a las $\Gamma(1)$-órbitas, es decir, tal que $\Gamma(1)\backslash U = \mathbb{Z}\backslash U$. La función

$$q(z) = \begin{cases} e^{2\pi i z} & z \in X \\ 0 & z = \infty \end{cases}$$

induce un homeomorfismo $V = \Gamma(1)\backslash U \cong \tilde{V} \subseteq \mathbb{D}$, dado por

$$\Gamma(1)\cdot z \mapsto q(z).$$

Un dominio fundamental de $X(1)$ es $D \cup \{\infty\}$, donde D es un dominio fundamental de $X(1)$, como el visto en la proposición 1.6. Ahora $X(1)$ es un cociente de $\bar{D} \cup \{\infty\}$, por lo que es compacto.

Proposición 1.7. *La superficie $X(1)$ es homeomorfa a una esfera.*

Prueba. Esto se deduce a partir de la forma en que se pegan los bordes de D. Notar que las lineas verticales $\Re(z) = \pm 1/2$ se intersectan en ∞. Esto es evidente ya que las imágenes por $e^{2\pi i z}$ de todo par de lineas verticales en $\mathbb{C}$ es un par de líneas en el disco las cuales se intersectan en el origen. Por lo tanto podemos pensar en D como un triángulo.

La prueba de 1.6 muestra que dos elementos del borde de D son equivalentes por $\Gamma(1)$ si y solo si son simétricos respecto al eje imaginario. La figura 2 muestra el sentido en el que se pega el borde con esta simetría. El resultado es una superficie homeomorfa a una esfera.

□

La esfera S^2 es simplemente conexa, y el Teorema de Uniformización 1.1 nos dice que la única superficie de Riemann compacta y simplemente conexa es la esfera de Riemann. Por lo tanto se tiene un resultado más fuerte:

Corolario 1.4. *$Y(1)$ es isomorfa a la esfera de Riemann.*

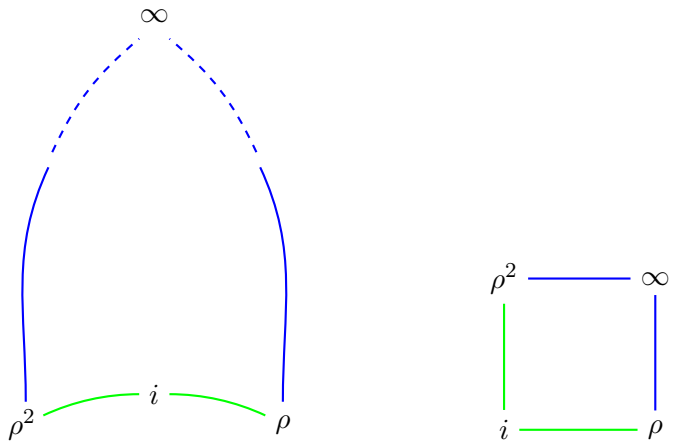


FIGURA 2.

6. Subgrupos de $\Gamma(1)$

Sea Γ un subgrupo de $\Gamma(1)$ índice finito. La superficie $Y(\Gamma) = \Gamma\backslash\mathbb{H}$ se define de forma similar a cuando $\Gamma = \Gamma(1)$. Agregando una cantidad finita de puntos, podemos hacer que esta superficie sea compacta.

PROPOSICIÓN 1.8. *La órbita de ∞ por $\Gamma(1)$ es $\mathbb{Q} \cup \{\infty\} = \mathbb{P}^1(\mathbb{Q})$.*

PRUEBA. Los elementos de la órbita de ∞ son de la forma

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \infty = \frac{a}{c} \in \mathbb{Q}\,.$$

Recíprocamente, si $a/c \in \mathbb{Q}$ con a, c enteros coprimos, existen $b, d \in \mathbb{Z}$ tales que $ad - bc = 1$, es decir,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) = \mathrm{SL}_2(\mathbb{Z}).$$

□

Ahora definimos $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. Para todo elemento $\sigma\infty \in \mathbb{Q}$ con $\sigma \in \Gamma$, definimos los entornos de $\sigma\infty$ como la imagen por σ de los entornos de ∞, de modo que σ sea un homeomorfismo. La superficie $X(\Gamma) = \Gamma\backslash\mathbb{H}^*$ es la unión de $\Gamma\backslash\mathbb{H}$ con las clases de Γ-equivalencia en $\mathbb{Q} \cup \{\infty\}$. Cuando $\Gamma = \Gamma(1)$ se agrega un solo punto a $\Gamma(1)\backslash\mathbb{H}$ y esto coincide con la definición de $X(1)$. El conjunto de cúspides de Γ es el mismo que para $\Gamma(1)$, aunque se puede partir en una cantidad finita de Γ-órbitas.

La razón de que las cúspides sean las mismas en Γ es que las transformaciones parabólicas tienen orden infinito, mientras que Γ tiene índice finito, luego contiene alguna potencia de cada transformación parabólica.

PROPOSICIÓN 1.9 (Carta en el infinito). *Sea h el menor entero positivo tal que $T^h \in \Gamma$. La función $q(z) = \exp(2\pi i/h)$, extendida continuamente a $q(\infty) = 0$, define un homeomorfismo de $\Gamma\backslash V^*$ en el disco abierto con centro en el origen y radio $e^{-2\pi/h}$, donde $V^* = \{w \in \mathbb{H} : \Im(w) > 1\} \cup \{\infty\}$.*

PRUEBA. Existe un entorno W de ∞ donde las Γ-órbitas coinciden con las órbitas por el estabilizador de ∞, el cual es cíclico generado por T^h. El entorno

$$W = V^* = \{w \in \mathbb{H} : \Im(w) > 1\} \cup \{\infty\}$$

satisface esta condición. La acción de Γ en V^* es igual a la acción de $\mathbb{Z}$ descrita en el ejemplo (1.4).

□

PROPOSICIÓN 1.10. *Sean Γ un subgrupo discreto de $\mathrm{SL}_2(\mathbb{R})$ y Γ' un subgrupo de Γ de índice finito. Sean γ_1, γ_2,..., $\gamma_m \in \gamma$ tales que*

$$\Gamma = \Gamma'\gamma_1 \cup \Gamma'\gamma_2 \cup ... \cup \Gamma'\gamma_m \quad \textit{(unión disjunta)}$$

Si D es un dominio fundamental de Γ, entonces

$$D' = \Gamma'\gamma_1 D \cup \Gamma'\gamma_2 D \cup ... \cup \Gamma'\gamma_m D$$

es un dominio fundamental para Γ', posiblemente no conexo.

De hecho, siempre se pueden elegir los γ_i de modo que D' sea conexo.

COROLARIO 1.5. *La superficie $X(\Gamma) = \Gamma\backslash\mathbb{H}^*$ es compacta.*

PRUEBA. Un dominio fundamental D' de Γ se puede escribir como unión finita de dominios fundamentales para $\Gamma(1)$, cada uno con clausura compacta. Entonces la clausura de D' es compacta. Su imagen por la proyección $\mathbb{H}^* \to \Gamma\backslash\mathbb{H}^*$ es sobreyectiva.

□

DEFINICIÓN 1.9. *Se define el **subgrupo de congruencia principal de** $\Gamma(1)$ **de nivel N** como el kernel de la reducción módulo N,*

$$\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \,:\, a \equiv d \equiv 1,\ b \equiv c \equiv 0 \ mod\ N \right\}.$$

*Se dice que un subgrupo de $\Gamma(1)$ es **de congruencia** si contiene a $\Gamma(N)$, para algún N. Si N es el menor entero con esta propiedad, el subgrupo se dice de congruencia **de nivel N**.*

*Se define la **curva modular de nivel N***

$$X(N) = \Gamma(N)\backslash\mathbb{H}$$

así como su compactificación

$$Y(N) = \Gamma(N)\backslash\mathbb{H}^* = X(N) \cup \{\Gamma(N) \cdot \gamma\infty : \gamma \in \Gamma(1)\}.$$

Por el teorema del isomorfismo, $\Gamma(1)/\Gamma(n) \cong SL_2(\mathbb{Z}/n\mathbb{Z})$ para cada n. El orden del último grupo es finito, por lo que $\Gamma(n)$ tiene índice finito en $\Gamma(1)$.

EJEMPLO 1.6. *El subgrupo $\Gamma(2)$ tiene índice 6 en $\Gamma(1)$. Está generado por las matrices de la forma*

$$\pm \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix}.$$

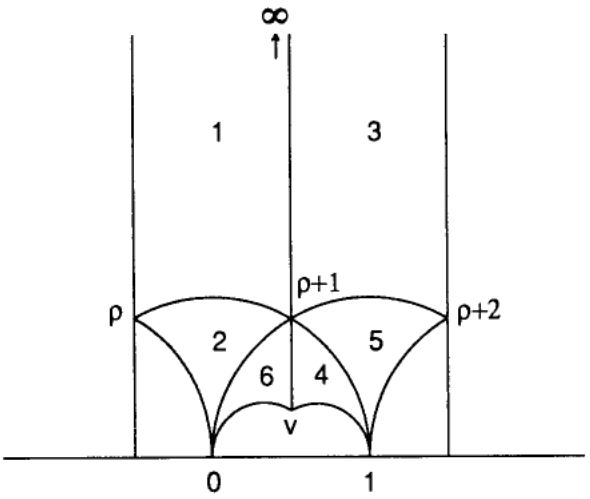


FIGURA 3. Imagen tomada del libro de S. Katok, *Fuchsian groups*.

Estas matrices son parabólicas (tienen traza igual a 2), por lo que no hay puntos elípticos para $\Gamma(2)$. *Existen tres cúspides no equivalentes:*

- ∞.
- $S(\infty) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$.
- $TS(\infty) = T(0) = 1$.

Un dominio fundamental de $Y(2) = \Gamma(2)\backslash\mathbb{H}^*$ *consiste de 6 copias de un dominio fundamental de* $Y(1)$, *una por cada coclase de* $\Gamma(2)$ *en* $\Gamma(1)$.

El segmento $[0, \rho]$ *tiene imagen* $[0, v]$ *por la transformación* $ST^{-2}S \in \Gamma(2)$. *A su vez,* $[1, \rho + 2]$ *se pega con* $[1, v]$, *y los segmentos* $[\infty, \rho]$, $[\infty, \rho + 2]$ *son equivalentes por* $z \pm 2$. *La superficie resultante es topológicamente una esfera.*

Capítulo 2

Funciones elípticas

1. Preliminares de curvas elípticas

DEFINICIÓN 2.1. *Llamamos* ***curva de Weierstrass*** *al conjunto de soluciones de una ecuación de la forma*

$$y^2 = x^3 + ax + b \tag{2}$$

sobre un cuerpo k dado, con $a, b, x, y \in k$.[1] *Se asume además que las raíces del polinomio en x del lado derecho son todas distintas en la clausura algebraica de k.*

Si $Ax+By = C$ es una recta, entonces combinando su ecuación con (2) obtendríamos en general un polinomio cúbico en x. Por lo tanto podríamos decir que, en la clausura algebraica $\bar{k}$, toda recta intersecta a una curva elíptica en tres puntos, contando multiplicidades. Además si dos de esos tres puntos tienen coordenadas en k, entonces lo mismo vale para el tercero.

Solo hay un problema con la afirmación anterior, y sucede cuando intersectamos la curva con una recta vertical $x = x_0$. En este caso la ecuación se transforma en $y^2 = c$ y deja de ser cúbica: tiene dos soluciones $(x_0, \pm\sqrt{c})$ en vez de tres. Sin embargo, la afirmación es cierta en el plano proyectivo:

DEFINICIÓN 2.2. *Sea $E/k : y^2 = x^3 + ax + b$ una curva de Weierstrass definida sobre el cuerpo k. Se llama* ***curva elíptica*** *al conjunto de soluciones de la homogeneización*

$$y^2 z = x^3 + axz^2 + bz^3, \tag{3}$$

en el plano proyectivo $\mathbb{P}^2(k)$.

OBSERVACIÓN 2.1. *En el plano afín $\{(x : y : z) \ : \ z \neq 0\}$, podemos dividir por z^3 para recuperar la ecuación (2) en coordenadas proyectivas:*

$$(y/z)^2 = (x/z)^3 + a(x/z) + b\,.$$

Por lo tanto las soluciones son las mismas cuando $z \neq 0$, y cuando $z = 0$ obtenemos una solución extra a (3): el punto $\mathcal{O} = (0 : 1 : 0)$, i.e: $x = 0 = z$, $y \neq 0$.

En vista de la oservación anterior, vamos a hablar de una curva elíptica $E : y^2 = x^3 + ax + b$ como una curva en $k \times k$ con un punto "en el infinito", aunque en realidad la curva vive en $\mathbb{P}^2(\bar{k})$.

[1] La ecuación general de una curva elíptica tiene más términos, pero puede convertirse a la forma $y^2 = x^3 + ax + b$ si el cuerpo tiene característica mayor a 3.

DEFINICIÓN 2.3. *Por **recta proyectiva** en $\mathbb{P}^2(k)$ nos referimos al conjunto de raíces en $\mathbb{P}^2(k)$ de un polinomio homogéneo de grado 1 en $k[x, y, z]$.*

OBSERVACIÓN 2.2. *Notar que si $z \neq 0$, las rectas proyectivas se transforman en rectas afines $A(x/z) + B(y/z) = C$, y cuando $z = 0$ hay un punto más: la dirección $(-B : A : 0)$. En particular, las rectas verticales $Ax = Cz$ cortan a toda curva elíptica en el punto $\mathcal{O}$.*

Hemos obtenido el siguiente resultado:

PROPOSICIÓN 2.1. *Sea E/k una curva elíptica sobre un cuerpo k. Si k es algebraicamente cerrado, toda recta proyectiva intersecta a E en exactamente tres puntos, contando multiplicidades. Si k no es algebraicamete cerrado pero dos puntos de la intersección tienen coordenadas en k, entonces el tercer punto también.*

Una propiedad interesante de las curvas elípticas es la siguiente, que no vamos a probar:

PROPOSICIÓN 2.2. *Se puede definir una operación de suma en toda curva elíptica de modo que:*

1. *El elemento neutro es $\mathcal{O}$.*
2. *Tres puntos colineales suman $\mathcal{O}$.*

Dijimos que las rectas verticales intersectan a la curva en $\mathcal{O}$ y en dos puntos $(x, \pm y)$, por lo que

$$(x, y) + \mathcal{O} + (x, -y) = \mathcal{O},$$

y necesariamente

$$-(x, y) = (x, -y).$$

Si $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ son dos puntos de la curva, sea R el tercer punto de intersección de la curva con la recta que los une. Cuando $P = Q$ se toma la recta tangente a la curva en el punto.

$$P + Q + R = 0 \implies P + Q = -R.$$

Se define la suma

$$P + Q = \begin{cases} (x_3, -y_3) & \text{si } R = (x_3, y_3) \\ \mathcal{O} & \text{si } R = \mathcal{O} \end{cases}$$

Es decir, la suma es el opuesto del tercer punto de intersección. Con esta operación, la curva elíptica es un grupo abeliano con elemento neutro $\mathcal{O}$. Verificar esto es sencillo excepto por la asociatividad, pero en definitiva se sigue de usar la definición y hacer cuentas.

PROPOSICIÓN 2.3 (fórmula de la suma). *Sea $y^2 = x^3 + ax + b$ una curva de Weierstrass, y sean $P = (x_1, y_1)$, $Q = (x_2, y_2)$ dos puntos en la curva, con $x_1 \neq x_2$. La suma $(x_3, y_3) = P + Q$ está dada por*

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2,$$
$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1.$$

PRUEBA. Sea $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$. Los puntos P y Q definen la recta $Y = \lambda X - \lambda x_1 + y_1$. Sustituyendo en la ecuación,

$$-(\lambda X - \lambda x_1 + y_1)^2 + X^3 + aX + b = 0.$$

Sabemos que x_1, x_2 son raíces. La suma de todas las raíces es menos el coeficiente en X^2, esto es λ^2. Luego,

$$x_3 = \lambda^2 - x_1 - x_2.$$

Entonces el punto (x_3, y') pertenece también a la recta, donde

$$y' = \lambda x_3 - \lambda x_1 + y_1.$$

Finalmente

$$y_3 = -y' = \lambda(x_1 - x_3) - y_1.$$

□

2. Retículos y bases

Sean $\omega_1, \omega_2 \in \mathbb{C}$ tales que $\tau = \omega_1/\omega_2 \notin \mathbb{R}$. El par ordenado $\{\omega_1, \omega_2\}$ es una base de $\mathbb{C}$ como $\mathbb{R}$-espacio vectorial. Intercambiando ω_1 y ω_2 si es necesario podemos asumir que ω_1/ω_2 pertenece al semiplano superior. El *retículo* generado por ω_1, ω_2 es el subgrupo aditivo

$$\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}.$$

Otro par $\omega_1', \omega_2' \in \Lambda$,

$$\begin{aligned} \omega_1' &= a\omega_1 + b\omega_2 \\ \omega_2' &= c\omega_1 + d\omega_2 \end{aligned} \qquad a, b, c, d \in \mathbb{Z}$$

es una base si y solo si $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1$

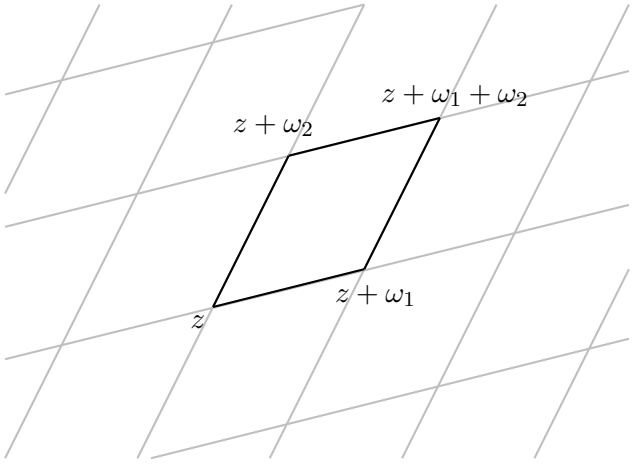
Además $\tau' = \omega_1'/\omega_2'$ tiene parte imaginaria dada por

$$\Im(\tau') = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{\Im(\tau)}{|\, c\tau + d\,|^2}$$

Por lo tanto las bases ordenadas $\{\omega_1', \omega_2'\}$ de Λ son aquellas de la forma

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

DEFINICIÓN 2.4. *Si $\{\omega_1, \omega_2\}$ es base de Λ y $z \in \mathbb{C}$ el paralelogramo con vértices z, $z+\omega_1$, $z+\omega_2$, $z+\omega_1+\omega_2$ es un* ***paralelogramo fundamental*** *de Λ.*



DEFINICIÓN 2.5 (Toro complejo $\mathbb{C}/\Lambda$). *El cociente $\mathbb{C}/\Lambda$ se define como el conjunto de clases de la equivalencia*

$$\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}$$

Equivalentemente, es el conjunto de órbitas en $\mathbb{C}$ por la acción

$$\mathbb{C} \times \Lambda \to \mathbb{C} \qquad (z, \omega) \mapsto z + \omega$$

Sea $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ la proyección canónica $z \mapsto z + \Lambda$. Un subconjunto $V \subseteq \mathbb{C}/\Lambda$ es abierto si y solo si $\pi^{-1}(V)$ es abierto en $\mathbb{C}$. Con esta topología, π es continua y abierta. Notar que $\mathbb{C}/\Lambda$ es compacto al ser la imagen continua por π de un paralelogramo fundamental.

OBSERVACIÓN 2.3. *Topológicamente, $\mathbb{C}/\Lambda$ es un toro.*

Podemos dar a $\mathbb{C}/\Lambda$ una estructura de superficie de Riemann de la siguiente forma: sea $U \subseteq \mathbb{C}$ un abierto conexo tal que ningún par de puntos en U son equivalentes por Λ. El mapa π es un homeomorfismo restricto a U, y su inversa $\phi = \pi^{-1}$ es una carta. Las cartas definidas así son todas compatibles: sean V_1, V_2 dos abiertos en $\mathbb{C}/\Lambda$ y considero las cartas corresponidentes, $\phi_1 : V_1 \to \mathbb{C}$, $\phi_2 : V_2 \to \mathbb{C}$. Defino el mapa de transición,

$$\psi = \phi_2 \circ \phi_1^{-1} : \phi_1(V_1 \cap V_2) \to \phi_2(V_1 \cap V_2).$$

Para todo $z \in \phi_1(V_1 \cap V_2)$, $\psi(z) - z = C(z) \in \Lambda$, y como ψ es continua y Λ es discreto, $C(z) = C$ es constante y $\psi = z + C$ es biholomorfa.

PROPOSICIÓN 2.4. *Sean Λ, Λ' dos retículos en $\mathbb{C}$. Todo elemento $\alpha \in \mathbb{C}$ tal que $\alpha\Lambda \subseteq \Lambda'$ define un mapa holomorfo*

$$\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda', \qquad z + \Lambda \mapsto \alpha z + \Lambda'.$$

Además todo mapa holomorfo $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ es de esta forma para algún α.

PRUEBA. La primera parte es un ejercicio básico de álgebra. Supongamos que tenemos un mapa holomorfo $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$. Tenemos que $\mathbb{C}$ es el cubrimiento universal de $\mathbb{C}/\Lambda$ para todo Λ. Un resultado conocido de topología nos dice que entonces el mapa φ se levanta a un mapa continuo $\tilde{\varphi}$ tal que $\tilde{\varphi}(0) = 0$ y de forma que conmute el siguiente diagrama.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{\varphi}} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda & \xrightarrow{\varphi} & \mathbb{C}/\Lambda' \end{array}$$

Por definición, que φ sea holomorfa quiere decir que $\varphi \circ \pi = \tilde{\varphi}$ es holomorfa en $\mathbb{C}$. Para todo $\omega \in \Lambda$, la función $\tilde{\varphi}(z) - \tilde{\varphi}(z-\omega)$ es continua y toma valores en el conjunto discreto Λ, por lo tanto debe ser constante. Entonces la derivada de $\tilde{\varphi}$ debe ser doblemente periódica

$$\frac{d}{dz}\tilde{\varphi}(z) - \frac{d}{dz}\tilde{\varphi}(z-\omega) = 0$$

Siendo además holomorfa en todo $\mathbb{C}$, se deduce que $\frac{d}{dz}\tilde{\varphi}(z)$ es constante igual a un $\alpha \in \mathbb{C}$, y $\varphi(z) = \alpha z + \beta$. Tomando $z = 0$ se obtiene $\beta = 0$.

□

COROLARIO 2.1. *Dos toros complejos $\mathbb{C}/\Lambda$, $\mathbb{C}/\Lambda'$ son isomorfos si y solo si existe $\alpha \in \mathbb{C}$ tal que $\alpha\Lambda = \Lambda'$*

DEFINICIÓN 2.6. *Sea Λ un retículo en $\mathbb{C}$ y f una función meromorfa invariante por la suma de elementos de Λ, es decir*

$$f(z+\omega) = f(z) \quad \omega \in \Lambda$$

*Se dice que f es una **función doblemente periódica** con respecto a Λ. También se le llama a f **función elíptica**.*

OBSERVACIÓN 2.4. *Si f es una función doblemente periódica, entonces $\pi(z) = \pi(z') \implies f(z) = f(z')$. Por lo tanto f define una función $\tilde{f} : \mathbb{C}/\Lambda \to \mathbb{C}$ tal que $f = \tilde{f} \circ \pi$. Recíprocamente, una función $\tilde{f}$ es meromorfa en $\mathbb{C}/\Lambda$ si y solo si existe una f como antes (por definición). Las funciones meromorfas en $\mathbb{C}/\Lambda$ corresponden exactamente a las funciones meromorfas en $\mathbb{C}$ invariantes por la acción de Λ.*

LEMA 2.1. *Sea f una función meromorfa en una superficie de Riemann compacta S.*

1. *La cantidad de ceros de f es igual a su cantidad de polos, contando multiplicidades.*
2. *La suma de los residuos de f es cero.*

PRUEBA. Primero probamos (2). Sea γ una curva dentro de un abierto U isomorfo a un abierto de $\mathbb{C}$. De acuerdo al teorema de los residuos,

$$\int_\gamma f dz = 2\pi i \left(\sum_p \mathrm{Res}_p(f) \right),$$

donde la suma es sobre los polos encerrados por γ en U. Tiene sentido hablar del "interior"de la curva precisamente porque ésta vive en un entorno isomorfo a un subconjunto del plano complejo. Como la superficie es compacta se puede elegir un cubrimiento finito por cartas (ψ, U_ψ), y luego una triangulación de modo que cada triángulo está contenido en un U_ψ. Al integrar, los lados de los triángulos adyacentes se cancelan y se obtiene el resultado.

Para probar (1) se usa que el residuo de $f'(z)/f(z)$ en un punto es igual al orden de f en ese punto.

□

El siguiente corolario se va a usar extensamente en lo que sigue:

COROLARIO 2.2. *Sea f meromorfa en una superficie de Riemann compacta. Existe un $n > 0$ tal que f toma cada valor n veces (contando multiplicidades).*

PRUEBA. Tomar n igual al número de polos de f. Para cada $c \in \mathbb{C}$ la función $f(z) - c$ tiene n ceros. □

Llamamos a n el *grado* de f.

PROPOSICIÓN 2.5. *Sea f una función doblemente periódica respecto al retículo Λ. Elegir un paralelogramo fundamental D que no intersecte a las raíces ni a los polos de f. Las siguientes sumas son sobre los puntos en el interior de D.*

1. $\sum \mathrm{Res}_P(f) = 0$
2. $\sum \mathrm{ord}_P(f) = 0$
3. $\sum \mathrm{ord}_P(f) \cdot P = 0 \pmod{\Lambda}$

PRUEBA. Si consideramos a f como una función en $\mathbb{C}/\Lambda$, (1) y (2) son casos particulares del lema anterior. La parte (3) es un poco más delicada pero se obtiene de integrar la función $f'(z)/f(z)$ en el borde de un paralelogramo fundamental. □

COROLARIO 2.3. *Toda función doblemente periódica no constante tiene al menos dos polos.*

PRUEBA. Si f es doblemente periódica, la parte (1) de la proposición anterior implica que, o bien f no tiene polos, o tiene al menos dos. Si no tiene polos, entonces f es holomorfa en el paralelogramo fundamental, y en particular es acotada en $\mathbb{C}$. Del teorema de Liouville se deduce que f es constante en tal caso.

□

3. Una función doblemente periódica

El corolario anterior nos sugiere cómo podría verse el ejemplo más básico de función doblemente periódica: podríamos construir una función invariante por la acción de Λ y con un polo doble en cada punto del retículo,

$$f(z) = \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^2} \ ,$$

y esto va a ser una función meromorfa siempre y cuando la serie converja absolutamente en compactos fuera de Λ, es decir siempre que intercambiar el orden de los

términos no altere la suma. De hecho, una pequeña modificación en esta expresión resulta en una función doblemente periódica, la función $\wp$ de Weierstrass, pero para demostrarlo resulta más fácil trabajar con su derivada,

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

Proposición 2.6. *La serie que define a $\wp'(z)$ converge absolutamente para todo $z \notin \Lambda$.*

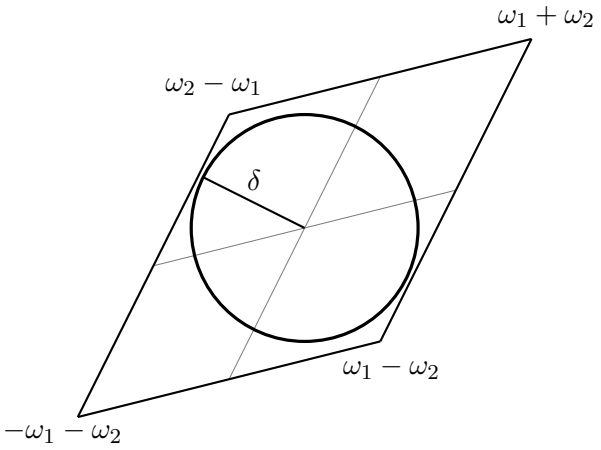
Prueba.

$$\begin{aligned}\frac{1}{|z|^3} + \sum_{\omega\in\Lambda-\{0\}} \frac{1}{|z-w|^3} &\leq \frac{1}{|z|^3} + \sum_{\omega\in\Lambda-\{0\}} \left(\frac{|w|}{|z-w|}\right)^3 \frac{1}{|w|^3} \\ &\leq \frac{1}{|z|^3} + \max_{\omega\in\Lambda-\{0\}} \left\{\left(\frac{|w|}{|z-w|}\right)^3\right\} \sum_{\omega\in\Lambda-\{0\}} \frac{1}{|w|^3} \\ &= \frac{1}{|z|^3} + K \sum_{\omega\in\Lambda-\{0\}} \frac{1}{|w|^3}\end{aligned}$$

Ahora consideremos el paralelogramo $\mathcal{P}$ con vértices $-\omega_1-\omega_2$, $\omega_1-\omega_2$, $-\omega_1+\omega_2$, $\omega_1+\omega_2$, y sea δ la distancia del origen al punto más cercano del borde $\partial\mathcal{P}$. Los conjuntos $(n\cdot\partial\mathcal{P})\cap\Lambda = \{nz : z\in\partial\mathcal{P}\}\cap\Lambda$, $n\geq 1$ forman una partición de $\Lambda-\{0\}$, y para cada n, la intersección $(n\cdot\partial\mathcal{P})\cap\Lambda$ tiene exactamente $4(2n-1)-4$ puntos. Entonces,

$$\sum_{\omega\in\Lambda-\{0\}} \frac{1}{|w|^3} \leq \sum_{n=1}^{\infty} \frac{1}{(n\delta)^3}(4(2n-1)-4) < \infty.$$

□



Ahora podemos definir

$$\wp(z) = \frac{1}{z^3} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

y $\wp$ es holomofa y doblemente periódica porque su derivada lo es.

PROPOSICIÓN 2.7. *El cuerpo de funciones doblemente periódicas está generado por $\wp$ y $\wp'$ sobre $\mathbb{C}$.*

PRUEBA. Sea f una funcion doblemente periódica y supongamos que además es una función par, i.e: $f(-z) = f(z)$. La derivada k-ésima cumple

$$f^{(k)}(z) = (-1)^k f^{(k)}(-z).$$

En particular, si f tiene un cero en z_0 y $z_0 \equiv -z_0 \bmod \Lambda$ entonces las derivadas de orden impar en z_0 y $-z_0$ se anulan y obtenemos que estos puntos son ceros de f de orden par. Reemplazando f por $1/f$ se obtiene un resultado igual para los polos de f.

Sean $z_1, z_2, ..., z_n$ representantes módulo Λ de los ceros y polos de f que no pertenecen a Λ.

$$\begin{array}{ll} z_i \not\equiv -z_i & 1 \leq i \leq m \\ z_i \equiv -z_i \not\equiv 0 & m < i \leq n \end{array}$$

La función $\wp(z) - \wp(z_i)$ tiene solo un polo doble en el origen cuando se la piensa como función en el cociente $\mathbb{C}/\Lambda$, por lo tanto tiene exactamente dos ceros. Cuando $i \leq m$ tiene dos ceros simples en $\pm z_i$, y cuando $i > m$ tiene un cero doble en $z_i \equiv -z_i$.

Si m_i es el orden de f en z_i, sea $g(z)$ dada por

$$g(z) = \prod_{1 \leq i \leq m} (\wp(z) - \wp(z_i))^{m_i} \prod_{1 \leq i \leq m} (\wp(z) - \wp(z_i))^{m_i/2}.$$

Como f y g tienen exactamente los mismos ceros y polos fuera de Λ, la proposición (2.5) implica que tienen el mismo orden en cada punto de Λ. La función f/g, al ser holomorfa y doblemente periódica, debe ser constante. Luego $f = cg \in \mathbb{C}(\wp)$.

Si f es impar, $\wp' \cdot f$ es par y pertenece a $\mathbb{C}(\wp)$, luego $f \in \mathbb{C}(\wp, \wp')$.

Ahora supongamos solamente que f es doblemente periódica. En dicho caso puede descomponerse como la suma de una función par y una impar:

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}$$

□

4. La curva elíptica E(Λ)

Como vimos en la sección anterior, las funciones doblemente periódicas están determinadas a menos de una constante por su comportamiento en los polos y ceros. Esto es cierto en general para las funciones meromorfas en una superficie de Riemann compacta, y las funciones doblemente periódicas pueden verse como funciones en la superficie

$\mathbb{C}/\Lambda$. Otra forma de caracterizar estas funciones es por los coeficientes de las potencias negativas de z en su expansión de Laurent. Por ejemplo, la función $\wp$ de Weierstrass es la única función doblemente periódica (a menos de una constante) que satisface la condicion de crecimiento

$$\wp(z) = \frac{1}{z^2} + O(z^2),$$

en un entorno del origen y que no tiene ningún otro polo. Si tuviéramos otra función f doblemente periódica y con las mismas condiciones, entonces $\wp - f$ sería holomorfa y tomaría el valor cero en el origen, luego sería idénticamente igual a cero en todo $\mathbb{C}$. Así, trabajando con las expansiones de Laurent, es fácil encontrar ecuaciones que relacionen dos funciones doblemente periódicas.

PROPOSICIÓN 2.8. *La función $\wp$ satisface la ecuación diferencial*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_2\wp(z) - 140G_3\,, \tag{4}$$

donde

$$G_k = \sum_{\omega\in\Lambda-\{0\}} \frac{1}{\omega^{2k}}.$$

PRUEBA.

$$\frac{1}{(z-w)^2} = \frac{1}{w^2} + \frac{2z}{w^3} + \frac{3z^2}{w^4} + ...$$
$$\frac{-2}{(z-w)^3} = \frac{2}{w^3} + \frac{6z}{w^4} + \frac{12z^2}{w^5} + \frac{20z^3}{w^6}...$$

Observar que $\sum \frac{1}{\omega^k} = 0$ para k impar, ya que si $\omega \in \Lambda$ entoces $-\omega \in \Lambda$ y $(-\omega)^{-k} + \omega^{-k} = 0$. Obtenemos las siguientes expansiones:

$$\wp(z) = \frac{1}{z^2} + 3z^2\sum\frac{1}{\omega^4} + 5z^4\sum\frac{1}{\omega^6} + O(z^6)$$
$$\wp'(z) = -\frac{2}{z^3} + 6z\sum\frac{1}{\omega^4} + 20z^3\sum\frac{1}{\omega^6} + O(z^5)$$

$$\wp(z)^3 = \frac{1}{z^6} + \frac{9}{z^2}\sum\frac{1}{\omega^4} + 15\sum\frac{1}{\omega^6} + O(z^2)$$
$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24}{z^2}\sum\frac{1}{\omega^4} - 80\sum\frac{1}{\omega^6} + O(z^2)$$

$$\begin{aligned}\wp'(z)^2 - 4\wp(z)^3 &= -\frac{60}{z^2}\sum\frac{1}{\omega^4} - 140\sum\frac{1}{\omega^6} + O(z^2)\\ &= -60G_2\frac{1}{z^2} - 140G_3 + O(z^2)\\ &= -60G_2\wp(z) - 140G_3 + O(z^2)\end{aligned}$$

La expresión

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_2\wp(z) + 140G_3$$

toma el valor cero cuando $z \in \Lambda$ y es holomorfa en un entorno de dichos puntos. Como además es holomorfa en el resto de $\mathbb{C}$ y es acotada, debe ser constante e igual a cero.

□

Una observación notable es que la ecuación (1) tiene la misma forma que la ecuación de una curva elíptica, con soluciones $(\wp(z), \wp'(z))$.

DEFINICIÓN 2.7. *Dado un retículo Λ, se llama $E(\Lambda)$ a la curva*

$$y^2 = 4x^3 - 60G_2x - 140G_3 \tag{5}$$

definida sobre los complejos. Los coeficientes G_2, G_3 dependen del retículo. Frecuentemente se escribe la ecuación (5) en forma más compacta

$$y^2 = 4x^3 - g_2x - g_3.$$

Si escribimos $x = \wp(z)$, entonces (1) implica que $y = \pm\wp'(z) = \wp'(\pm z)$. Las soluciones son

$$(x, y) = (\wp(z), \pm\wp'(z)) = (\wp(\pm z), \wp'(\pm z)).$$

Los puntos $\pm z$ son las raíces de $f(z) = \wp(z) - x$. Como f tiene solo un polo de orden dos mod Λ, entonces por el lema (2.1) tiene exactamente dos raíces en un paralelogramo fundamental.

Definimos el siguiente mapa $\mathbb{C}/\Lambda \to E(\Lambda)$,

$$\phi(z) = \begin{cases} (\wp(z), \wp'(z)) & z \neq 0, \\ \mathcal{O} & z = 0. \end{cases}$$

De la discusión de arriba es claro que es sobreyectivo.

LEMA 2.2. *El mapa ϕ es inyectivo.*

DEMOSTRACIÓN. La función $\wp'(z)$ tiene exactamente tres raíces en $\mathbb{C}$, ya que tiene un polo de orden tres. Además sabemos que si $z \equiv -z \bmod \Lambda$,

$$\wp'(z) = \wp'(-z) = -\wp'(z)$$

y entonces $\wp'(z) = 0$.

Hay solo tres puntos (mod Λ) conguentes son su opuesto. Éstos son

$$\omega_1/2, \quad \omega_2/2, \quad (\omega_1 + \omega_2)/2$$

donde ω_1, ω_2 es una base de Λ.

Entonces

$$\wp'(z) = 0 \iff z \equiv -z \bmod \Lambda.$$

Sea (x, y) un punto en la curva $E(\Lambda)$. Solo hay dos raíces $\pm z$ de $\wp(z) - x$. Si $z \not\equiv -z \mod \Lambda$, entonces $\wp'(z) \neq 0$ y $\wp'(-z) = -\wp'(z)$, por lo que $\phi(\pm z) = (x, \pm y)$ son distintos.

Solo falta ver que ϕ es inyectiva en los puntos de orden 2, i.e: $z \equiv -z$.

Dijimos que la ecuación $\wp(z) = x$ tiene solo dos raíces $\pm z$, pero si $z \equiv -z$ ésta es una raíz doble y no hay ninguna otra.

□

Por lo tanto el mapa $\phi(z)$ parametriza la curva $E(\Lambda)$.

LEMA 2.3. *Si tres puntos $\phi(z_1)$, $\phi(z_2)$, $\phi(z_3)$ en $E(\Lambda)$ pertenecen a una misma recta entonces*

$$z_1 + z_2 + z_3 \equiv 0 \quad \text{mód } (\Lambda).$$

PRUEBA. La función

$$\alpha\wp(z) + \beta\wp'(z) - \gamma \tag{6}$$

es doblemente periódica y tiene un polo de orden 3 en el origen si $\beta \neq 0$. Por lo tanto tiene exactamente tres raíces z_1, z_2, z_3 contando multiplicidades, que por la proposición (2.5) cumplen

$$z_1 + z_2 + z_3 \equiv 0 \mod \Lambda. \tag{7}$$

Ahora es inmediato el problema de encontrar el tercer punto de intersección dados otros dos. Si $P = (\wp(z_1), \wp'(z_1))$ y $Q = (\wp(z_2), \wp'(z_2))$ son dos puntos sobre la curva y $z_1 + z_2 \not\equiv 0 \mod \Lambda$, el punto $R = (\wp(-z_1 - z_2), \wp'(-z_1 - z_2)) = (\wp(z_1 + z_2), -\wp'(z_1 + z_2))$ es colineal con P y Q. Si $z_1 + z_2 \equiv 0$, entonces

$$\wp(z_1) = \wp(-z_2) = \wp(z_2),$$

es decir los puntos P y Q tienen igual coordenada x. En este caso, $\beta = 0$ y $\wp(z) = \gamma$ solo tiene dos raíces. Luego los únicos puntos de intersección son P, Q y $\mathcal{O} = \phi(0)$, y se cumple el enunciado del lema:

$$z_1 + z_2 + 0 \equiv 0\,.$$

□

TEOREMA 2.1. *La curva*

$$E(\Lambda): \quad y^2 = 4x^3 - (60G_2)x - 140G_3$$

es una curva elíptica sobre $\mathbb{C}$, cuyos puntos están parametrizados por el mapa ϕ. Además, ϕ es un isomorfismo de grupos,

$$\phi(z_1) + \phi(z_2) = \phi(z_1 + z_2).$$

PRUEBA. Que ϕ es un isomorfismo de grupos se deduce de la demostración del lema. Solo hace falta verificar que la curva es no singular, es decir que el discriminante $\Delta = 4g_2^3 - 27g_3^2$ es distinto de cero, o bien que el polinomio $4x^3 - g_2x - g_3$ no tiene raíces repetidas. Notar que x es raíz si y solo si el punto $(x, 0) \in E(\Lambda)$ tiene orden dos. El

mapa ϕ se restringe a una biyección (isomorfismo de grupos de torsion) entre los puntos de orden dos de $\mathbb{C}/\Lambda$ y $E(\Lambda)$. Las raíces son

$$\begin{aligned} e_1 &= \wp(\omega_1/2), \\ e_2 &= \wp(\omega_2/2), \\ e_3 &= \wp(\omega_1/2+\omega_2/2), \end{aligned}$$

y se tiene

$$4x^3 - g_2x - g_3 = 4(x-e_1)(x-e_2)(x-e_3).$$

□

COROLARIO 2.4. *Fórmula aditiva de $\wp$:*

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

siempre que $z \neq z'$.

PRUEBA. Usar la proposición anterior y la fórmula de la suma para curvas de Weierstrass (2.3). □

COROLARIO 2.5. *Las curvas elípticas $E(\Lambda)$, $E(\Lambda')$ son isomorfas si y solo si existe $\alpha \in \mathbb{C}$ tal que $\alpha\Lambda = \Lambda'$.*

OBSERVACIÓN 2.5. *La importancia de la proposición anterior radica en que no solo da una parametrización explícita de una familia de curvas elipticas sino que además nos dice cuál es su estructura de grupo. Por ejemplo, permite encontrar el subgrupo $E[N]$ de puntos de orden N, también llamados de N-torsión. En una curva elíptica general, no necesariamente definida sobre $\mathbb{C}$, puede ser extremadamente difícil encontrar estos puntos. Sin embargo para un retículo Λ con base $\{\omega_1, \omega_2\}$, el subgrupo de N-torsión de $E(\Lambda)$ es*

$$E[N] = \left\{ \frac{i}{N}\omega_1 + \frac{j}{N}\omega_2 \ : \quad i,j = 0,1,...,N-1 \right\} \cong (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z}).$$

De hecho, toda curva elíptica compleja

$$E : y^2 = x^3 + ax + b$$

está determinada a menos de isomorfismo por su j-invariante

$$j(E) = 1728a^3/\Delta$$

y veremos luego que el j-invariante es una función modular que define un isomorfismo $\Gamma(1)\backslash\mathbb{H} \to \mathbb{C}$. De modo que vale el resultado más general:

TEOREMA 2.2. *Toda curva elíptica E sobre los complejos es isomorfa a $E(\Lambda)$ para algún retículo Λ.*

La noción general de curva elíptica es una curva proyectiva no singular E de género uno, junto a un punto distinguido $\mathcal{O} \in E$. Se puede demostrar que toda tal curva admite dos funciones meromorfas x, y, tales que x tiene un polo triple en $\mathcal{O}$, e y tiene un polo doble en $\mathcal{O}$. Además, considerando la dimensión de los distintos subespacios de funciones con polos de hasta un grado determinado, se puede probar que hay una relación lineal entre $x^2, y^3, xy, y^2, x, y, 1$, la cual puede ponerse en la forma

$$y^2 = x^3 + ax + b. \tag{8}$$

El mapa que a cada punto $P \in E$ le asigna el par $(x(P), y(P))$ da una parametrización de la curva (8). Decimos que esta curva y E son *birracionalmente equivalentes*. Del hecho de que E sea no singular se deduce $\Delta = 4a^3 - 27b^2 \neq 0$.

A su vez E se puede ver como una superficie de Riemann compacta de género 1, y toda tal superficie admite una estructura como curva algebraica. El siguiente teorema resume esta discusión:

Teorema 2.3. *Existen equivalencias naturales entre las siguientes categorias:*

1. *Objetos: Curvas elípticas E sobre $\mathbb{C}$.*
   Morfismos: mapas regulares $E \to E'$ que son homomorfismos de grupos.
2. *Objetos: Superficies de Riemann compactas de género 1 con un punto distinguido 0.*
   Morfismos: Mapas holomorfos $E \to E'$ que llevan 0 en $0'$.
3. *Objetos: Retículos $\Lambda \subset \mathbb{C}$.*
   Morfismos: $\hom(\Lambda, \Lambda') = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda'\}$.

Capítulo 3

Formas modulares

1. Funciones modulares

Sea Γ un subgrupo de índice finito en $\Gamma(1)$. Una **función modular** para Γ es una función meromorfa en la superficie de Riemann compacta $\Gamma\backslash\mathbb{H}^*$. Normalmente se la considera como una función meromorfa en $\mathbb{H}^*$ invariante por Γ. En este sentido, una función modular f para Γ es una función en $\mathbb{H}$ tal que

1. $f(z)$ es invariante por Γ.
2. $f(z)$ es meromorfa en $\mathbb{H}$.
3. $f(z)$ es meromorfa en las cúspides.

El estabilizador de la cúspide ∞ en $\Gamma(1)$ es el subgrupo cíclico generado por $T(z) = z+1$. Cualquier subgrupo es generado por alguna potencia de T, de modo que el estabilizador de la cúspide ∞ en Γ es generado por T^h para algún $h > 0$ (h se llama el *ancho* de la cúspide). Toda función modular f para Γ se puede escribir en un entorno de ∞ como función de $q = \exp(2\pi iz/h)$,

$$f = f^*(q),$$

y decimos que f es meromorfa en ∞ si f^* es meromorfa en 0. Una función g, holomorfa en un entorno de un punto a excepto tal vez en a, se puede extender a una función holomorfa en a si y solo si es acotada en un entorno de dicho punto. Se deduce que g es meromorfa en a si y solo si existe un entero $n > 0$ tal que $(z-a)^n g(z)$ es acotada en un entorno de a. Entonces que $f(z)$ sea meromorfa en ∞ significa que $q^n f^*(q)$ sea acotada (como función de q) en un entorno de $q = 0$ para cierto $n > 0$, esto es, si y solo si existe $A > 0$ tal que $e^{Aiz} f(z)$ es acotada para $z \to \infty$ (a lo sumo f crece exponencialmente con la parte imaginaria de z).

Si τ es otra cúspide distinta de ∞, existe $\sigma \in \Gamma(1)$ tal que $\tau = \sigma(\infty)$. Decimos que f es meromorfa en τ si $f \circ \sigma$ es meromorfa en ∞. Como f es invariante por Γ, solo hace falta verificar que sea meromorfa en una cantidad finita de cúspides: los representantes módulo la equivalencia por Γ.

Ejemplo 3.1. *Habíamos visto en el ejemplo (1.6) que las cúspides de* $\Gamma(2)$ *son* $\{0, 1, \infty\}$. *El estabilizador de* ∞ *en* $\Gamma(2)$ *es generado por* $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot z = z + 2$. *Entonces toda función modular* f *se escribe* $f(z) = f^*(q)$, $q = \exp(2\pi iz/2)$, *y* f *es meromorfa en* ∞ *si y solo si* $f^*(q)$ *es meromorfa en* $q = 0$. *A su vez,* f *es meromorfa en 0 si y solo si* $f(Sz) = f(-1/z)$ *es meromorfa en* ∞, *y* f *es meromorfa en 1 si y solo si* $f(TSz) = f(1 - 1/z)$ *es meromorfa en* ∞.

PROPOSICIÓN 3.1. *Si f es una función modular holomorfa en ∞, entonces f es constante.*

PRUEBA. Se puede ver a f como mapa holomorfo de superficies de Riemann compactas $\Gamma\backslash\mathbb{H}^* \to \mathbb{C}\cup\{\infty\}$. Suponer que no es constante. Su imagen es cerrada porque $\Gamma\backslash\mathbb{H}^*$ es compacto, y además es abierta porque las funciones holomorfas no constantes son abiertas. Como la esfera de Riemann $\mathbb{C}\cup\{\infty\}$ es conexa, f es sobreyectiva, pero por hipótesis $f \neq \infty$. □

2. Formas modulares

DEFINICIÓN 3.1. *Sea Γ un subgrupo de $\Gamma(1)$ de índice finito. Una **forma modular** respecto a Γ de peso $2k$ es una función f en $\mathbb{H}$ tal que:*

1. *Cumple $f(\gamma z) = (cz+d)^{2k} f(z)$ para todo $z \in \mathbb{H}$ y $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.*
2. *Es holomorfa en $\mathbb{H}$.*
3. *Es holomorfa en las cúspides de Γ.*

*Decimos que f es una **forma cuspidal** si es cero en las cúspides.*

Si f satisface estas condiciones con la palabra meromorfa *en lugar de* holomorfa*, entonces se dice que f es una forma modular meromorfa.*

PROPOSICIÓN 3.2. *Sea $\Lambda(z) = z\mathbb{Z}+\mathbb{Z}$ el retículo generado por z y 1. La serie de Eisenstein $G_k(\Lambda(z))$, $k>1$, es una forma modular de peso $2k$ respecto a $\Gamma(1)$ que toma el valor $2\,\zeta(2k)$ en infinito.*

PRUEBA. Para toda matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, se tiene

$$(az+b)\mathbb{Z}+(cz+d)\mathbb{Z} = z\mathbb{Z}+\mathbb{Z}$$

$$G_k\left(\frac{az+b}{cz+d}\mathbb{Z}+\mathbb{Z}\right) = (cz+d)^{-2k} G_k\Big((az+b)\mathbb{Z}+(cz+d)\mathbb{Z}\Big) = (cz+d)^{-2k} G_k(z\mathbb{Z}+\mathbb{Z})$$

□

COROLARIO 3.1. *$\Delta = g_2^3 - 27g_3^2$ es una forma modular de peso 12.*

OBSERVACIÓN 3.1. *No existen formas modulares no nulas de peso impar, ya que esto implicaría*

$$f(z) = f\Big(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\cdot z\Big) = f\Big(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\cdot z\Big) = f(z)(-1)^k = -f(z),$$

$$\Longrightarrow\ f(z) = 0$$

PROPOSICIÓN 3.3. *No existen formas modulares no nulas de peso negativo.*

PRUEBA. Veremos luego que Δ vale cero en ∞ (ejemplo 3.3). Si f fuera una forma modular de peso $-k$, con $k>0$, entonces $g = f^{12}\Delta^k$ sería una función modular con $g(\infty) = 0$. Por la proposición (3.1), g es constante e igual a cero, lo que fuerza $f = 0$. □

Sea $\omega = f(z)\,dz$ una forma diferencial en $\mathbb{H}$, donde $f(z)$ es una función meromorfa. El pullback de ω por la acción de Γ es

$$\begin{aligned}\gamma^*\omega &= f(\gamma z)\,d\,\frac{az+b}{cz+d}\\ &= f(\gamma z)\,\frac{a(cz+d)-c(az+b)}{(cz+d)^2}\,dz\\ &= f(\gamma z)\,(cz+d)^{-2}\,dz\end{aligned}$$

Se deduce que ω es invariante por γ si y solo si f es una forma modular meromorfa de peso 2.

Proposición 3.4. *Hay una correspondencia entre los siguientes conjuntos:*

- { Formas modulares meromorfas de peso 2 respecto a Γ }.
- { Formas diferenciales meromorfas en $\mathbb{H}^*$ invariantes por Γ }.
- { Formas diferenciales meromorfas en $\Gamma\backslash\mathbb{H}^*$ }.

Decimos que ω es un *k-diferencial* si se escribe localmente como $\omega = f(z)\,(dz)^k$. En ese caso,

$$\gamma^*\omega = f(\gamma z)(d\gamma)^k = f(\gamma z)(cz+d)^{-2k}(dz)^k,$$

y ω es invariante por Γ si y solo si $f(z)$ es una forma modular (meromorfa) de peso $2k$.

3. El espacio de formas modulares

Definición 3.2. *Sea Γ un subgrupo de $\Gamma(1)$ de índice finito, y k un entero. Se denota por $\mathcal{M}_k(\Gamma)$ al $\mathbb{C}$-espacio vectorial de las formas modulares respecto a Γ de peso $2k$.*

Para cada k el espacio $\mathcal{M}_k(\Gamma)$ tiene dimensión finita. Vamos a explotar la correspondencia entre formas modulares y diferenciales para dar una fórmula explícita de la dimensión; el paso clave involucra el teorema de Riemann-Roch aplicado a la superficie de Riemann compacta $\Gamma\backslash\mathbb{H}^*$, el cual nos da la dimensión de ciertos espacios de funciones meromorfas. Tratar dicho teorema aquí escaparía al alcance de este trabajo y por lo tanto nos limitaremos a invocarlo cuando sea necesario.

Teorema 3.1. *La dimensión de $\mathcal{M}_k(\Gamma)$ es*

$$\dim(\mathcal{M}_k(\Gamma)) = \begin{cases} 0 & \text{si } k<0\\ 1 & \text{si } k=0\\ (2k-1)(g-1)+v_\infty\,k+\sum_P k[1-1/e_P] & \text{si } k>0\end{cases}$$

donde g es el género de $X(\Gamma)=\Gamma\backslash\mathbb{H}^*$, v_∞ es la cantidad de cúspides no equivalentes, y la última suma es sobre los puntos elípticos de Γ. Por e_P denotamos el orden del estabilizador de P en $\Gamma(1)/\{\pm I\}$, y $[k(1-1/e_P)]$ es la parte entera de $k(1-1/e_P)$.

Antes de probar el teorema necesitamos un lema:

Lema 3.1. *Sea f una forma modular meromorfa de peso $2k$, y sea ω el correspodiente k-diferencial en $\Gamma\backslash\mathbb{H}^*$. Sea P la imagen de $Q\in\mathbb{H}$ por la proyección en $\Gamma\backslash\mathbb{H}^*$.*

1. *Si Q es un punto elíptico con multiplicidad e, entonces*

$$\operatorname{ord}_Q(f) = e \operatorname{ord}_P(\omega) + k(e-1).$$

2. *Si Q es una cúspide, entonces*

$$\operatorname{ord}_Q(f) = \operatorname{ord}_P(\omega) + k.$$

3. *Para el resto de los puntos,*

$$\operatorname{ord}_Q(f) = \operatorname{ord}_P(\omega).$$

Observación 3.2. *El lema anterior muestra que si $\omega = f(z)(dz)^k$ es un k-diferencial holomorfo, f no es necesariamente holomorfa. Por lo tanto, la proposición (3.4) no vale si cambiamos la palabra meromorfa por holomorfa.*

Prueba del lema. 1. La estructura compleja se definió de forma que hay un diagrama conmutativo

$$\begin{array}{ccc} U & \xrightarrow{Q\mapsto 0} & \mathbb{D} \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle z^e} \\ V & \xrightarrow{P\mapsto 0} & \mathbb{D} \end{array}$$

donde los mapas horizontales son isomorfismos. El de abajo es precisamente la carta local en P. Por lo tanto no perdemos generalidad si asumimos que U y V son el disco $\mathbb{D}$ y $P = Q = 0$.

Sea f una función en el disco, y sea $f^*(z) = f(z^e)$ el pullback. Si f tiene orden m en 0, entonces $f^*w = f(z^e)$ tiene orden $e \cdot m$ en 0.

Ahora si $\omega = f(z)dz$ es un k-diferencial en el disco,

$$\omega^* = f(z^e)(dz^e)^k = f(z^e)\, e^k\, z^{(e-1)k}\, (dz)^k,$$

$$\implies \operatorname{ord}_Q(\omega^*) = e \operatorname{ord}_P(f) + k(e-1).$$

2. Considero el mapa $q : \mathbb{H} \to \mathbb{D} - \{0\}$, dado por $q(z) = \exp(2\pi i z/h)$, y sea $\omega = f(q)(dq)^k$ un k-diferencial en el disco sin el origen. Por otro lado, $dq = (2\pi i/h)q$, entonces el pullback por q es

$$\omega^* = (cte)\, f(q(z))\, q(z)^k\, (dz)^k$$

y esto prueba la fórmula.

3. En este caso p es un isomorfismo local y por lo tanto no hay nada que probar.

□

Prueba del teorema. Sea $f \in \mathcal{M}_k(\Gamma)$ con k positivo. Como f es holomorfa, se tiene:

$$\begin{aligned} e\,\mathrm{ord}_P(\omega) + k(e-1) = \mathrm{ord}_Q(f) \geq 0 \text{ si Q es punto elíptico,} \\ \mathrm{ord}_P(\omega) + k = \mathrm{ord}_Q(f) \geq 0 \text{ si Q es cúspide,} \\ \mathrm{ord}_P(\omega) = \mathrm{ord}_Q(f) \geq 0 \text{ en cualquier otro caso.} \end{aligned}$$

Fijamos un k-diferencial ω_0, y escribimos $\omega = h \cdot \omega_0$. Se deduce que

$$\begin{aligned} \mathrm{ord}_P(h) + \mathrm{ord}_P(\omega_0) + k(1-1/e) \geq 0 \text{ si Q es punto elíptico,} \\ \mathrm{ord}_P(h) + \mathrm{ord}_P(\omega_0) + k \geq 0 \text{ si Q es cúspide,} \\ \mathrm{ord}_P(h) + \mathrm{ord}_P(\omega_0) \geq 0 \text{ en cualquier otro caso.} \end{aligned}$$

Por lo tanto ω es un k-diferencial si y solo si

$$\mathrm{Div}(h) + D \geq 0,$$

donde

$$D = \mathrm{Div}(\omega_0) + \sum k \cdot P + \sum [k(1-1/e)] \cdot P.$$

El conjunto de las funciones h es un $\mathbb{C}$-espacio vectorial, llamado $\mathcal{L}(D)$. Su dimensión la da el teorema de Riemann-Roch,

$$\dim(\mathcal{L}(D)) = 1 - g + \deg(D). \tag{9}$$

El grado del divisor de un 1-diferencial es $2g-2$. Como ω_0 es un k-diferencial, tiene grado $k(2g-2)$. Por lo tanto,

$$\dim(\mathcal{M}_k(\Gamma)) = \dim(\mathcal{L}(D)) = 1 - g - k(2g-2) - v_\infty\, k - \sum [k(1-1/e)] \cdot P,$$

y de ahí se prueba el caso $k > 0$.
Los casos $k = 0$ y $k < 0$ son las proposiciones (3.1) y (3.3) respectivamente.

□

Observación 3.3. *Leyendo la prueba anterior, parecería que nunca usamos que k fuera positivo. De hecho lo usamos cuando invocamos Riemann-Roch. La fórmula (9) normalmente tiene un término más, el cual es difícil de calcular, pero este término se anula si el grado de D es mayor a $2g-2$.*

Ejemplo 3.2. *La curva $\Gamma(1)\backslash\mathbb{H}^*$ es homeomorfa a la esfera, y por lo tanto tiene género $g = 0$. La dimensión de $\mathcal{M}_k(\Gamma(1))$ para $k = 1, 2, 3, \ldots$ es*

$$\dim \mathcal{M}_k = 1 - k + [k/2] + k[2k/3], \qquad k > 1$$

k	$= 1$	2	3	4	5	6	$\ldots$
$\dim \mathcal{M}_k$	$= 0$	1	1	1	1	2	$\ldots$

$$\dim \mathcal{M}_{k+6} = \dim \mathcal{M}_k + 1$$

4. Ceros de formas modulares

PROPOSICIÓN 3.5. *Sean f una forma modular meromorfa de peso $2k$, y ω el correspondiente diferencial en $\Gamma\backslash\mathbb{H}^*$. Sea v_∞ la cantidad de cúspides no equivalentes. Igual que antes, e_Q es el orden del estabilizador de Q si éste es un punto elíptico; es igual a 1 en caso contrario. Entonces,*

$$\sum \Big\{ \operatorname{ord}_Q(f)/e_Q - k(1-1/e_Q) \Big\} = k(2g-2) + k \cdot v_\infty.$$

PRUEBA. Sabemos que para un punto elíptico Q,

$$\operatorname{ord}_Q(f)/e_Q = \operatorname{ord}_{p(Q)}(\omega) + k(1-1/e_Q)$$

para una cúspide,

$$\operatorname{ord}_Q(f) = \operatorname{ord}_{p(Q)}(\omega) + k$$

y para el resto de los puntos

$$\operatorname{ord}_Q(f) = \operatorname{ord}_{p(Q)}(\omega).$$

Sumando estas ecuaciones se obtiene

$$\sum \Big\{ \operatorname{ord}_Q(f)/e_Q - k(1-1/e_Q) \Big\} = \deg(\operatorname{Div}(\omega)) + k \cdot v_\infty.$$

Como mencionamos antes, el grado del divisor de un k-diferencial es $k(2g-2)$. □

EJEMPLO 3.3. *Cuando $\Gamma = \Gamma(1)$ se tiene*

$$\frac{1}{2}\operatorname{ord}_i(f) + \frac{1}{3}\operatorname{ord}_\rho(f) + \operatorname{ord}_\infty(f) + \sum \operatorname{ord}_Q(f) = k(2\cdot 0 - 2) + k + k(1/2) + k(2/3) = k/6$$

donde la suma es sobre el resto de los puntos en un dominio fundamental.
Se deduce que:

1. *G_3 tiene solo un cero en i.*
2. *G_2 tiene solo un cero en ρ.*
3. *Como Δ no tiene ceros en $\mathbb{H}$, entonces tiene un cero simple en ∞.*

Las partes (1) y (2) se pueden probar de forma elemental, usando que el retículo $\Lambda(i) = i\mathbb{Z} + \mathbb{Z}$ es invariante por multiplicar por i, y de manera similar para ρ.

Usando que j tiene un polo simple en ∞ y es holomorfa en $\mathbb{H}$, se puede probar lo siguiente:

LEMA 3.2. *La función modular $j = 1728 g_2^3/\Delta$ define un isomorfismo $\Gamma(1)\backslash\mathbb{H}^* \to \mathbb{C} \cup \{\infty\}$.*

PRUEBA. Como Δ tiene un único cero, j tiene un único polo. Luego tiene grado 1 (cf Corolario 2.2).

□

Podemos reformular el Teorema (2.2) de la siguiente manera:

TEOREMA 3.2. *Hay una correspondencia biyectiva*

$$\Big\{ \textit{ Puntos de } X(1) \Big\} \longleftrightarrow \Big\{ \textit{Curvas elípticas sobre } \mathbb{C} \Big\} / \sim$$

$$\Gamma(1)\tau \longleftrightarrow E(\Lambda(\tau))$$

donde el cociente por $\sim$ *significa tomar clases de isomorfismo.*

El énfasis está en el hecho de que el conjunto de clases de isomorfismo de curvas elípticas aparece identificado con los puntos de una curva modular. Esto es un caso particular de un *espacio de móduli*, lo cual estudiaremos a continuación.

Capítulo 4

Espacios de móduli

1. Bases de N-torsión

Como se vio en el capítulo 2, el subgrupo de N-torsión de una curva elíptica definida sobre $\mathbb{C}$ es isomorfo a $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$. Si $\{\omega_1, \omega_2\}$, es una base del retículo Λ, entonces $\{\omega_1/N, \omega_2/N\}$ es una base de $E[N]$ como $\mathbb{Z}/N\mathbb{Z}$-módulo.

Cualquier otra base es de la forma

$$\{a\omega_1/N + b\omega_2/N, c\omega_1/N + d\omega_2/N\}, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Definición 4.1. *Sean P, Q dos puntos de N-torsión de $E[\Lambda]$, y sea $\{\omega_1, \omega_2\}$ una base del retículo Λ.*

Existe una matriz γ tal que

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \cdot \begin{pmatrix} \omega_1/N \\ \omega_2/N \end{pmatrix}$$

Se define el ***pairing de Weil*** *de (P, Q) como*

$$e_N(P, Q) = e^{2\pi i \det \gamma / N}$$

El pairing de Weil es una raíz primitiva de la unidad si y solo si $\{P, Q\}$ es una base de $E[N]$. Notar que está bien definida aunque $\det(\gamma)$ solo tenga sentido módulo N. El pairing es independiente de la base del retículo $\{\omega_1, \omega_2\}$ escogida.

2. Subgrupos de congruencia

En el capítulo 1 definimos $\Gamma(N)$ como el kernel en $\Gamma(1)$ del homomorfismo reducción módulo N, es decir las matrices congruentes con la identidad módulo N. Un subgrupo de $\Gamma(1)$ es de congruencia si contiene a $\Gamma(N)$ para algún N, y el nivel de un subgrupo de congruencia es el menor N con esta propiedad. Definimos dos subgrupos de congruencia de interés particular.

Definición 4.2. *Se definen los siguientes subgrupos de $\Gamma(1)$:*

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : \ c \equiv 0 \ mod \ N \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : \ c \equiv 0 \ mod \ N, \ a \equiv d \equiv 1 \ mod \ N \right\}.$$

Una *curva elíptica marcada* de $\Gamma_0(N)$ es un par (E, C) donde E es una curva elíptica sobre $\mathbb{C}$ y C es un subgrupo cíclico de E de orden N. Dos tales pares (E, C), (E', C') son isomorfos, denotado $(E, C) \sim (E', C')$, si existe un isomorfismo de curvas elípticas $E \to E'$ que se restringe a un isomorfismo $C \to C'$. El conjunto de todas las clases de isomorfismo de curvas elípticas se escribe

$$S_0(N) = \{ \text{ Curvas elípticas marcdas para } \Gamma_0(N) \}/\sim$$

y la clase de (E, C) se escribe $[E, C]$.

Una curva elíptica marcada de $\Gamma_1(N)$ es un par (E, Q) donde E es una curva elíptica sobre $\mathbb{C}$ y Q es un punto de E de N-torsión. Dos pares (E, Q), (E', Q') son isomorfos si existe un isomorfismo $E \to E'$ que lleva Q en Q'. El conjunto de clases de isomorfismo es

$$S_1(N) = \{ \text{ Curvas elípticas marcdas para } \Gamma_1(N) \}/\sim$$

y la clase de (E, Q) se escribe $[E, Q]$.

Una curva elíptica marcada de $\Gamma(N)$ es un par $(E, (P, Q))$ donde E es una curva elíptica sobre $\mathbb{C}$ y (P, Q) es un par de puntos que generan el subgrupo N-torsión $E[N]$ con pairing de Weil $e_N(P, Q) = e^{2\pi i/N}$. Dos pares $(E, (P, Q))$, $(E', (P', Q'))$ son isomorfos si existe un isomorfismo $E \to E'$ que lleva P en P' y Q en Q'. El conjunto de clases de isomorfismo es

$$S(N) = \{ \text{ Curvas elípticas marcdas para } \Gamma(N) \}/\sim$$

y la clase de $(E, (P, Q))$ se escribe $[E, (P, Q)]$.

3. Curvas modulares como espacios de móduli

Los conjuntos $S_0(N)$, $S_1(N)$ y $S(N)$ son *espacios de móduli* de clases de isomorfismo de curvas elípticas complejas junto a información sobre la N-torsión.

Definición 4.3. *Recordamos la curva modular $X(N) = \Gamma(N)\backslash\mathbb{H}$. Se definen tambiéen*

$$X_0(N) = \Gamma_0(N)\backslash\mathbb{H}$$

$$X_1(N) = \Gamma_1(N)\backslash\mathbb{H}$$

así como sus compactificaciones $Y_0(N)$, $Y_1(N)$.

En lo que sigue denotamos por Λ_τ al retículo $\Lambda = \tau\mathbb{Z} + \mathbb{Z}$ y E_τ a la curva elíptica $E(\Lambda_\tau)$.

Teorema 4.1. *Sea N un entero positivo.*

1. *El espacio de móduli de $\Gamma_0(N)$ es*

$$S_0(N) = \{ [E_\tau, \langle 1/N + \Lambda_\tau \rangle] : \tau \in \mathbb{H} \}.$$

Dos puntos $[E_\tau, \langle 1/N + \Lambda_\tau \rangle]$, $[E_{\tau'}, \langle 1/N + \Lambda_{\tau'} \rangle]$ son iguales si y solo si $\Gamma_0(N)\tau = \Gamma_0(n)\tau'$. Es decir, hay una biyección

$$\psi_0 : S_0(N) \xrightarrow{\sim} Y_0(N), \qquad [E_\tau, \langle 1/N + \Lambda_\tau \rangle] \mapsto \Gamma_0(N)\tau.$$

2. *El espacio de móduli de* $\Gamma_1(N)$ *es*

$$S_1(N) = \{\ [E_\tau, 1/N + \Lambda_\tau] \ : \ \tau \in \mathbb{H}\ \}.$$

Dos puntos $[E_\tau, 1/N + \Lambda_\tau]$, $[E_{\tau'}, 1/N + \Lambda_{\tau'}]$ *son iguales si y solo si* $\Gamma_1(N)\tau = \Gamma_1(n)\tau'$.

Hay una biyección

$$\psi_1 : S_1(N) \xrightarrow{\sim} Y_1(N), \qquad [E_\tau, 1/N + \Lambda_\tau] \mapsto \Gamma_1(N)\tau.$$

3. *El espacio de móduli de* $\Gamma(N)$ *es*

$$S(N) = \{\ [E_\tau, (1/N + \Lambda_\tau, \tau/N + \Lambda_\tau)] \ : \ \tau \in \mathbb{H}\ \}.$$

Dos puntos $[E_\tau, (1/N + \Lambda_\tau, \tau/N + \Lambda_\tau)]$, $[E_{\tau'}, (1/N + \Lambda_{\tau'}, \tau'/N + \Lambda_{\tau'})]$ *son iguales si y solo si* $\Gamma(N)\tau = \Gamma(N)\tau'$.

Hay una biyección

$$\psi : S(N) \xrightarrow{\sim} Y(N), \qquad [E_\tau, (1/N + \Lambda_\tau, \tau/N + \Lambda_\tau)] \mapsto \Gamma(N)\tau.$$

Prueba. La siguiente demostración se basa en [DS05, Teorema 1.5.1].
Recordemos que todo isomorfismo $E_\tau \xrightarrow{\sim} E_{\tau'}$ es de la forma

$$z + \Lambda_\tau \mapsto mz + \Lambda_{\tau'}$$

para un $m \in \mathbb{C}$ con $m\Lambda_\tau = \Lambda_{\tau'}$.
Notar que

$$m\Lambda_\tau = \Lambda_{\tau'} \iff \begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \cdot \begin{pmatrix} \tau' \\ 1 \end{pmatrix}, \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1), \tag{10}$$

Esto es, si y solo si

$$m = c\tau' + d \qquad\qquad \tau = \frac{a\tau' + b}{c\tau' + d} \tag{11}$$

Es decir, las curvas E_τ, $E_{\tau'}$ son isomorfas si y solo si $\tau = \gamma(\tau')$ para un $\gamma \in \Gamma(1)$ o, equivalentemente,

$$\Gamma(1)\tau = \Gamma(1)\tau'$$

.

Parte (2):
Veamos que todo punto $[E, Q] \in S_0$ es de la forma $[E_\tau, (1/N + \Lambda_\tau)]$.

Sabemos que $E \sim E_{\tau'}$ para un $\tau' \in \mathbb{H}$. Luego $[E, Q] = [E_{\tau'}, (c/N + d\tau'/N + \Lambda_{\tau'})]$. Como Q tiene orden N, entonces los tres enteros c, d, N no comparten ningún factor, es decir, existen a, b, k con $ad - bc - kN = 1$, o $ad - bc \equiv 1 \bmod N$.

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Se puede levantar γ a una matriz de $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$.

Tomando m y τ como en (11) se obtiene un isomorfismo $E_\tau \xrightarrow{\sim} E_{\tau'}$ el cual lleva $1/N + \Lambda_\tau$ en el punto $c\tau'/N + d/N + \Lambda_{\tau'}$.

Dados dos puntos $[E_\tau, 1/N + \Lambda_\tau]$, $[E'_\tau, 1/N + \Lambda_{\tau'}]$, éstos son iguales por definición si y solo si existe un isomorfismo como en (10) para el cual

$$(c\tau' + d)/N + \Lambda_\tau = 1/N + \Lambda_\tau.$$

Esto es, si y solo si $(c, d) \equiv (0, 1) \bmod N$,

$$\begin{aligned} &\iff \gamma \in \Gamma_1(N) \\ &\iff \Gamma_1(N)\tau = \Gamma_1(N)\tau' \end{aligned}$$

Parte (1):

Sea $[E, C] \in S_0(N)$ y sea Q un generador de C. Por la parte anterior hay un isomorfismo $E_\tau \xrightarrow{\sim} E_{\tau'}$ que lleva el punto $1/N + \Lambda_\tau$ en Q. Luego $[E, C] = [E_\tau, \langle 1/N + \Lambda_\tau \rangle]$.

Sean $[E_\tau, \langle 1/N + \Lambda_\tau \rangle]$, $[E_{\tau'}, \langle 1/N + \Lambda_{\tau'} \rangle]$ dos puntos de $S_0(N)$. Son iguales si y solo si existe

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$$

tal que

$$\begin{aligned} \tau &= \gamma(\tau') \\ \langle c\tau'/N + d/N + \Lambda_{\tau'} \rangle &= \langle 1/N + \Lambda_{\tau'} \rangle \end{aligned}$$

La última condición es equivalente a $c \equiv 0 \bmod N$ y d coprimo con N, lo que a su vez significa que $\gamma \in \Gamma_0(N)$.

Parte (3):

Toda base de N-torsión de E_τ es de la forma

$$(a\tau/N + b/N,\ c\tau/N + d/N), \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Si el pairing de Weil es $e^{2\pi i/N}$ entonces de hecho $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Igual que antes, podemos asumir $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, y obtenemos un isomorfismo de $E[\Lambda_{\gamma(\tau)}]$ en $E[\Lambda_\tau]$ dado por $z \mapsto z \cdot (c\tau + d)$ y el cual lleva el par $(\gamma(\tau)/N,\ 1/N)$ en la base anterior.

Por último, considerar dos curvas E_τ, $E_{\tau'}$ y un isomorfismo $z \mapsto mz$

$$\begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \cdot \begin{pmatrix} \tau' \\ 1 \end{pmatrix}, \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1),$$

La imagen del par $(\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)$ es $(a\tau'/N + b/N + \Lambda_{\tau'}, c\tau'/N + d/N + \Lambda_{\tau'})$, y ésta es igual a $(\tau'/N + \Lambda_{\tau'}, 1/N + \Lambda_{\tau'})$ si y solo si se satisfacen las congruencias

$$a \equiv d \equiv 1 \bmod N,$$
$$c \equiv b \equiv 0 \bmod N.$$

□

Bibliografía

[DS05] Fred Diamond y Jerry Shurman. *A first course in modular forms*. Vol. 228. Graduate Texts in Mathematics. Springer-Verlag, New York, 2005.

[Mil17] James S. Milne. *Modular Functions and Modular Forms (v1.31)*. PDF disponible en www.jmilne.org/math/. 2017.