Universidad de Cantabria

Facultad de Ciencias

FORMAS MODULARES Y CURVAS ELÍPTICAS
(Modular forms and elliptic curves)

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Juan Carlos Boigues Pérez

Director: Jesús Javier Jiménez Garrido

Julio - 2023

Índice general

AGRADECIMIENTOS

En primer lugar, me gustaría expresar mi más sincero agradecimiento a Jesús Javier, mi tutor en este trabajo. A través de sus enseñanzas, las innumerables tutorías y correcciones, he adquirido una base sólida de conocimientos que han hecho posible el desarrollo de esta memoria.

Asimismo, quiero agradecer a todos mis profesores durante estos cuatro años, tanto de la universidad de Cantabria como de la Universidad Autónoma de Madrid. Cada uno de ustedes ha permitido mi desarrollo tanto académico como personal.

Por último, quiero expresar mi gratitud tanto a mis compañeros como a mi familia, cuyo apoyo y amistad incondicional han sido de gran ayuda para superar los momentos difíciles y celebrar los éxitos obtenidos.

RESUMEN

En 1957 los matemáticos japoneses Y. Taniyama y G. Shimura plantearon, sin demostrar, un resultado que relacionaba las formas modulares con las curvas elípticas, dos objetos matemáticos a priori inconexos. Gracias al trabajo de A. Weil, se establecieron las bases que respaldaban la posible validez de la denominada conjetura de Taniyama-Shimura-Weil, conocida actualmente como el teorema de la modularidad. Este trabajo se centra en comprender de manera precisa todos los elementos que intervienen en el enunciado de dicho teorema. Con este propósito, se estudiarán las formas modulares que son funciones meromorfas en el semiplano superior complejo que cumplen una cierta condición de regularidad. En segundo lugar, se presentarán los toros complejos y las curvas elípticas y se detallará la relación que existe entre ambas nociones. Por último, se introducirán las curvas modulares, las dotaremos de una topología y de una estructura de superficie de Riemann y mostraremos cómo se pueden compactificar. Empleando estos elementos, se enunciará la versión analítico-compleja del teorema de la modularidad.

Palabras clave: grupo modular, forma modular, toro complejo, curva elíptica, curva modular, superficies de Riemann, teorema de la modularidad.

ABSTRACT

In 1957 the Japanese mathematicians Y. Taniyama and G. Shimura formulated, without proving it, a result that connected modular forms with elliptic curves, two a priori unrelated mathematical objects. Thanks to the work of A. Weil, the foundations supporting the possible validity of the so-called Taniyama-Shimura-Weil conjecture, now known as the modularity theorem, were established. This work focuses on understanding precisely all the elements involved in the statement of this theorem. For this purpose, modular forms which are meromorphic functions in the complex upper halfplane satisfying a certain regularity condition will be studied. Secondly, complex tori and elliptic curves will be presented and the relationship between both notions will be detailed. Finally, modular curves will be introduced, we will endow them with a topology and a Riemann surface structure and show how they can be compactified. Using these elements, the analytic-complex version of the modularity theorem will be stated.

Key words: modular group, modular form, complex torus, elliptic curve, modular curve, Riemann surfaces, modularity theorem.

Capítulo 1

Introducción

En términos generales, el teorema de la modularidad asegura que todas las curvas elípticas racionales provienen de formas modulares. El propósito de este trabajo es desarrollar la afirmación anterior, es decir, comprender en detalle todas las nociones que intervienen en el enunciado de este teorema. De entre las distintas versiones de este resultado que existen, hemos elegido la analítico-compleja la cual se expresa por medio de superficies de Riemann. Al adoptar este enfoque, obtendremos una visión amplia del problema al mismo tiempo que accesible a partir de los conocimientos previos. Concretamente, la formulación que se abordará es la siguiente

Teorema de la modularidad. *Sea E una curva elíptica compleja con $j(E) \in \mathbb{Q}$. Entonces existen $N \in \mathbb{N}_{\geq 1}$ y una aplicación holomorfa y sobreyectiva entre superficies de Riemann compactas desde la curva modular $X_0(N)$ a la curva elíptica E,*

$$X_0(N) \to E.$$

A esta función se le conoce como parametrización modular de E.

La importancia del teorema de la modularidad radica en que establece una conexión entre dos áreas aparentemente alejadas de las matemáticas: el análisis armónico y la teoría de números. De un cierto modo, podría afirmarse que esta relación aparece de forma esporádica en los trabajos de C. F. Gauss y L. Kronecker del siglo XIX. Entre los resultados de C. F. Gauss en teoría de números que motivaron los hallazgos de los siglos posteriores, cabe de destacar la ley de reciprocidad cuadrática. Esta ley afirma que si p es un número primo, el número de raíces cuadradas de un número entero n en aritmética módulo p depende sólo de p módulo $4n$. Por ejemplo, para comprobar si 3 es un cuadrado en aritmética módulo 672023 basta saber si 3 es un cuadrado módulo 11 porque $672023 = 12 \cdot 56001 + 11$. En gran medida, el estudio de los cuerpos de números algebraicos y sus anillos de enteros de los años siguientes estaba ocasionado por el intento de generalizar la reciprocidad cuadrática para potencias superiores a la segunda. En particular, E. Artin demostró una versión general en 1927 para la cual todas las leyes de reciprocidad conocidas hasta el momento eran casos especiales.

Durante algunas décadas se pensó que la cuestión estaba cerrada, pero, inesperadamente, en 1954, M. Eichler encontró una ley de reciprocidad, para ecuaciones en dos variables, que no se deducía del teorema de E. Artin. Un año más tarde, inspirado por el trabajo de Eichler, Y. Taniyama planteó, en forma de pregunta, la conexión entre formas modulares y curvas elípticas que buscamos entender en esta memoria. En 1957, junto con su colaborador G. Shimura, escribió de manera rigurosa esta cuestión estableciendo el enunciado preciso que conocemos. Una década más tarde, A. Weil redescubrió la conjetura, estableció el marco teórico y encontró evidencias sólidas que apoyaban la veracidad de la misma. La conjetura de Taniyama-Shimura-Weil, conocida actualmente como teorema de la modularidad, cambió el paradigma de la teoría de números en la segunda mitad del siglo XX.

En el transcurso de los siguientes años, se trató de demostrar la conjetura, aunque no se produjeron avances significativos y el resultado parecía en cierta forma inalcanzable. Sin embargo, a mediados de la década de los 80 se dio un nuevo impulso a la teoría cuando se mostró que la veracidad de la conjetura implicaría la validez del último teorema de Fermat. Recordamos que el último teorema de Fermat establece que para todo $n \in \mathbb{N}_{\geq 3}$ la ecuación $x^n + y^n = z^n$ no tiene soluciones enteras con $xyz \neq 0$. En diferentes trabajos, G. Frey,

J.P. Serre y K. Ribet mostraron que si el último teorema de Fermat fuera falso, es decir, si existieran $n \in \mathbb{N}_{\geq 3}$ y $a,b,c \in \mathbb{Z} \setminus \{0\}$ con $a^n + b^n = c^n$, entonces la curva elíptica dada por la ecuación $y^2 = x(x-a^n)(x-b^n)$ no verificaría la conjetura de Taniyama-Shimura-Weil.

En 1995, motivado por este resultado, A.Wiles, con la ayuda de R. Taylor, demostró la conjetura Taniyama-Shimura-Weil en el caso de curvas elípticas semiestables. Esta versión era suficiente para probar la veracidad del último teorema de Fermat. Basándose en el trabajo de A. Wiles, C.Breuil, B. Conrad, F. Diamond y R. Taylor, abordaron los casos restantes hasta demostrar el resultado completo en 1999. Desde entonces, las generalizaciones del teorema de la modularidad han sido objeto de una intensa investigación. Como sugirió R. Langlands en la década de 1970, cuando estableció las bases del conocido como Programa Langlands, resulta que la conjetura Taniyama-Shimura-Weil puede reformularse como un caso especial de un panorama mucho más amplio. Las conjeturas del Programa Langlands relacionan las representaciones $n-$dimensionales del grupo de Galois, que generalizan las representaciones dadas por las curvas elípticas, con las funciones automorfas, que generalizan las formas modulares. Aunque hay pocas dudas sobre la validez de estas conjeturas, la mayoría siguen sin haberse demostrado a día de hoy. Para mayor información sobre las referencias históricas que acabamos de mencionar nos referimos al libro "Amor y matemáticas" de E. Frenkel [5] y al artículo "Modular Arithmetic: Driven by Inherent Beauty and Human Curiosity" de R. Taylor [8].

En la versión del teorema de la modularidad, a la que nos referimos en esta memoria, intervienen esencialmente tres elementos fundamentales: las formas modulares, las curvas elípticas y, la noción que comunica ambos, las curvas modulares. Debemos señalar que no trataremos en este texto con otros conceptos que aparecen en la prueba del teorema o al enunciar otras versiones del mismo como son: las funciones L, las representaciones del grupo de Galois o los operadores de Hecke.

En consecuencia, el trabajo se estructura en tres capítulos, uno para cada noción, y un último capítulo donde completamos la información para poder enunciar el teorema de la modularidad. En concreto, en el Capítulo 2 presentaremos el grupo modular y describiremos la acción del mismo sobre el semiplano superior complejo. Empleando este grupo estableceremos la condición de modularidad que nos permitirá definir las formas modulares. Esta noción será, en ocasiones, demasiado restrictiva y necesitaremos limitar la condición de modularidad a ciertos subgrupos del grupo modular, conocidos como subgrupos de congruencias, procedimiento que detallaremos en la última sección del capítulo.

El Capítulo 3 se centra en el análisis de la estructura de los toros complejos, los cuales se construyen como el grupo cociente del plano complejo por un retículo $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$. Caracterizaremos los homomorfismos holomorfos entre toros complejos y veremos como agruparlos en clases de equivalencia. En la segunda sección introduciremos las funciones elípticas analizando el ejemplo fundamental de la función de Weierstrass. Esta función nos permitirá parametrizar toda curva elíptica desde un toro complejo, vinculando así ambas nociones. Por medio de esta identificación, podremos definir el invariante j de una curva elíptica.

Aunque las formas modulares están definidas en el plano superior complejo, dado que satisfacen la condición de modularidad, se puede considerar que su dominio natural es un espacio cociente del plano superior, que denominaremos curva modular. En el Capítulo 4, se definirán con rigor las curvas modulares y veremos qué relación tienen con los espacios de moduli que clasifican las curvas elípticas, conectando de este modo las dos nociones principales del trabajo. Analizaremos la topología de estas curvas y mostraremos cómo se pueden dotar de estructura de superficie de Riemann prestando especial atención a los puntos elípticos.

Finalmente, para poder enunciar el teorema de la modularidad en su variante analítico-compleja, necesitaremos compactificar las curvas modulares. Llevaremos acabo esta tarea en el Capítulo 5. Para lograrlo añadiremos a las curvas modulares un conjunto de puntos denominados cúspides junto con las correspondientes cartas. Concluiremos el trabajo presentando el teorema y comentando por encima su relación con otras versiones del mismo.

Capítulo 2

Grupo modular y formas modulares

El objetivo de este capítulo es introducir las nociones fundamentales de la teoría de formas modulares. Comenzaremos presentando el grupo modular y sus propiedades elementales. Empleando este grupo podremos establecer la condición de modularidad que nos permitirá definir las formas modulares. En ocasiones la condición de modularidad se satisface solamente para un subgrupo propio del grupo modular. Lo que nos conduce a una revisión más débil de dicha condición. En la última sección, se aborda este problema a través de los llamados subgrupos de congruencias. Salvo que se especifique lo contrario, en este capítulo hemos seguido el libro "A first course in modular forms"de F.Diamond y J.A.Shurman [4].

2.1. Grupo modular

En esta sección daremos la definición del grupo modular y una serie de propiedades que nos permitirán conocer como actúa este grupo sobre el plano superior complejo.

Definición 2.1. *Llamamos grupo modular al grupo especial lineal de orden 2 sobre los enteros, es decir,*

$$SL_2(\mathbb{Z}) \quad = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ a,b,c,d \in \mathbb{Z} \ y \ ad-cb=1 \right\},$$

donde la operación del grupo es el producto de matrices.

Cuando interpretamos las matrices de $SL_2(\mathbb{Z})$ como transformaciones del plano superior complejo resulta que γ y $-\gamma$ representan la misma transformación. Por ello, algunos autores denominan grupo modular al grupo proyectivo especial lineal $PSL_2(\mathbb{Z})$ que se obtiene identificando γ y $-\gamma$ en $SL_2(\mathbb{Z})$, es decir, haciendo el grupo cociente $SL_2(\mathbb{Z})$ sobre su centro $Z(SL_2(\mathbb{Z})) = \{I, \ -I\}$ donde I denota la matriz identidad. En todo caso, debe entenderse que el termino 'modular' proviene de su relación con el espacio de moduli de las curvas elípticas, que presentaremos en la Sección 4.1, y no de la aritmética modular.
Antes de estudiar la acción de grupo que define $SL_2(\mathbb{Z})$ sobre la esfera de Riemann, veamos que el grupo modular se puede generar con dos matrices.

Proposición 2.2. *El grupo modular está generado por*

$$\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad y \quad \beta = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Demostración. Como β y $\alpha \in SL_2(\mathbb{Z})$ basta ver que dada $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ una matriz cualquiera del grupo modular, está generada por β y α.
En primer lugar, probamos por inducción que para todo $k \in \mathbb{Z}$ se tiene que

$$\alpha^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}.$$

Comprobamos también que $O(\beta) = 4$ y que $\beta^2 = -I$. Empleando esta información tenemos que

- Si $c = 0$ y $a = d = 1$, entonces $\gamma = \alpha^b$.
- Si $c = 0$ y $a = d = -1$, entonces $\gamma = \alpha^{-b}\beta^2$.
- Si $c \neq 0$ entonces, podemos dividir a entre c y sabemos que existen $q, r \in \mathbb{Z}$ únicos tales que $a = cq + r$ con $0 \leqslant r < |c|$. Observamos que

$$\beta\alpha^{-q}\gamma = \begin{pmatrix} -c & -d \\ r & b - qd \end{pmatrix}.$$

  El Algoritmo de Euclides garantiza que tras un número finito de iteraciones podemos lograr una matriz con la entrada de la segunda fila y primera columna nula, es decir, una matriz de la forma de los apartados anteriores. En otras palabras, existen $m \in \mathbb{Z}$, $q_1, \ldots, q_n \in \mathbb{Z}$ y $\delta \in \{0, 2\}$ tales que

$$\left(\beta\alpha^{-q_n}\right) \cdots \left(\beta\alpha^{-q_1}\right) \gamma = \alpha^m \beta^\delta.$$

  Despejando se tiene que $\gamma = \left(\beta\alpha^{-q_1}\right)^{-1} \cdots \left(\beta\alpha^{-q_n}\right)^{-1} \alpha^m \beta^\delta$, luego γ está generado por α y β. □

Consideramos $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ la esfera de Riemann con la estructura estándar de superficie de Riemann. Recordamos que un automorfismo de la esfera de Riemann es una aplicación de $\widehat{\mathbb{C}}$ en $\widehat{\mathbb{C}}$ biholomorfa. Denotamos al conjunto de automorfismos por $Aut(\widehat{\mathbb{C}})$. Existe una forma clásica de identificar toda matriz con coeficientes complejos invertible con un automorfismo, es decir, de definir una acción de grupo de $GL_2(\mathbb{C})$ sobre $\widehat{\mathbb{C}}$. Basta considerar

$$\begin{array}{ccccc} GL_2(\mathbb{C}) & \to & & Aut(\widehat{\mathbb{C}}) & \\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \to & \tau & \mapsto & \widetilde{\gamma}(\tau) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \dfrac{a\tau + b}{c\tau + d}. \end{array}$$

Donde estamos teniendo en cuenta las consideraciones habituales sobre el infinito, es decir, si $c \neq 0$, entonces $\widetilde{\gamma}(-d/c) = \infty$ y $\widetilde{\gamma}(\infty) = a/c$ y si $c = 0$ entonces $\widetilde{\gamma}(\infty) = \infty$. Por ejemplo, las matrices α y β de la Proposición 2.2 se corresponden con las transformaciones $\widetilde{\alpha}(\tau) = \tau + 1$ y $\widetilde{\beta}(\tau) = -1/\tau$.
Observamos que se trata de una acción de grupo porque dadas $\gamma_1, \gamma_2 \in GL_2(\mathbb{C})$ se tiene que $\widetilde{\gamma_1 \cdot \gamma_2} = \widetilde{\gamma}_1 \cdot \widetilde{\gamma}_2$ y porque $\widetilde{I} = I$. Podemos considerar la restricción de esta acción a un subgrupo Γ de $GL_2(\mathbb{C})$. En particular, en este trabajo estamos interesados en considerar la restricción de la acción a $\Gamma = SL_2(\mathbb{Z})$.
Por otro lado, comprobamos de forma directa que el núcleo de la acción de grupo de $GL_2(\mathbb{C})$ sobre $\widehat{\mathbb{C}}$ es el conjunto de matrices escalares, es decir, $a = d$ y $b = c = 0$. En concreto, si consideramos la restricción a $SL_2(\mathbb{Z})$ este núcleo resulta ser $\{I, -I\}$, luego $\gamma_1, \gamma_2 \in SL_2(\mathbb{Z})$ definen el mismo automorfismo si y solo si $\gamma_1 = \pm\gamma_2$. Con esta salvedad, abusaremos de la notación y denotaremos por γ al automorfismo definido por $\gamma \in SL_2(\mathbb{Z})$ en lugar de escribir $\widetilde{\gamma}$.
Veamos ahora que dada $\gamma \in SL_2(\mathbb{Z})$ la correspondiente transformación define un automorfismo del plano superior complejo en sí mismo.

Proposición 2.3. *Sean $\mathbb{H} = \{\tau \in \mathbb{C} : \ Im(\tau) > 0\}$ el semiplano superior y $\gamma \in SL_2(\mathbb{Z})$. Entonces se tiene que*

$$\text{para todo } \tau \in \mathbb{H} \quad Im(\gamma(\tau)) = \frac{Im(\tau)}{|c\tau + d|^2} \quad \text{con} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Por consiguiente, si $Im(\tau) > 0$ tenemos que $Im(\gamma(\tau)) > 0$, luego la acción de $SL_2(\mathbb{Z})$ sobre $\widehat{\mathbb{C}}$ envía el plano superior en sí mismo. De hecho, para todo $\tau \in \mathbb{H}$ se cumple la siguiente cota

$$Im(\gamma(\tau)) \leq max\left\{Im(\tau), \frac{1}{Im(\tau)}\right\}.$$

Demostración. Observamos que $\mathrm{Im}(\gamma(\tau)) = \mathrm{Im}(a\tau + b/c\tau + d)$, multiplicando y dividiendo por el conjugado de $c\tau + d$ obtenemos que

$$\mathrm{Im}(\gamma(\tau)) = \mathrm{Im}\left(\frac{ac|\tau|^2 + bc\overline{\tau} + ad\tau + bd)}{|c\tau + d|^2}\right) = \frac{\mathrm{Im}(bc\overline{\tau} + ad\tau)}{|c\tau + d|^2},$$

teniendo en cuenta que $Im(\tau) = -Im(\overline{\tau})$ y que $ad - bc = 1$, concluimos que se cumple la igualdad. Empleando esta igualdad, si $|c\tau+d| \geq 1$ entonces $\mathrm{Im}(\gamma(\tau)) \leq \mathrm{Im}(\tau)$. Por otra parte si $|c\tau+d| < 1$ entonces necesariamente $c \neq 0$. Como $|\mathrm{Im}(c\tau+d)| \leq |c\tau+d|$ y $c \in \mathbb{Z}$ se cumple que

$$\frac{1}{|c\tau+d|^2} \leq \frac{1}{\mathrm{Im}(c\tau+d)^2} = \frac{1}{\mathrm{Im}(c\tau)^2} = \frac{1}{c^2\mathrm{Im}(\tau)^2}.$$

Por tanto, en este caso $\mathrm{Im}(\gamma(\tau)) \leq 1/\mathrm{Im}(\tau)$. □

2.2. Formas modulares respecto a $SL_2(\mathbb{Z})$

En esta sección estableceremos la definición de modularidad débil y de forma modular respecto a $SL_2(\mathbb{Z})$. Presentaremos varios ejemplos y estudiaremos algunas propiedades que nos permitan entender como actúan estas funciones en $\mathbb{H}$.

Definición 2.4. *Sean $k \in \mathbb{Z}$ y $f : \mathbb{H} \longrightarrow \mathbb{C}$ una función meromorfa. Se dice que es débilmente modular de peso k (respecto a $SL_2(\mathbb{Z})$) si*

$$\forall \tau \in \mathbb{H} \text{ y } \forall \gamma \in SL_2(\mathbb{Z}) \quad \text{se tiene que } f(\gamma(\tau)) = (c\tau+d)^k f(\tau),$$

donde (c,d) es la segunda fila de γ.

Claramente, las funciones constantes son débilmente modulares de peso 0 y la única función débilmente modular de peso k impar es la función nula porque $f = (-1)^k f$ tomando $\gamma = -I$. Para dar ejemplos no triviales de funciones que cumplen la condición de modularidad débil, vamos a estudiar algunas propiedades del factor que relaciona $f(\gamma(\tau))$ y $f(\tau)$ en la condición de modularidad.

Definición 2.5. *Sean $\gamma \in SL_2(\mathbb{Z})$ y $\tau \in H$. Llamaremos factor de automorfia a $j(\gamma,\tau) = c\tau + d$, donde (c,d) es la segunda fila de γ.*

Lema 2.6. *Para todo $\tau \in \mathbb{H}$ y para todo $\gamma, \gamma' \in SL_2(\mathbb{Z})$ se tiene que*

a) $j(\gamma\gamma', \tau) = j(\gamma, \gamma'(\tau))\, j(\gamma', \tau)$.

b) $\dfrac{d\gamma(\tau)}{d\tau} = \frac{1}{j(\gamma,\tau)^2}$.

Demostración. Dadas $\gamma, \gamma' \in SL_2(\mathbb{Z})$ con

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ y } \gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \text{ se tiene que } \gamma\gamma' = \begin{pmatrix} aa'+bc' & ab'+bd' \\ a'c+dc' & cb'+dd' \end{pmatrix}$$

a) Desarrollando los tres factores

$$j(\gamma\gamma', \tau) = (a'c+dc')\,\tau + (cb'+dd') \qquad j(\gamma', \tau) = c'\tau + d'$$
$$j(\gamma, \gamma'(\tau)) = \left(c\frac{a'\tau+b'}{c'\tau+d'} + d\right).$$

y multiplicando el segundo factor por el tercero obtenemos la igualdad con el primer factor.

b) Sea $\gamma(\tau) = (a\tau+b)/(c\tau+d)$, derivando se obtiene

$$\frac{d\gamma(\tau)}{d\tau} = \frac{a(c\tau+d) - c(a\tau+b)}{(c\tau+d)^2} = \frac{ad-cb}{(c\tau+d)^2} = \frac{1}{j(\gamma,\tau)^2}.$$

□

Veamos que si f cumple la condición de modularidad para un conjunto de elementos de $SL_2(\mathbb{Z})$, entonces también la cumple para el subgrupo que generan.

Corolario 2.7. *Sea $f : \mathbb{H} \to \mathbb{C}$ una función meromorfa. Si f cumple la condición de modularidad para $U = \{\gamma_1, \ldots, \gamma_q\} \subset SL_2(\mathbb{Z})$. Entonces f cumple la condición de modularidad para $\langle \gamma_1, \ldots, \gamma_q \rangle$.*

Demostración. Primero vamos a probar que cumple la condición de modularidad para $\rho = \gamma_1^{r_1}$. Como f cumple la condición de modularidad para γ_1 entonces podemos descomponer $f(\rho(\tau))$ como

$$f(\rho(\tau)) = f(\gamma_1^{r_1}(\tau)) = f(\gamma_1(\gamma_1^{r_1-1}(\tau)) = j(\gamma_1, \gamma_1^{r_1-1}(\tau))^k f(\gamma_1^{r_1-1}(\tau)).$$

Iterando el proceso $r_1 - 1$ veces obtenemos que

$$f(\rho(\tau)) = (j(\gamma_1, \gamma_1^{r_1-1}(\tau)) j(\gamma_1, \gamma_1^{r_1-2}(\tau)) \cdots j(\gamma_1, \tau))^k f(\tau).$$

Aplicando la parte a) del lema anterior $j(\gamma_1, \gamma_1(\tau)) j(\gamma_1, \tau) = j(\gamma_1^2, \tau)$, por tanto iterando este proceso r_1 veces se puede deducir que

$$f(\rho(\tau)) = j(\gamma_1^{r_1}, \tau)^k f(\tau).$$

Por ende, f cumple la condición de modularidad para $\rho = \gamma_1^{r_1}$. Aplicando el mismo procedimiento, se puede probar de forma directa que f cumple la propiedad de modularidad para $\rho = \gamma_1^{r_1} ... \gamma_q^{r_q}$, cualquier combinación lineal de U. □

En particular, gracias a la Proposición 2.2 sabemos que el grupo modular está generado por α y β. Por el Corolario 2.7 se prueba que si f cumple la condición anterior para α y β, entonces lo cumple para todo $\gamma \in SL_2(\mathbb{Z})$. Por tanto, podemos afirmar que f es función débilmente modular de peso k si y solo si para todo $\tau \in \mathbb{C}$, $f(\tau+1) = f(\tau)$ y $f(-1/\tau) = \tau^k f(\tau)$.
Para precisar la noción de forma modular necesitamos establecer una noción adecuada de holomorfía en infinito para las funciones que estamos considerando. Para ello, transformamos el semiplano superior en el disco punteado como se muestra en el siguiente lema.

Lema 2.8. *Sea $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$ y $\mathbb{D}' = \mathbb{D} \setminus \{0\}$. Consideramos la función $\mathbb{Z}-$periódica $\varphi : \mathbb{H} \longrightarrow \mathbb{D}'$ dada por $\varphi(\tau) = e^{2\pi i \tau}$. Entonces*

a) dado $a \in \mathbb{R}$ se cumple que $\lim_{\tau \to a} \varphi(\tau) = e^{2\pi i a} \in \delta\mathbb{D}$.

b) Se tiene que $\lim_{Im(\tau) \to \infty} \varphi(\tau) = 0$.

Empleamos esta función auxiliar para asociar a toda función holomorfa en $\mathbb{H}$ una función sobre el disco.

Definición 2.9. *Sea $f : \mathbb{H} \to \mathbb{C}$ una función meromorfa y débilmente modular de peso $k \in \mathbb{Z}$. Definimos $g = g_f : \mathbb{D}' \to \mathbb{C}$, la aplicación (sobre el disco) asociada a f por*

$$g(q) = f(\varphi^{-1}(q)) = f\left(\frac{log(q)}{2\pi i}\right).$$

Obsérvese que como f es débilmente modular y como $\alpha \in SL_2(\mathbb{Z})$, $f(\tau+1) = f(\tau)$, es decir, f es $\mathbb{Z}-$periódica y, por tanto, g está bien definida. Si además f es holomorfa en $\mathbb{H}$, tenemos que g es holomorfa en $\mathbb{D}'$ porque el logaritmo es una función holomorfa en un entorno de cada punto. Por tanto, g admite un desarrollo de Laurent en $\mathbb{D}'$.

Definición 2.10. *Sea $f : \mathbb{H} \to \mathbb{C}$ holomorfa y débilmente modular de peso $k \in \mathbb{Z}$. Decimos que f es holomorfa en infinito si la función asociada $g : \mathbb{D}' \to \mathbb{C}$ se extiende de manera holomorfa a $q = 0$, es decir, si g tiene una singularidad evitable en el origen.*

Esta definición de función holomorfa en infinito es diferente a la noción habitual, en este caso solo requiere que f se comporte de forma adecuada cuando nos aproximamos a infinito desde el semiplano superior. Empleando estas definiciones, estamos en disposición de introducir la noción de forma modular.

Definición 2.11. *Sean $k \in \mathbb{Z}$ y $f : \mathbb{H} \longrightarrow \mathbb{C}$. Se dice que es una forma modular de peso k si*

a) f es holomorfa en $\mathbb{H}$.

b) f es débilmente modular de peso k.

c) f es holomorfa en infinito.

El conjunto de formas modulares de peso k se denota por $M_k(SL_2(\mathbb{Z}))$.

Nótese que si f es holomorfa en infinito, es decir, si g es holomorfa en $q=0$, podemos restringir su desarrollo de Laurent en el origen a una suma sobre los naturales $g(q)=\sum_{n\in\mathbb{Z}} a_n q^n$. Por tanto, la función f admite un desarrollo en serie de Fourier

$$\text{para cada } \tau\in\mathbb{H} \text{ se cumple que } f(\tau)=g(\varphi(\tau))=\sum_{n=0}^{\infty} a_n(f)e^{2\pi i\tau n}.$$

Veamos que la holomorfía en infinito se puede caracterizar en términos de un límite.

Teorema 2.12. *Sea f una función débilmente modular y holomorfa en $\mathbb{H}$. Entonces f es holomorfa en infinito si y solo si existe el $\lim_{Im(\tau)\to\infty} f(\tau)$ y es finito.*

Demostración. Para empezar suponemos que f es holomorfa en infinito lo cual implica que g se extiende de manera holomorfa a 0 y por tanto que g es continua cuando $q=0$. Por el Lema 2.8, se tiene que $\lim_{\mathrm{Im}(\tau)\to\infty}\varphi(\tau)=0$. Luego

$$\lim_{\mathrm{Im}(\tau)\to\infty} f(\tau)=\lim_{\mathrm{Im}(\tau)\to\infty} g(\varphi(\tau))=\lim_{q\to 0} g(q),$$

el cual existe y es finito porque g es continua en $q=0$.
Recíprocamente, por hipótesis como existe el $\lim_{\mathrm{Im}(\tau)\to\infty} f(\tau)$ y es finito podemos afirmar que g tiene una singularidad evitable en $q=0$, luego en el origen se extiende de manera holomorfa, por consiguiente f es una función holomorfa en infinito. □

El ejemplo, no trivial, más simple de formas modulares viene dado por las series de Eisenstein. Para probar que son formas modulares necesitamos un par de resultados auxiliares previos. Para el desarrollo de este ejemplo se han seguido las notas de K. Conrad [2].

Lema 2.13. *La serie*

$$\sum_{(c,d)\in\left(\mathbb{Z}^2\right)^*} \frac{1}{\left(\sqrt{c^2+d^2}\right)^3}$$

converge donde $\left(\mathbb{Z}^2\right)^*=\mathbb{Z}^2\setminus\{(0,0)\}$.

Demostración. Sea $a=(c,d)$ denotamos $|a|_2=\sqrt{c^2+d^2}$. Para $n\in\mathbb{N}_{\geq 1}$ consideramos la función de conteo $r_2(n)=\#\left\{a\in(\mathbb{Z}^2)^*:\ |a|_2^2=n\right\}$ y vemos que

$$\sum_{a\in\left(\mathbb{Z}^2\right)^*}\frac{1}{|a|_2^3}=\sum_{a\in\left(\mathbb{Z}^2\right)^*}\frac{1}{\left(|a|_2^2\right)^{3/2}}=\sum_{n=1}^{\infty}\frac{r_2(n)}{n^{3/2}}=\lim_{N\to\infty}\sum_{n=1}^{N}\frac{r_2(n)}{n^{3/2}}.$$

Para ello, consideramos el conjunto $S(n)=\#\left\{a\in(\mathbb{Z}^2)^*:\ |a|_2^2\leq n\right\}$ para cada $n\in\mathbb{N}_{\geq 1}$. Por tanto $r_2(n)=S(n)-S(n-1)$ y, por ende, se tiene que

$$\sum_{n=1}^{N}\frac{r_2(n)}{n^{3/2}}=\sum_{n=1}^{N}\frac{S(n)-S(n-1)}{n^{3/2}}.$$

Estas series de tipo telescópico se pueden sumar empleando la siguiente fórmula que puede considerarse la versión discreta de la fórmula de integración por partes

$$\sum_{n=1}^{N}u_n(v_n-v_{n-1})=u_Nv_N-u_1v_0-\sum_{n=1}^{N-1}v_n(u_{n+1}-u_n).$$

Aplicando la fórmula para $u_n=1/n^{3/2}$ y $v_n=S(n)$ y, teniendo en cuenta que $v_0=0$, observamos que

$$\sum_{n=1}^{N}\frac{S(n)-S(n-1)}{n^{3/2}}=\frac{S(N)}{N^{3/2}}-\sum_{n=1}^{N-1}S(n)\left(\frac{1}{(n+1)^{3/2}}-\frac{1}{n^{3/2}}\right).$$

Escribiendo la diferencia entre $1/(n+1)^{3/2}$ y $1/(n)^{3/2}$ como una integral usando el teorema fundamental del cálculo, obtenemos que

$$\frac{S(N)}{N^{3/2}}-\sum_{n=1}^{N-1}S(n)\left(\frac{1}{(n+1)^{3/2}}-\frac{1}{n^{3/2}}\right)=\frac{S(N)}{N^{3/2}}+\frac{3}{2}\sum_{n=1}^{N-1}\int_n^{n+1}\frac{S(n)}{x^{5/2}}dx.$$

Dado que queremos agrupar las integrales en una única expresión necesitamos extender la función S a todo $x \in \mathbb{R}$ con $x \geq 1$. Para ello, consideramos la función escalonada $S(x) = \#\left\{a \in (\mathbb{Z}^2)^* : \ 1 \leq |a|_2^2 \leq x\right\}$ para cada $x \geq 1$. Luego $S(x) = S(n)$ para $n \leq x < n+1$ y por tanto

$$\frac{S(N)}{N^{3/2}} + \frac{3}{2}\sum_{n=1}^{N-1}\int_n^{n+1}\frac{S(n)}{x^{5/2}}dx = \frac{S(N)}{N^{3/2}} + \frac{3}{2}\int_1^N \frac{S(x)}{x^{5/2}}dx.$$

Para estimar el valor de $S(x)/x^{5/2}$ vamos a acotar $S(x)$ basándonos en su interpretación geométrica. El número $S(x)$ cuenta el número de puntos de coordenadas enteras no nulas en la bola centrada en el origen y radio $\sqrt{x}$. El número de enteros entre $-R \leq n \leq R$ es $2\lfloor R \rfloor + 1$ y cuando $R \geq 1$ tenemos que $R \leq 2\lfloor R \rfloor + 1 \leq 3R$. Por tanto se cumple que

$$R^2 \leq \#\left\{(a_1,a_2) \in (\mathbb{Z}^2)^* : \ 1 \leq |(a_1,a_2)|_\infty \leq R\right\} \leq 9R^2.$$

Como $|(a_1,a_2)|_\infty \leq |(a_1,a_2)|_2 \leq \sqrt{2}|(a_1,a_2)|_\infty$ tomando $x = R^2$ tenemos que $x/2 \leq S(x) \leq 9x$. Por ende, se tiene que

$$0 \leq \frac{S(N)}{N^{3/2}} + \frac{3}{2}\int_1^N \frac{S(x)}{x^{5/2}}dx \leq \frac{9}{N^{1/2}} + \frac{27}{2}\int_1^\infty \frac{dx}{x^{3/2}}dx = \frac{9}{N^{1/2}} + \frac{27}{4}$$

luego la sucesión de sumas parciales converge y la serie original también. □

Enunciamos el segundo resultado auxiliar.

Lema 2.14. *Sea $\Omega_{A,B} = \{\tau \in \mathbb{H} : |Re(\tau)| \leq A, \ Im(\tau) \geq B\}$ donde $A > 0$ y $B > 0$. Entonces existe un $C > 0$ tal que para todo $\tau \in \Omega$ todo $\delta \in \mathbb{R}$ se tiene que*

$$|\tau + \delta| \geq C \cdot sup\{1, |\delta|\}.$$

Demostración. Esta demostración se divide en cuatro casos

1. Si $|\delta| < 1$, entonces $|\tau+\delta| \geq \mathrm{Im}(\tau+\delta) = \mathrm{Im}(\tau) \geq B = B \cdot sup\{1,|\delta|\}$.
2. Si $1 \leq |\delta| \leq 3A$ y $\mathrm{Im}(\tau) \geq A$, entonces

$$|\tau+\delta| = \sqrt{(Re(\tau)+\delta)^2 + \mathrm{Im}(\tau)^2} \geq \sqrt{\mathrm{Im}(\tau)^2} \geq A \geq |\delta|/3 = (1/3)\cdot sup\{1,|\delta|\}.$$

3. Si $1 \leq |\delta| \leq 3A$ y $\mathrm{Im}(\tau) \leq A$. Considerando la función $\tau \mapsto |\tau+\delta|/|\delta|$, alcanza un mínimo $m > 0$, por ende $|\tau+\delta| \geq m|\delta| \geq m \cdot sup\{1,|\delta|\}$.
4. Si $|\delta| > 3A$, entonces

$$|\tau+\delta| \geq |\delta| - A \geq \frac{2}{3}|\delta| = \frac{2}{3}sup\{1,|\delta|\}.$$

Por tanto, considerando $C = min\{B, 1/3, m\}$ obtenemos la cota. □

Empleando estos resultados podemos detallar un ejemplo no trivial de forma modular.

Ejemplo 2.15. *Sea $k \in \mathbb{N}_{\geq 3}$. Definimos la Serie de Eisenstein de peso k para $\tau \in \mathbb{H}$ como*

$$G_k(\tau) = \sum_{(c,d)\in(\mathbb{Z}^2)^*} \frac{1}{(c\tau+d)^k}.$$

Nuestro objetivo es probar que $G_k(\tau)$ es una forma modular de peso k. Para empezar vamos a probar que la función es holomorfa en $\mathbb{H}$ para ello primero definimos

$$g_k = \sum_{(c,d)\in(\mathbb{Z}^2)^*} \frac{1}{sup\{|c|,|d|\}^k}.$$

Como $sup\{|c|,|d|\} \geq (\sqrt{2}/2)\sqrt{c^2+d^2}$ *vemos que*

$$g_k \leq g_3 \leq \sum_{(c,d)\in(\mathbb{Z}^2)^*} \frac{2\sqrt{2}}{\sqrt{c^2+d^2}^3},$$

por tanto gracias al Lema 2.13 podemos afirmar que es una serie convergente.
Dividimos $G_k(\tau)$ *en dos sumas tal que*

$$G_k(\tau) = \sum_{(c,d)\in(\mathbb{Z}^2)^*,\ c=0} \frac{1}{(c\tau+d)^k} + \sum_{(c,d)\in(\mathbb{Z}^2)^*,\ c\neq 0} \frac{1}{(c\tau+d)^k}$$

observamos que la primera suma es dos veces la función zeta de Riemann en k $(\zeta(k))$*, luego convergente. Dado* $\tau \in \Omega_{A,B}$*, teniendo en cuenta el Lema 2.14 y realizando el cambio de variable* $\delta = d/c$ *observamos que*

$$\begin{aligned}\sum_{(c,d)\in(\mathbb{Z}^2)^*,\ c\neq 0} \frac{1}{|c\tau+d|^k} &= \sum_{(c,d)\in(\mathbb{Z}^2)^*,\ c\neq 0} \frac{1}{|c|^k|\tau+\delta|^k} \leq \sum_{(c,d)\in(\mathbb{Z}^2)^*,\ c\neq 0} \frac{1}{|c|^k C^k sup\{1,|\delta|\}^k} \\ &= \frac{1}{C^k} \sum_{(c,d)\in(\mathbb{Z}^2)^*,\ c\neq 0} \frac{1}{sup\{|c|,|d|\}^k} = \frac{g_k}{C^k}.\end{aligned}$$

Por lo demostrado anteriormente podemos afirmar que la segunda suma también converge. Por tanto por el teorema de comparación de Wiestrass podemos concluir que $G_k(\tau)$ *es absoluta y uniformemente convergente para cualquier punto de* $\Omega_{A,B}$*. Teniendo en cuenta que A y B son fijos pero arbitrarios entonces* $G_k(\tau)$ *es absoluta y uniformemente convergente en un entorno de todo punto* $\tau \in \mathbb{H}$*. Por consiguiente,* $G_k(\tau)$ *es holomorfa en* $\mathbb{H}$*. Para ver la condición de holomorfía en infinito hay que calcular* $lim_{Im(\tau)\to\infty} G_k(\tau)$*, como es una suma absolutamente convergente podemos introducir el limite dentro del sumatorio y así obtener que el limite es igual a* $\zeta(k)$*. Por tanto,* $G_k(\tau)$ *es holomorfa en infinito. Para finalizar hay que comprobar que* $G_k(\tau)$ *cumple la condición de modularidad. Dado* $\gamma \in SL_2(\mathbb{Z})$ *se tiene que*

$$G_k(\gamma(\tau)) = \sum_{(c',d')\in(\mathbb{Z}^2)^*} \frac{1}{\left(c'\left(\frac{a\tau+b}{c\tau+d}\right)+d'\right)^k} = (c\tau+d)^k \sum_{(c',d')\in(\mathbb{Z}^2)^*} \frac{1}{\left(\left(c'a+cd'\right)\tau+d'd+c'b\right)^k}.$$

Denominando $\widehat{c} = c'a+cd'$ *y* $\widehat{d} = c'b+d'd$*. Observamos que existe una biyección en* $(\mathbb{Z}^2)^*$ *que envía* (c',d') *en* $(\widehat{c},\widehat{d})$ *dado que* γ *es invertible y que*

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} c' \\ d' \end{pmatrix} = \begin{pmatrix} \widehat{c} \\ \widehat{d} \end{pmatrix}.$$

En conclusión, $G_k(\gamma(\tau)) = (c\tau+d)^k G_k(\tau)$*, es decir, podemos afirmar que es una función modular.*

Terminamos el capítulo enunciando algunas propiedades algebraicas del conjunto de formas modulares.

Proposición 2.16. $M_k(SL_2(\mathbb{Z}))$ *forma un* $\mathbb{C}$*-espacio vectorial.*

Demostración. Las condiciones sobre holomorfía se preservan para la suma y el producto por escalares. Por tanto solo debemos comprobar la modularidad, la cual se comprueba de forma directa sacando factor común al factor de automorfia. □

Proposición 2.17.

a) El producto de una forma modular de peso k y otra de peso m es una forma modular de peso $k+m$*.*

b) $M(SL_2(\mathbb{Z})) = \oplus_{k\in\mathbb{Z}} M_k(SL_2(\mathbb{Z}))$ *es un* $\mathbb{C}$*-álgebra.*

Demostración. Las condiciones sobre holomorfía se preservan sobre el producto de funciones holomorfas, además teniendo en cuenta que $(c\tau+d)^m(c\tau+d)^k = (c\tau+d)^{m+k}$ la primera parte de la proposición queda demostrada. Utilizando a) y que para todo $k \in \mathbb{Z}$ $M_k(SL_2(\mathbb{Z}))$ es un $\mathbb{C}$ espacio vectorial obtenemos la segunda parte de la proposición. □

Definición 2.18. *Una forma cuspidal de peso k es una forma modular de peso k cuyo termino independiente en su serie de Fourier es nulo, es decir $a_0(f) = 0$. El conjunto de funciones cuspidales de peso k se denota por $S_k(SL_2(\mathbb{Z}))$.*

Proposición 2.19.

a) $S_k(SL_2(\mathbb{Z}))$ forma un subespacio vectorial de $M_k(SL_2(\mathbb{Z}))$.

b) $S(SL_2(\mathbb{Z})) = \oplus_{k\in\mathbb{Z}} S_k(SL_2(\mathbb{Z}))$ es un ideal de $M(SL_2(\mathbb{Z}))$.

Demostración. Se comprueba de forma directa que $S_k(SL_2(\mathbb{Z}))$ es cerrado para la suma y el producto por escalares dado que el término independiente de la serie de Fourier resultante se obtiene realizando la combinación lineal oportuna de los términos independientes. Del mismo modo, si el termino independiente de una de las series es cero su producto también tiene termino independiente nulo luego $S(SL_2(\mathbb{Z}))$ es un ideal. □

2.3. Modularidad respecto a subgrupos de congruencias

En determinadas ocasiones no podemos garantizar que la condición de modularidad se cumpla para todos los elementos de $SL_2(\mathbb{Z})$. En esta sección vamos a generalizar los conceptos de función modular débil y forma modular a un tipo particular de subgrupos propios de $SL_2(\mathbb{Z})$, los subgrupos de congruencias.

Definición 2.20. *Sea $n \in \mathbb{N}_{\geq 1}$. Llamamos subgrupo principal de congruencias de nivel n a*

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

Entendiendo que la congruencia de matrices es entrada a entrada, es decir, que $a \equiv 1 \mod n$, $b \equiv 0 \mod n$, $c \equiv 1 \mod n$ y $d \equiv 0 \mod n$. Cabe destacar el caso particular en el que $n = 1$, se tiene que $\Gamma(1) = SL_2(\mathbb{Z})$.

Proposición 2.21. *Para cada $n \in \mathbb{N}_{\geq 1}$ tenemos que $\Gamma(n)$ es un subgrupo de $SL_2(\mathbb{Z})$.*

Demostración. Por construcción notamos que $\Gamma(n)$ está contenido en $SL_2(\mathbb{Z})$ y que es no vacío porque $I \in \Gamma(n)$.

$$\text{Dadas } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ y } \gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \text{ se cumple que } \gamma^{-1}\gamma' = \begin{pmatrix} da' - bc' & db' - bd' \\ -a'c + ac' & -cb' + ad' \end{pmatrix}.$$

Teniendo en cuenta que la suma de las clases módulo n es la clase de la suma y que el producto de las clases es la clase del producto comprobamos que $\gamma^{-1}\gamma' \in \Gamma(n)$. Por tanto, es subgrupo de $SL_2(\mathbb{Z})$. □

Definición 2.22. *Diremos que un subgrupo $\Gamma \subseteq SL_2(\mathbb{Z})$ es un subgrupo de congruencias si contiene un subgrupo principal de congruencias, es decir, si existe $n \in \mathbb{N}_{\geq 1}$ tal que $\Gamma(n) \subseteq \Gamma$. En dicho caso, decimos que Γ es un subgrupo de congruencias de nivel n.*

En el siguiente ejemplo vamos a introducir algunos subgrupos de congruencias los cuales tomarán especial relevancia a la hora de construir isomorfismos entre espacios de moduli en la Sección 4.1.

Ejemplo 2.23. *Dado $n \in \mathbb{N}_{\geq 1}$ consideramos*

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\mod n) \right\},$$

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} (\mod n) \right\},$$

donde $*$ denota cualquier número entero no especificado.

Proposición 2.24. *Para cada $n \in \mathbb{N}_{\geq 1}$ se cumple que $\Gamma(n) \lhd \Gamma_1(n)$, $\Gamma_1(n) \lhd \Gamma_0(n)$, $\Gamma_0(n) \lhd SL_2(\mathbb{Z})$*

Demostración. Definimos la siguiente aplicación

$$\Gamma_1(n) \longrightarrow (\mathbb{Z}/n\mathbb{Z}) \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b \mod n.$$

El núcleo de esta aplicación son las matrices que pertenecen a $\Gamma_1(n)$ y que $b \equiv 0 \mod n$ que por definición es $\Gamma(n)$. Por tanto, $\Gamma(n)$ es un subgrupo normal de $\Gamma_1(n)$. Por otra parte, consideramos la aplicación

$$\Gamma_0(n) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \mod n.$$

El núcleo está formado por las matrices que pertenecen a $\Gamma_0(n)$ tal que $d \equiv 1 \mod n$. Además sabemos que el determinante de la matriz tiene que ser congruente con $1 \mod n$. Por consiguiente como $c \equiv 0 \mod n$ y $d \equiv 1 \mod n$ entonces $a \equiv 1 \mod n$ y por tanto el núcleo de la aplicación es $\Gamma_1(n)$. En otras palabras $\Gamma_1(n)$ es subgrupo normal de $\Gamma_0(n)$. Para finalizar construimos la aplicación

$$SL_2(\mathbb{Z}) \longrightarrow (\mathbb{Z}/n\mathbb{Z}) \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto c \mod n$$

cuyo núcleo está formado por $\Gamma_0(n)$ y por tanto $\Gamma_0(n)$ es subgrupo normal de $SL_2(\mathbb{Z})$. □

Una vez vistos una serie de ejemplos de subgrupos de congruencias enunciamos una propiedad importante a la hora de construir las cartas de las curvas modulares en el Capítulo 5.

Proposición 2.25. *Sea Γ un subgrupo de congruencias de nivel N con $N \in \mathbb{N}_{\geq 1}$. Entonces $[SL_2(\mathbb{Z}) : \Gamma]$ es finito.*

Demostración. Como Γ es un subgrupo de congruencias de nivel N entonces $\Gamma(N) \subseteq \Gamma$. Se puede comprobar de forma directa que $\Gamma(N) \lhd SL_2(\mathbb{Z})$. En este caso, construimos la aplicación $f : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ donde $f(\gamma) = \gamma \mod N$. Se puede probar de manera sencilla que es un homomorfismo de grupos y cuyo $Ker(f) = \Gamma(N)$. Por tanto aplicando el primer teorema de isomorfía obtenemos que $SL_2(\mathbb{Z})/\Gamma(N) \approx SL_2(\mathbb{Z}/N\mathbb{Z})$. Por ende

$$[SL_2(\mathbb{Z}) : \Gamma(N)] = |SL_2(\mathbb{Z}/N\mathbb{Z})| < N^4$$

y podemos concluir que $[SL_2(\mathbb{Z}) : \Gamma]$ es finito, porque $[SL_2(\mathbb{Z}) : \Gamma] \leq [SL_2(\mathbb{Z}) : \Gamma(N)]$. □

Estamos en disposición de establecer la noción de modularidad respecto a un subgrupo de congruencias.

Definición 2.26. *Sean $k \in \mathbb{Z}$, Γ un subgrupo de congruencias de $SL_2(\mathbb{Z})$ de nivel $N \in \mathbb{N}_{\geq 1}$ y $f : \mathbb{H} \to \mathbb{C}$ una función meromorfa. Decimos que f es función débilmente modular de peso k y nivel N con respecto a Γ, si para todo $\gamma \in \Gamma$ y para todo $\tau \in \mathbb{H}$*

$$j(\gamma, \tau)^{-k} f(\gamma(\tau)) = f(\tau).$$

Ahora vamos a considerar un subgrupo propio de $SL_2(\mathbb{Z})$ y vamos a dar un ejemplo de una función modular débil sobre ese subgrupo pero que no cumple las condiciones de modularidad sobre $SL_2(\mathbb{Z})$.

Ejemplo 2.27. *El subgrupo que vamos a considerar es*

$$\Gamma_\theta = \left\langle \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \right\rangle$$

Este subgrupo tiene una relevancia importante en teoría de números dada su relación con el número de formas posibles de descomponer un número natural como suma de cuatro cuadrados. Al número de formas de descomponer $n \in \mathbb{N}$ en $k \in \mathbb{N}_{\geq 1}$ cuadrados enteros lo denotamos por

$$r(n,k) = \# \left\{ v \in \mathbb{Z}^k : n = \sum_{i=1}^{k} v_i^2 \right\}.$$

Obsérvese que $r(0,1) = 1$, $r(n,1) = 2$ si $n \in \mathbb{N}_{\geq 1}$ es un cuadrado y $r(n,1) = 0$ si n no es un cuadrado. Nótese también que la definición de $r(n,k)$ se tiene en cuenta el orden de los sumandos de modo que $r(1,2) = 4$

porque $1=(0)^2+(\pm 1)^2$ *y* $1=(\pm 1)^2+(0)^2$. *Para cada* $k\in\mathbb{N}_{\geq 1}$ *definimos la función generatriz de la sucesión* $(r(n,k))_{n=0}^{\infty}$ *como*

$$\theta(\tau,k)=\sum_{n=0}^{\infty} r(n,k)q^n,$$

donde $q=e^{2\pi i\tau}$ *con* $\tau\in\mathbb{H}$. *Acotando de un modo rudimentario* $r(n,k)\leq(2n+1)^k$, *luego* $\theta(\tau,k)$ *es holomorfa en* $\mathbb{H}$. *En concreto, estamos interesados en estudiar la función generatriz para* $k=4$, *es decir, queremos ver que* $\theta(\tau,4)$ *cumple la condición de modularidad para* Γ_θ *pero no para* $SL_2(\mathbb{Z})$.
Antes de pasar a la demostración listamos una serie de propiedades de $\theta(\tau,k)$ *y* $r(n,k)$ *cuya demostración es directa pero laboriosa.*

- *Si* $k_1+k_2=k$, *entonces* $r(n,k)=\sum_{l+m=n} r(l,k_1)r(m,k_2)$.
- *Para todo* $\tau\in\mathbb{H}$ *se tiene que* $\theta(\tau,k_1)\theta(\tau,k_2)=\theta(\tau,k_1+k_2)$.
- *La función* θ *es* $\mathbb{Z}$ *periódica, es decir,* $\theta(\tau+1,k)=\theta(\tau,k)$ *para todo* $\tau\in\mathbb{H}$.
- *Se cumple la ley de transformación*

$$\theta(-1/(4\tau),1)=\sqrt{-2\tau i}\,\theta(\tau,1).$$

  Como $-2i\tau$ *está en el semiplano de la derecha cuando* $\tau\in\mathbb{H}$, *la fórmula tiene sentido cuando consideramos la rama principal de la raíz.*

Por simplicidad, denotamos $\theta(\tau,1)=\theta(\tau)$. *Observamos que*

$$\theta(\tau)=\sum_{d=-\infty}^{\infty} e^{2\pi i d^2\tau}=1+2q+2q^4+2q^9+2q^{16}+\cdots+2q^{d^2}+O(q^{d^2}).$$

Aplicando las propiedades mencionadas con anterioridad y realizando el cambio de variable dado por $\eta=-1-(1/(4\tau))$ *obtenemos que*

$$\begin{aligned}\theta(\tau/(4\tau+1))&=\theta(-1/(4\eta))=\sqrt{-2\eta i}\,\theta(\eta)=\sqrt{2(1+(1/4\tau))i}\,\theta(-1-(1/4\tau))\\&=\sqrt{2(1+(1/4\tau))i}\,\theta(-(1/4\tau))=\sqrt{2(1+(1/4\tau))i}\sqrt{-2\tau i}\,\theta(\tau)\\&=\sqrt{4\tau(1+(1/4\tau))}\,\theta(\tau)=\sqrt{4\tau+1}\,\theta(\tau).\end{aligned}$$

Empleando esta formula podemos probar que $\theta(\tau,4)$ *es una función modular débil de peso 2 respecto a* Γ_θ. *Para ello por el Corolario 2.7 basta probar que cumple la condición de modularidad para los cuatro generadores. Considerando las matrices que generan* Γ_θ *tenemos que estudiar la condición de modularidad para las transformaciones* $\tau\mapsto\tau+1$ *y* $\tau\mapsto\tau/(4\tau+1)$.
Empleando las propiedades anteriores

$$\theta\left(\frac{\tau}{4\tau+1},4\right)=\theta\left(\frac{\tau}{4\tau+1}\right)^4=(4\tau+1)^2\theta(\tau)^4=(4\tau+1)^2\theta(\tau,4)\quad y\quad \theta(\tau+1,4)=\theta(\tau,4).$$

De un modo análogo a las formas modulares, establecemos la definición de forma modular respecto a un subgrupo de congruencias. Para ello, necesitamos adaptar en primer lugar la noción de holomorfía en infinito dado que no podemos garantizar que f sea $\mathbb{Z}-$periódica. Sin embargo, observamos que como Γ es un subgrupo de congruencias entonces existe un $h\in\mathbb{N}_{\geq 1}$ tal que $\Gamma(h)\subseteq\Gamma$ y por tanto α^h está contenido en Γ. Sabemos que α^h se corresponde con la transformación $\alpha^h(\tau)=\tau+h$. En consecuencia, toda función modular respecto a Γ es $h\mathbb{Z}$-periódica. Al igual que en la Definición 2.9, consideramos la aplicación $\varphi_h:\mathbb{H}\longrightarrow\mathbb{D}'$ dada por $\varphi_h(\tau)=e^{\frac{2\pi i\tau}{h}}$. Gracias a esto, podemos construir una función débilmente modular y holomorfa en $\mathbb{D}'$ $g_h:\mathbb{D}'\longrightarrow\mathbb{C}$ dada por $g_h(q)=f\left(log(q)h/(2\pi i)\right)$. Por tanto, razonando como en la Sección 2.2 podemos concluir que f es holomorfa en infinito si g se extiende de manera holomorfa a $\mathbb{D}$. Se puede comprobar que la definición no depende del $h\in\mathbb{N}_{\geq 1}$ elegido siempre que $\alpha^h\in\Gamma$. Por simplicidad, usaremos la notación $[\gamma]_k$ para referirnos al operador de peso k que actúa sobre f como $f[\gamma]_k(\tau)=j(\gamma,\tau)^{-k}f(\gamma(\tau))$ para todo $\gamma\in SL_2(\mathbb{Z})$ y para todo $\tau\in\mathbb{H}$. Recordamos que $j(\gamma,\tau)=c\tau+d$. Con esta notación establecemos la definición.

Definición 2.28. *Sean Γ un subgrupo de congruencias de $SL_2(\mathbb{Z})$ y $k \in \mathbb{Z}$. Una función $f : \mathbb{H} \to \mathbb{C}$ es una forma modular de peso k con respecto a Γ si*

a) f es una función holomorfa en $\mathbb{H}$.

b) f es una función modular de peso k con respecto a Γ.

c) Para todo $\gamma \in SL_2(\mathbb{Z})$ se tiene que $f[\gamma]_k$ es holomorfa en infinito.

El conjunto de todas las formas modulares de peso k respecto a Γ se denota por $M_k(\Gamma)$.

Nótese que en la tercera condición no nos limitamos a exigir que f sea holomorfa en infinito, dado que para preservar una estructura adecuada en $M_k(\Gamma)$ necesitamos ser más restrictivos con los requerimientos. En este caso podemos garantizar que la condición de holomorfía en el infinito sobre $f[\gamma]_k$ tiene sentido gracias al siguiente resultado.

Proposición 2.29. *Sean Γ un subgrupo de congruencias, $\gamma \in SL_2(\mathbb{Z})$, $k \in \mathbb{Z}$ y f una función holomorfa en $\mathbb{H}$ y débilmente modular de peso k con respecto a Γ. Entonces $\gamma^{-1}\Gamma\gamma$ es un subgrupo de congruencias y $f[\gamma]_k$ es una función holomorfa en $\mathbb{H}$ y débilmente modular de peso k con respecto a $\gamma^{-1}\Gamma\gamma$.*

Demostración. Como $\Gamma(N) \lhd SL_2(\mathbb{Z})$ deducimos que $\gamma\Gamma(N)\gamma^{-1} \subseteq \Gamma(N)$ y, por ende, que $\Gamma(N) \subseteq \gamma^{-1}\Gamma(N)\gamma$. Por tanto, $\Gamma(N) \subseteq \gamma^{-1}\Gamma\gamma$ y concluimos que $\gamma^{-1}\Gamma\gamma$ es un subgrupo de congruencias. En relación a la segunda parte de la proposición, $f[\gamma]_k$ es composición de funciones holomorfas en $\mathbb{H}$ y por tanto es holomorfa en $\mathbb{H}$. Para ver que cumple la condición de modularidad, tomamos $\gamma^{-1}\beta\gamma \in \gamma^{-1}\Gamma\gamma$ y vemos que

$$f[\gamma]_k(\gamma^{-1}\beta\gamma(\tau)) = j(\gamma, \gamma^{-1}\beta\gamma(\tau))^{-k} f(\beta\gamma(\tau)). \tag{2.1}$$

Aplicando la propiedad a) del Lema 2.6 deducimos las siguientes igualdades

$$j(\gamma, \gamma^{-1}\beta\gamma(\tau)) = j(\beta\gamma, \tau) j(\gamma^{-1}\beta\gamma, \tau)^{-1} \quad \text{y} \quad j(\beta\gamma, \tau) = j(\beta, \gamma(\tau)) j(\gamma, \tau).$$

Ahora aplicando las igualdades anteriores a (2.1) deducimos que

$$f[\gamma]_k(\gamma^{-1}\beta\gamma(\tau)) = j(\gamma^{-1}\beta\gamma, \tau)^k j(\gamma, \tau)^{-k} f(\gamma(\tau)) = j(\gamma^{-1}\beta\gamma, \tau)^k f[\gamma]_k.$$

Por tanto, $f[\gamma]_k$ cumple la condición de modularidad respecto a $\gamma^{-1}\Gamma\gamma$. □

Observamos que la tercera condición se ha enunciado de manera independiente al subgrupo de congruencias Γ. Sin embargo, en la practica sólo necesitamos comprobar que se satisface para un número finito de $\alpha_j \in SL_2(\mathbb{Z})$, los representantes de las clases laterales de $SL_2(\mathbb{Z})$ módulo Γ. En otras palabras, dado $\gamma \in SL_2(\mathbb{Z}) = \cup_{j=1}^{k} \Gamma\alpha_j$ tenemos que $\gamma = \varphi\alpha_j$ para algún $\varphi \in \Gamma$ y algún $j \in \{1, \ldots, k\}$, luego por la condición de modularidad $f[\gamma]_k = f[\varphi\alpha_j]_k = f[\alpha_j]_k$. En cierto modo, esta observación nos permite decir que la tercera condición representa la holomorfía en los puntos limites. Para precisar la noción de punto límite necesitamos identificar los puntos de $\mathbb{Q} \cup \{\infty\}$ módulo Γ.

Definición 2.30. *Sea $\Gamma \subseteq SL_2(\mathbb{Z})$ un subgrupo de congruencias. Dados s, $s' \in \mathbb{Q} \cup \{\infty\}$ decimos que son $\Gamma-$equivalentes si existe $\gamma \in \Gamma$ tal que $\gamma(s) = s'$. Cada una de las clases de equivalencia definidas por esta relación se denomina cúspide de Γ, la motivación geométrica que justifica esta terminología se presenta en la Sección 5.2.*

Observamos que dado $s = \frac{m}{n} \in \mathbb{Q}$ con $m \in \mathbb{Z}$ y $n \in \mathbb{N}_{\geq 1}$ con $mcd(n, m) = 1$ podemos construir

$$\gamma_s = \begin{pmatrix} m & b \\ n & d \end{pmatrix}.$$

Donde $b, d \in \mathbb{Z}$ se eligen empleando la Identidad de Bezout para que cumplan $md - nb = 1$. De este modo, resulta que $\gamma_s \in SL_2(\mathbb{Z})$ y que $\gamma_s(\infty) = s$. En consecuencia, el grupo modular actúa de manera transitiva sobre $\mathbb{Q} \cup \{\infty\}$. En otras palabras, si $\Gamma = SL_2(\mathbb{Z})$ hay una única cúspide cuya clase se denota por ∞. En general, podemos garantizar que el número de cúspides es finito gracias a la Proposición 2.25 y el siguiente lema.

Lema 2.31. *Sean $\Gamma \subseteq SL_2(\mathbb{Z})$ y γ, $\gamma' \in SL_2(\mathbb{Z})$ con $\gamma\Gamma = \gamma'\Gamma$. Entonces $\gamma(\infty)$ y $\gamma'(\infty)$ están en la misma cúspide de Γ.*

Demostración. Si tomamos dos elementos de una misma clase lateral en $SL_2(\mathbb{Z})$ módulo Γ, es decir, $\gamma \in \Gamma\gamma'$ tenemos que

$$s = \gamma(\infty) = \varphi(\gamma'(\infty)) = \varphi(s'),$$

con $\varphi \in \Gamma$. Luego $s = \gamma(\infty)$ y $s' = \gamma'(\infty)$ están en la misma cúspide. □

Por consiguiente, al requerir que $f[\gamma]_k$ sea holomorfa en infinito para todo $\gamma \in SL_2(\mathbb{Z})$, podemos garantizar que dado $s \in \mathbb{Q} \cup \{\infty\}$ la función $f[\gamma_s]_k$ es holomorfa en ∞. Por tanto, f es holomorfa en s de modo que garantizamos que f sea holomorfa en las cúspides. Este hecho es fundamental para garantizar que las formas modulares respecto a Γ forman un espacio vectorial de dimensión finita.
Concluimos la sección con un resultado que establece una condición suficiente que garantiza la holomorfía en infinito de las formas modulares.

Proposición 2.32. *Sean Γ un subgrupo de congruencias de nivel N, $q_N = e^{(2\pi i\tau)/N}$ con $\tau \in \mathbb{H}$ y f una aplicación que cumple la condición de holomorfía en $\mathbb{H}$ y la condición de modularidad de peso k respecto a Γ. Si podemos expresar f como*

$$f(\tau) = \sum_{n=0}^{\infty} a_n q_N^n$$

y existen constantes $C, r > 0$ tal que $|a_n| \leq Cn^r$ para todo $n \in \mathbb{N}_{\geq 1}$, entonces $f[\gamma]_k$ es holomorfa en infinito para todo $\gamma \in SL_2(\mathbb{Z})$.

Demostración. Para probar la proposición primero vamos a probar que $f(\tau)$ está acotada cuando $y = \mathrm{Im}(\tau)$ tiende a infinito. En concreto,veremos que

$$|f(\tau)| \leq |C_0| + \frac{C_1}{y^r} \text{ cuando } y \to \infty.$$

Utilizando las hipótesis de la proposición y que $|q_N^n| = e^{(-2\pi ny)/N}$ siendo $\tau = x + yi$ obtenemos que

$$|f(\tau)| \leq \sum_{n=0}^{\infty} |a_n q_N^n| \leq \sum_{n=0}^{\infty} |a_n||q_N^n| = |a_0| + \sum_{n=1}^{\infty} |a_n||q_N^n| \leq |a_0| + C\sum_{n=1}^{\infty} n^r e^{(-2\pi ny)/N}.$$

Sea $h(t) = t^r e^{(-2\pi ty)/N}$. Derivando obtenemos que la derivada se anula en los puntos $t = 0$ y $t = Nr/2\pi y$ y calculando la segunda derivada obtenemos que el punto $t = Nr/2\pi y$ es un punto de máximo y que $h(t)$ es creciente en el intervalo $[0, Nr/2\pi y]$ y decreciente en $[Nr/2\pi y, \infty)$. Por tanto siendo $m \in \mathbb{Z}$ tal que $m \leq Nr/2\pi y < m+1$ obtenemos que

$$\sum_{n=1}^{\infty} n^r e^{(-2\pi ny)/N} = \sum_{n=1}^{m-1} h(n) + \sum_{n=m+2}^{\infty} h(n) + h(m) + h(m+1).$$

Por otra parte, como h es creciente cuando $n < m$ podemos acotar $h(n)$ por $\int_n^{n+1} h(t)dt$. De forma similar, observando que h es decreciente cuando $n > m+1$ podemos acotar $h(n)$ por $\int_{n-1}^{n} h(t)dt$. Por tanto, se cumple que

$$\sum_{n=1}^{\infty} n^r e^{(-2\pi ny)/N} \leq \int_0^{\infty} h(t)dt + h(m) + h(m+1).$$

Como $h(Nr/2\pi y)$ es el máximo entonces podemos acotar el sumatorio por

$$\int_0^{\infty} h(t)dt + h(m) + h(m+1) \leq \int_0^{\infty} h(t)dt + 2h\left(\frac{Nr}{2\pi y}\right) = \int_0^{\infty} h(t)dt + 2\left(\frac{Nr}{2\pi y}\right)^r e^{-r}.$$

Eligiendo una $\widetilde{C}$ suficientemente grande

$$C\sum_{n=1}^{\infty} n^r e^{(-2\pi ny)/N} \leq \widetilde{C}\left(\int_0^{\infty} h(t)dt + \frac{1}{y^r}\right).$$

En consecuencia

$$|f(\tau)| \leq |a_0| + \widetilde{C}\left(\int_0^\infty h(t)dt + \frac{1}{y^r}\right).$$

En la integral teniendo en cuenta que Γ es la función Gamma de Euler y realizando el cambio de variable $\ell = 2\pi yt/N$ obtenemos que

$$\int_0^\infty h(t)dt = \int_0^\infty \left(\frac{\ell N}{2\pi y}\right)^r e^{-\ell}\frac{N}{2\pi y}d\ell = \left(\frac{N}{2\pi}\right)^r \frac{1}{y^{r+1}}\int_0^\infty \ell^r e^{-\ell}d\ell = \left(\frac{N}{2\pi}\right)^r \frac{1}{y^{r+1}}\Gamma(r+1) = \frac{C_1}{y^{r+1}}.$$

Luego

$$|f(\tau)| \leq C_0 + \frac{C_2}{y^r} \quad \forall y \geq 1. \tag{2.2}$$

Por último, vamos a probar que $f[\gamma]_k$ es holomorfa en infinito. Como para todo $\gamma \in SL_2(\mathbb{Z})$ la transformada $f[\gamma]_k$ es una función holomorfa en $\mathbb{H}$ y cumple la propiedad de modularidad para el subgrupo $\gamma^{-1}\Gamma\gamma$ por la Proposición 2.29, haciendo las mismas transformaciones que en los razonamientos anteriores se puede expresar como una serie de Laurent tal que

$$f[\gamma]_k(\tau) = \sum_{n\in\mathbb{Z}} a'_n q_N^n$$

con $q_N = e^{2\pi i\tau/N}$. Para demostrar que es holomorfa basta con demostrar que la serie de Laurent sólo tiene sumandos naturales y para ello tenemos que demostrar que

$$\lim_{q_N\to 0} f[\gamma]_k(\tau)q_N = 0.$$

Teniendo en cuenta la cota para $|f(\tau)|$ dada en (2.2), considerando la $\mathrm{Im}(\tau)$ lo suficientemente grande o q_N suficientemente pequeño obtenemos que

$$|f[\gamma]_k(\tau)q_N| = |f(\gamma(\tau))(c\tau+d)^{-k}q_N| \leq \left(C_0 + \frac{C}{\mathrm{Im}(\gamma(\tau))^r}\right)|c\tau+d|^{-k}|q_N|.$$

Por la Proposición 2.3, se cumple que

$$|f[\gamma]_k(\tau)q_N| \leq \left(C_0 + \frac{|c\tau+d|^{2r}}{y^r}\right)|c\tau+d|^{-k}|q_N|.$$

Como $f[\gamma]_k$ es $N\mathbb{Z}-$ periódica podemos asumir que si $\tau = x+iy$ entonces $0 \leq x \leq N$, de esta manera $|c\tau+d|^{2r}/y^r$ se comporta como y^r cuando $y \to \infty$ asumiendo que $r \geq 1$. Por tanto, se cumple que

$$|f[\gamma]_k(\tau)q_N| \leq (M_0 + M_1 y^r)\, y^{-k} e^{\frac{-2\pi y}{N}}.$$

Luego $\lim_{\mathrm{Im}(\tau)\to\infty} f[\gamma]_k(\tau)q_N = 0$ para todo $\gamma \in SL_2(\mathbb{Z})$. En consecuencia, $f[\gamma]_k$ es holomorfa en infinito para todo γ. □

Con este resultado probamos de forma directa la holomorfía en infinito de $\Theta(\tau,4)$ porque $|r(n,4)| \leq C\cdot n^4$ para todo $n \in \mathbb{N}_{\geq 1}$.

Capítulo 3

Toros complejos y curvas elípticas

En este capítulo estudiaremos los conceptos de toro complejo y curva elíptica. La primera sección está dedicada a establecer los resultados fundamentales sobre toros complejos. En la segunda sección se presentarán las funciones elípticas prestando especial interés a la función de Weierstrass. Por último, mediante estas funciones relacionaremos las curvas elípticas con los toros complejos. Aparecerán en esta sección las nociones de discriminante y la función $j : \mathbb{H} \to \mathbb{C}$.

3.1. Toros complejos

En esta sección introduciremos la noción de toro complejo. Veremos como dotar al toro complejo de estructura de grupo y de estructura de superficie de Riemann. Caracterizaremos las aplicaciones entre toros que respeten dicha estructura, lo que nos permitirá agrupar los toros en clases de equivalencia. Concluiremos describiendo el emparejamiento de Weil en un toro complejo. En esta sección hemos empleado [4] como referencia principal.

Definición 3.1. *Un retículo en* $\mathbb{C}$ *es un conjunto* $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ *con* $\{w_1, w_2\}$ *una base de* $\mathbb{C}$ *sobre* $\mathbb{R}$.

Dada una base $\{w_1, w_2\}$ de $\mathbb{C}$ sobre $\mathbb{R}$ diremos que está normalizada si $w_1/w_2 \in \mathbb{H}$.

Lema 3.2. *Dado* Λ *un retículo en* $\mathbb{C}$ *siempre es posible tomar* $\widetilde{w_1}$, $\widetilde{w_2} \in \Lambda$ *tal que*

$$\Lambda = \widetilde{w_1}\mathbb{Z} \oplus \widetilde{w_2}\mathbb{Z} \quad y \quad \frac{\widetilde{w_1}}{\widetilde{w_2}} \in \mathbb{H}.$$

Demostración. Basta tomar $\widetilde{w_1} = -w_1$ o $\widetilde{w_2} = -w_2$ en caso de que la base no esté normalizada. □

Lema 3.3. *Considerando dos retículos* $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ *y* $\Lambda^* = w_1^*\mathbb{Z} \oplus w_2^*\mathbb{Z}$ *con* $w_1/w_2 \in \mathbb{H}$ *y* $w_1^*/w_2^* \in \mathbb{H}$. *Entonces* $\Lambda = \Lambda^*$ *si y solo si*

$$\text{para algún } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \quad \begin{pmatrix} w_1^* \\ w_2^* \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}.$$

Demostración. Para probar la implicación inversa observamos que como la matriz pertenece a $SL_2(\mathbb{Z})$ entonces es una matriz invertible y además su inversa también pertenece a $SL_2(\mathbb{Z})$, gracias a esto podemos escribir w_1 y w_2 con respecto a w_1^* y w_2^* como $w_1 = a'w_1^* + b'w_2^*$ y $w_2 = c'w_1^* + d'w_2^*$ con a', b', c' y d' números enteros. Por tanto Λ está contenido en Λ^*, la otra contención viene dada por hipótesis por lo tanto ambos retículos son iguales.
Por otro lado para demostrar la implicación directa como Λ es igual a Λ^* podemos escribir w_1 y w_2 como una matriz A dos por dos con coeficientes enteros por w_1^* y w_2^*. Por ende, podemos considerar A como la matriz de cambio de base de $\{w_1, w_2\}$ a $\{w_1^*, w_2^*\}$ y al revés, podemos considerar B como la matriz de cambio de base de $\{w_1^*, w_2^*\}$ a $\{w_1, w_2\}$. Todo ello implica que AB tiene que ser igual a la identidad. Usando las propiedades de los determinantes y que B es una matriz de números enteros invertible entonces el determinante de B es 1 ó -1. Como w_1/w_2 y w_1^*/w_2^* pertenecen a $\mathbb{H}$, A y B conservan la orientación luego A y B $\in SL_2(\mathbb{Z})$. □

Definición 3.4. *Sea Λ un retículo sobre $\mathbb{C}$, se define un toro complejo como el grupo cociente de $\mathbb{C}$ por un retículo Λ, es decir,*

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

Por consiguiente, algebraicamente un toro complejo es un grupo abeliano con la suma heredada de $\mathbb{C}$. La aplicación de paso al cociente define de forma natural una topología sobre el toro complejo y nos permite identificar un dominio fundamental de la acción del retículo sobre $\mathbb{C}$. Por tanto, desde el punto de vista geométrico se trata de un paralelogramo formado por $\{w_1, w_2\}$ con sus lados opuestos identificados entre sí. Con esta representación en mente, veamos que se puede dotar al toro complejo de estructura de superficie de Riemann. Para demostrarlo hemos seguido las notas de "Riemann Surfaces"de C. Clarkson [3].

Proposición 3.5. *Sean $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ un retículo y $\mathbb{C}/\Lambda$ el toro complejo con la topología cociente. Considerando los conjuntos*

$$\begin{aligned} U_1 &= \{x_1w_1 + x_2w_2 \in \mathbb{C} : x_1,\ x_2 \in (0,1)\} \\ U_2 &= \{x_1w_1 + x_2w_2 \in \mathbb{C} : x_1,\ x_2 \in (-1/2,1/2)\} \\ U_3 &= \{x_1w_1 + x_2w_2 \in \mathbb{C} : x_1,\ x_2 \in (-1/4,3/4)\} \end{aligned}$$

y las cartas Π_i^{-1} con $i \in \{1,\ 2,\ 3\}$ donde $\Pi_i : U_i \to \Pi(U_i) \subseteq \mathbb{C}/\Lambda$ es la aplicación de paso al cociente restringida a U_i, entonces $\mathbb{C}/\Lambda$ es una superficie de Riemann.

Demostración. Dividiremos la demostración en dos partes. Primero demostraremos que $\mathbb{C}/\Lambda$ es una $2-$variedad conexa. Por último, probaremos que $\Pi_i^{-1} \circ \Pi_j$ con $i,\ j \in \{1,\ 2,\ 3\}$ y $i \neq j$ son aplicaciones holomorfas.

1. Empezaremos probando que $\mathbb{C}/\Lambda$ es localmente homeomorfo a $\mathbb{C}$. Para ello, basta probar que el conjunto $\{\Pi(U_i)\}_{i\in\{1,\ 2,\ 3\}}$ es un conjunto de abiertos que recubre todo $\mathbb{C}/\Lambda$ y que Π_i con $i \in \{1,\ 2,\ 3\}$ son homeomorfismos. La primera parte se deduce teniendo en cuenta que Π es una aplicación abierta y que el conjunto formado por $\{x_1w_1 + x_2w_2 \in \mathbb{C} : x_1,\ x_2 \in [0,1]\} \subseteq \cup_{i\in\{1,\ 2,\ 3\}} U_i$. Por otra parte sabemos que Π_i es una aplicación continua y sobreyectiva por definición. Falta probar que es una aplicación inyectiva y podremos concluir que es un homeomorfismo. Sean $v, z \in U_1$ con $v \neq z$, entonces existen $x_1,\ x_2,\ y_1,\ y_2 \in (0,1)$ tal que $x_1w_1 + x_2w_2 = v$ y $y_1w_1 + y_2w_2 = z$. Por ende, tenemos que $|x_1 - y_1| < 1$ y $|x_2 - y_2| < 1$. Como $v \neq z$, podemos asumir que $|x_1 - y_1| \neq 0$, si no fuera el caso, entonces, $|x_2 - y_2| \neq 0$. Esto implica que $x_1 - y_1 \notin \mathbb{Z}$, lo que conlleva a que $(x_1 - y_1)w_1 + (x_2 - y_2)w_2 \notin \Lambda$. Por tanto $\Pi_1(v) \neq \Pi_1(z)$ y podemos concluir que es una aplicación inyectiva. Para el caso Π_2 y Π_3 se razona de forma análoga.
   Ahora vemos que $\mathbb{C}/\Lambda$ es Hausdorff. Sean $v, z \in \mathbb{C}/\Lambda$ tal que $v \neq z$. Entonces $z \in \Pi(U_i)$ y $v \in \Pi(U_j)$ con $i,\ j \in \{1,\ 2,\ 3\}$, denotamos $v' = \Pi_j^{-1}(v)$ y $z' = \Pi_i^{-1}(z)$. Como $\{w_1, w_2\}$ una base de $\mathbb{C}$ sobre $\mathbb{R}$ existen $x_1,\ x_2,\ y_1,\ y_2 \in \mathbb{R}$ únicos tal que $v' = x_1w_1 + x_2w_2$ y $z' = y_1w_1 + y_2w_2$. Sin perdida de generalidad asumimos que $x_1 \notin \mathbb{Z}$. Sean $\delta > 0$ la distancia de x_1 a $\mathbb{Z}$ y B_z la bola abierta de radio $\delta/2$ centrado en z'. Claramente, $\overline{B_z}$ y Λ son disjuntos. Si $v' \in \Lambda$, entonces v y z están separados por los conjuntos $\Pi(B_z)$ y $\Pi(\mathbb{C} \setminus \overline{B_z})$. Si $v' \notin \Lambda$ entonces $y_k \notin \mathbb{Z}$ para un $k \in \{1,\ 2\}$. Sean $\varepsilon > 0$ la distancia de y_k a $\mathbb{Z}$ y B_v la bola abierta de radio $\varepsilon/2$ centrada en v'. Como $v \neq z$ y $\mathbb{C}$ es hausdorff, existen dos entornos U de z' y V de v' tal que $U \cap V = \emptyset$. En este caso z y v están separados por los conjuntos $\Pi(U \cap B_z)$ y $\Pi(V \cap B_v)$. Por tanto, concluimos que $\mathbb{C}/\Lambda$ es Hausdorff.
   Por último, falta probar que es conexo. Como $\mathbb{C}$ es conexo y por definición Π es una aplicación continua, se tiene que $\Pi(\mathbb{C}) = \mathbb{C}/\Lambda$ es conexo. Gracias a esto, concluimos que $\mathbb{C}/\Lambda$ es una $2-$variedad conexa.

2. Para ver que es una superficie de Riemann falta probar que $\Pi_i^{-1} \circ \Pi_j$ con $i,\ j \in \{1,\ 2,\ 3\}$ y $i \neq j$ es holomorfa para el conjunto $U_i \cap U_j$ dado que restringida a este conjunto es la identidad.

□

Recordamos que la noción de función holomorfa entre superficies de Riemann tiene sentido dado que la holomorfía es una noción local. Además, si X e Y son superficies de Riemann compactas y $f : X \to Y$ es holomorfa entonces o f es constante o f es sobreyectiva. Para probarlo basta observar que como f es continua entonces $f(X)$ es compacto y conexo por serlo X. Por el teorema de la aplicación abierta de variable compleja, $f(X)$ es abierto si f no es constante. En este caso, $f(X)$ es un conjunto abierto-cerrado

de Y, que es conexo, luego $f(X) = Y$. El teorema de la modularidad que enunciaremos en el Capítulo 5 garantiza la existencia de una aplicación no constante, luego sobreyectiva, entre superficies de Riemann compactas. Volviendo a los toros complejos, este resultado se aplica a las funciones holomorfas entre ellos. En este caso, podemos describir de manera precisa su aspecto.

Proposición 3.6. *Sea $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda^*$ una aplicación holomorfa entre dos toros complejos. Entonces*

a) Existen m, $b \in \mathbb{C}$ tal que $m\Lambda \subseteq \Lambda^*$ y $\varphi(z+\Lambda) = mz+b+\Lambda^*$.

b) La aplicación es invertible si y solo si $m\Lambda = \Lambda^*$.

Demostración. Para demostrar la primera parte de la proposición se construye una aplicación auxiliar $\tilde{\varphi} = \Pi_{\Lambda^*}^{-1} \circ \varphi \circ \Pi_\Lambda$, donde $\Pi_\Lambda : \mathbb{C} \to \mathbb{C}/\Lambda$ son las aplicaciones de paso al cociente en cada toro. Esta aplicación nos permite levantar $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda^*$ a una aplicación $\tilde{\varphi} : \mathbb{C} \to \mathbb{C}$ entendiendo que al considerar Π_Λ^{-1} estamos trabajando en la carta correspondiente. Fijamos $\alpha \in \Lambda$ y construimos la función auxiliar dada por $f_\alpha(z) = \tilde{\varphi}(z+\alpha) - \tilde{\varphi}(z)$ que es holomorfa por ser resta de funciones holomorfas. Como $z+\alpha-z \in \Lambda$ tenemos que $\varphi(z+\alpha) = \varphi(z)$ en $\mathbb{C}/\Lambda^*$ luego $\tilde{\varphi}(z+\alpha) - \tilde{\varphi}(z) \in \Lambda^*$. Como f_α es continua y Λ^* es discreto, tenemos que f_α es constante. Derivando tenemos que $\tilde{\varphi}'(z+\alpha) = \tilde{\varphi}'(z)$. Esta igualdad es cierta para todo $\alpha \in \Lambda$ y todo $z \in \mathbb{C}$, es decir, $\tilde{\varphi}'$ es $\Lambda-$periódica y holomorfa en $\mathbb{C}$, luego por el Teorema de Liouville es constante. En consecuencia, existen m, $b \in \mathbb{C}$ tales que $\tilde{\varphi}(z) = mz+b$, luego $\varphi(z+\Lambda) = mz+b+\Lambda^*$. Por otro lado, si $\lambda \in m\Lambda$, entonces $\lambda = m\alpha$ con $\alpha \in \Lambda$, por ende se tiene que

$$\varphi(\alpha+\Lambda) = m\alpha+b+\Lambda^* \quad y \quad \varphi(\alpha+\Lambda) = b+\Lambda^*$$

luego $\lambda = m\alpha \in \Lambda^*$.
En relación con la segunda parte de la proposición, razonamos por reducción al absurdo para demostrar la implicación directa. Suponemos que existe $z \in \Lambda^*$ con $z \notin m\Lambda$. Calculamos

$$\varphi(z/m+\Lambda) = b+\Lambda^* \quad y \quad \varphi(0+\Lambda) = b+\Lambda^*,$$

luego φ no es inyectiva. Para probar la implicación inversa, se construye $\varphi^{-1}(w+\Lambda^*) = (w-b)/m+\Lambda$ y como $m\Lambda = \Lambda^*$, entonces comprobamos que φ^{-1} está bien definida y es la inversa de φ. □

Empleando la proposición anterior podemos caracterizar las aplicaciones holomorfas que además son homomorfismos de grupos.

Corolario 3.7. *Sea $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda^*$ una aplicación holomorfa entre dos toros complejos. Sabemos que existen $m, b \in \mathbb{C}$ tal que $\varphi(z+\Lambda) = mz+b+\Lambda^*$ con $m\Lambda \subseteq \Lambda^*$. Entonces son equivalentes*

a) φ es un homomorfismo de grupos.

b) $b \in \Lambda^*$, por tanto $\varphi(z+\Lambda) = mz+\Lambda^*$.

c) $\varphi(0+\Lambda) = 0+\Lambda^*$.

Demostración. Para empezar, suponemos que la condición $c)$ es cierta, esto implica que la clase de 0 es la misma que la clase de b y por tanto se cumple la condición $b)$. Suponiendo que se cumple la condición $b)$ y utilizando la propiedad distributiva de la multiplicación entonces $m(z+\Lambda)+m(z'+\Lambda) = m(z+z')+\Lambda$ y por tanto se cumple la propiedad $a)$. Finalmente, la propiedad $a)$ implica la propiedad $c)$ de forma directa. □

A partir de estos resultados podemos caracterizar la existencia de un homomorfismo holomorfo no trivial entre toros complejos en términos de los retículos que lo definen.

Corolario 3.8. *Sean $\mathbb{C}/\Lambda$ y $\mathbb{C}/\Lambda^*$ dos toros complejos. Entonces existe $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda^*$ un homomorfismo holomorfo no nulo entre dos toros complejos si y solo si existe $m \in \mathbb{C} \setminus \{0\}$ tal que $m\Lambda \subseteq \Lambda^*$. Además, podemos decir que existe φ es un isomorfismo de grupos si y solo si existe $m \in \mathbb{C} \setminus \{0\}$ tal que $m\Lambda = \Lambda^*$.*

Gracias a este corolario podemos definir un isomorfismo que tiene un interés especial. Consideramos el retículo $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ con $w_1/w_2 \in \mathbb{H}$, denotando $\tau = w_1/w_2$ podemos construir $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$. Como $w_2 \neq 0$ y además $(1/w_2)\Lambda = \Lambda_\tau$, el corolario anterior nos garantiza que existe un isomorfismo holomorfo entre ambos toros complejos. Esto muestra que cualquier toro complejo se puede identificar con uno generado a partir de $\tau \in \mathbb{H}$ y 1. Este τ no es único pero si existe τ^* tal que $\Lambda_\tau = \Lambda_{\tau^*}$ gracias al Lema 3.3 sabemos

que existe un $\lambda \in SL_2(\mathbb{Z})$ tal que $\lambda(\tau) = \tau^*$. Por tanto podemos decir que cada toro está identificado con un punto $\tau \in \mathbb{H}$ único salvo la acción de $SL_2(\mathbb{Z})$ sobre $\mathbb{H}$.
Por otro lado, queremos agrupar los toros en clases de equivalencia pero la noción de isomorfismo es demasiado restrictiva y necesitamos considerar una noción más débil.

Definición 3.9. *Se define como isogenia un homomorfismo holomorfo no nulo entre toros complejos.*

Esta definición coincide con la definición más general para grupos algebraicos donde una isogenia es un morfismo sobreyectivo con núcleo finito. Como los toros complejos son superficies de Riemann compactas el núcleo tiene que ser finito porque φ es holomorfo y no nulo. Empleando la descripción del Corolario 3.7, vemos que es sobreyectivo. Claramente los isomorfismos holomorfos son isogenias pero existen isogenias que no son de este tipo.

Ejemplo 3.10. ***La multiplicación por un entero*** $N \in \mathbb{N}_{\geq 1}$ *, es la aplicación dada por*

$$[N] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda, \qquad z+\Lambda \mapsto Nz+\Lambda.$$

La multiplicación por N está bien definida ya que $N\Lambda \subseteq \Lambda$*. Se prueba de forma directa que es un homomorfismo sobreyectivo y holomorfo, luego es una isogenia. El núcleo está formado por los puntos* $z+\Lambda$ *tal que* $N(z+\Lambda) = 0$ *este conjunto se denomina el conjunto de N-torsión de* $\mathbb{C}/\Lambda$*, se denota como* $E[N]$*. Si* $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$*, identificando el toro con el paralelogramo correspondiente, vemos que*

$$E[N] = \left\{ \frac{a}{N} w_1 + \frac{b}{N} w_2 \ : a,b \in \{0,1,\ldots,N-1\} \right\}.$$

En consecuencia, $E[N]$ *es isomorfo a* $\mathbb{Z}/N\mathbb{Z}$ *x* $\mathbb{Z}/N\mathbb{Z}$*, luego para* $N \neq 1$ *no es un isomorfismo.*

Ejemplo 3.11. ***Cociente por un grupo cíclico.***
Sean $\mathbb{C}/\Lambda$ *un toro complejo,* $N \in \mathbb{N}_{\geq 1}$ *y C un subgrupo cíclico contenido en* $E[N]$ *isomorfo a* $\mathbb{Z}/N\mathbb{Z}$*. Los elementos de C son clases de la forma* $c+\Lambda$ *luego la unión de estas clases* $\widetilde{C}$ *forma un superretículo de* Λ*. Abusando de notación utilizamos el mismo símbolo para el subgrupo C que para el superretículo* $\widetilde{C}$*. Construyendo así la aplicación*

$$\Pi_C : \mathbb{C}/\Lambda \to \mathbb{C}/C \qquad z+\Lambda \mapsto z+C.$$

La aplicación Π_C *es un homomorfismo holomorfo sobreyectivo y su núcleo es C.*

La siguiente proposición muestra que los ejemplos de isogenia anteriores son los básicos y toda isogenia se forma a partir de ellos.

Proposición 3.12. *Toda isogenia es una composición de una multiplicación por un entero, un cociente por un grupo cíclico y un isomorfismo.*

Demostración. Sea $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda^*$ una isogenia. Por definición φ es un homomorfismo holomorfo, luego por el Corolario 3.7 existe $m \in \mathbb{C}$ tal que $\varphi(z+\Lambda) = mz+\Lambda^*$. Como φ es no nula $m \neq 0$. El núcleo de esta aplicación son los $z+\Lambda$ tal que $mz \in \Lambda^*$, es decir, el núcleo es $K = m^{-1}\Lambda^*/\Lambda$. Cuando sea necesario identificaremos K con el superretículo $m^{-1}\Lambda^*$ de Λ abusando de la notación. Como φ es una isogenia sabemos que el núcleo es finito. Si N es el orden de K como subgrupo de $\mathbb{C}/\Lambda$ para todo $z+\Lambda \in K$ se tiene que $N(z+\Lambda) = 0+\Lambda$ luego $K \subseteq E[N]$. Por el teorema de estructura para grupos abelianos finitos existen $n, n' \in \mathbb{N}_{\geq 1}$ tal que K es isomorfo a $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/nn'\mathbb{Z}$. Utilizando las aplicaciones descritas con anterioridad, vamos a escribir φ como composición de tres aplicaciones. En primer lugar, $[n] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ la isogenia de multiplicación por n. Obsérvese que esta aplicación lleva K en nK que es un subgrupo isomorfo a $\mathbb{Z}/n'\mathbb{Z}$. En segundo lugar, $\Pi_{nK} : \mathbb{C}/\Lambda \to \mathbb{C}/nK$ la isogenia de paso al cociente cuyo núcleo es nK. Por último, construímos la aplicación dada por

$$F : \mathbb{C}/nK \to \mathbb{C}/\Lambda^*, \qquad z+nK \mapsto \frac{m}{n}z+\Lambda^*.$$

Como $(m/n)nK = \Lambda^*$, aplicando el Corolario 3.8, se concluye que esta aplicación es un isomorfismo. Por tanto, la composición de las tres aplicaciones lleva

$$z+\Lambda \xrightarrow{[n]} nz+\Lambda \xrightarrow{\Pi_{nK}} nz+nK \xrightarrow{F} mz+\Lambda^*,$$

y podemos concluir que $\varphi = F \circ \Pi_{nK} \circ [n]$. □

Introducimos la noción de grado para isogenias que coincide con la definición general de aplicaciones holomorfas entre superficies de Riemann compactas.

Definición 3.13. *Sea $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda^*$ una isogenia. Llamamos grado de φ a*

$$deg(\varphi) = |Ker(\varphi)|.$$

Aunque no todas las isogenias son isomorfismos, admiten una pseudo inversa.

Proposición 3.14. *Sea $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda^*$ una isogenia. Entonces existe $\widehat{\varphi} : \mathbb{C}/\Lambda^* \to \mathbb{C}/\Lambda$ una única isogenia tal que $\widehat{\varphi} \circ \varphi = [deg(\varphi)]$, es decir, la composición de φ con $\widehat{\varphi}$ es la isogenia de multiplicación por $deg(\varphi)$. Denominamos a la isogenia $\widehat{\varphi}$ isogenia dual de φ.*

Demostración. Por el Corolario 3.7, $\varphi(z+\Lambda) = mz+\Lambda^*$ con $m \in \mathbb{C}\setminus\{0\}$ y $m\Lambda \subseteq \Lambda^*$. Si $\{w_1^*, w_2^*\}$ es una base de Λ^* existen $n_1, n_2 \in \mathbb{N}_{\geq 1}$ tal que $\{n_1 w_1^*, n_2 w_2^*\}$ es una base de $m\Lambda$. Por ende, $n_1 n_2 \Lambda^* \subseteq m\Lambda$, luego $\frac{n_1 n_2}{m}\Lambda^* \subseteq \Lambda$ y tenemos que

$$\widehat{\varphi}(z+\Lambda^*) = \frac{n_1 n_2}{m} z + \Lambda$$

es una isogenia por el Corolario 3.8 y cumple que $\widehat{\varphi} \circ \varphi = [n_1 n_2]$.
Veamos que $n_1 n_2 = deg(\varphi)$. Observamos que $\left\{\frac{n_1 w_1^*}{m}, \frac{n_2 w_2^*}{m}\right\}$ es una base de Λ. Por lo tanto, $Ker(\varphi)$ es isomorfo a $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ lo que muestra que $n_1 n_2 = deg(\varphi)$.
Finalmente, si $f : \mathbb{C}/\Lambda^* \to \mathbb{C}/\Lambda$ es otra isogenia tal que $f \circ \varphi = [deg(\varphi)]$ tenemos que existe $m^* \in \mathbb{Z}$ no nulo tal que $f(z+\Lambda^*) = m^* z + \Lambda^*$. Observamos que como f y φ son sobreyectivas

$$f(z+\Lambda^*) = f(\varphi(w+\Lambda)) = deg(\varphi)(w+\Lambda) = \widehat{\varphi}(\varphi(w+\Lambda)) = \widehat{\varphi}(z+\Lambda^*).$$

Lo que garantiza la unicidad de $\widehat{\varphi}$. □

Proposición 3.15. *Las isogenias establecen una relación de equivalencia sobre el conjunto de los toros complejos.*

Demostración. Comprobamos de forma directa que es reflexiva tomando $\varphi = I$. Para probar que es simétrica basta considerar $\widehat{\varphi}$ la isogenia dual. Finalmente, como la composición de isogenias es una isogenia se tiene que es transitiva. □

Por otro lado, como hemos estudiado en los ejemplos anteriores, la aplicación $[deg(\varphi)]$ tiene grado $deg(\varphi)^2$, por tanto, como el grado de una composición de isogenias es el producto de los grados, se puede deducir que el $deg(\widehat{\varphi}) = deg(\varphi)$. La siguiente proposición muestra algunas propiedades básicas de la isogenia dual.

Proposición 3.16. *Sea $\varphi, \psi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda^*$ y $\chi : \mathbb{C}/\Lambda^* \to \mathbb{C}/\Lambda$ tres isogenias. Entonces se cumple que*

a) $\widehat{\varphi \circ \chi} = \widehat{\chi} \circ \widehat{\varphi}$.

b) $\varphi = \widehat{(\widehat{\varphi})}$.

c) $\widehat{\varphi + \psi} = \widehat{\varphi} + \widehat{\psi}$.

Demostración. La primera y la segunda propiedad se prueban de forma rutinaria comparando las aplicaciones y empleando la unicidad de la isogenia dual. Para probar la tercera propiedad, considerando dos retículos $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ y $\Lambda^* = w_1^*\mathbb{Z} \oplus w_2^*\mathbb{Z}$ con $w_1/w_2 \in \mathbb{H}$ y $w_1^*/w_2^* \in \mathbb{H}$, $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda^*$ una isogenia y $m \in \mathbb{C}\setminus\{0\}$ tal que $\varphi(z+\Lambda) = mz+\Lambda^*$. Como $m\Lambda \subseteq \Lambda^*$ existe $\alpha \in M_2(\mathbb{Z})$ tal que

$$\begin{pmatrix} mw_1 \\ mw_2 \end{pmatrix} = \alpha \begin{pmatrix} w_1^* \\ w_2^* \end{pmatrix}.$$

Denotando por α a la transformación asociada a la matriz, se tiene que

$$\frac{w_1}{w_2} = \frac{mw_1}{mw_2} = \frac{aw_1^* + bw_2^*}{cw_1^* + dw_2^*} = \frac{a\left(\frac{w_1^*}{w_2^*}\right) + b}{c\left(\frac{w_1^*}{w_2^*}\right) + d} = \alpha\left(\frac{w_1^*}{w_2^*}\right).$$

De forma análoga a la Proposición 2.3, obtenemos que

$$\mathrm{Im}(\alpha(\tau)) = \frac{det(\alpha)\mathrm{Im}(\tau)}{|j(\alpha,\tau)|^2}.$$

Por tanto, tomando $\tau = w_1^*/w_2^*$ vemos que $det(\alpha) > 0$. Como $\{aw_1^* + bw_2^*,\ cw_1^* + dw_2^*\}$ es una base de $m\Lambda$, gracias a la forma normal de Smith, podemos encontrar una base $\{\widetilde{w_1}, \widetilde{w_2}\}$ de Λ^* tal que existen $r_1, r_2 \in \mathbb{Z}$ con $r_1\widetilde{w_1} = aw_1^* + bw_2^*$ y $r_2\widetilde{w_2} = cw_1^* + dw_2^*$. Resulta que $[\Lambda^* : m\Lambda] = r_1 \cdot r_2 = det(\alpha)$. Por otro lado, como $Ker(\varphi) = m^{-1}\Lambda^*/\Lambda$ tenemos que

$$deg(\varphi) = |Ker(\varphi)| = [m^{-1}\Lambda^* : \Lambda] = [\Lambda^* : m\Lambda] = det(\alpha).$$

Como $\widehat{\varphi} \circ \varphi = [deg(\varphi)]$ la isogenia dual induce una matriz $\widehat{\alpha}$ que cumple que $\widehat{\alpha} \cdot \alpha = deg(\varphi)I$ luego $\widehat{\alpha} = deg(\varphi)\alpha^{-1}$. Como esta matriz determina la isogenia dual, calculando las matrices de $\widehat{\varphi + \psi}$ y $\widehat{\varphi} + \widehat{\psi}$ y comprobando que coinciden obtenemos la igualdad. □

Para concluir la sección, vamos a presentar una herramienta importante en el estudio de los toros complejos.

Definición 3.17. *Sean $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ un retículo y $N \in \mathbb{N}_{\geq 1}$, se define el subgrupo de $N-$torsión del grupo aditivo del toro $\mathbb{C}/\Lambda$ como*

$$E[N] = \{P \in \mathbb{C}/\Lambda : [N]P = 0\} = \langle w_1/N + \Lambda\rangle \times \langle w_2/N + \Lambda\rangle.$$

Este subgrupo es análogo al subgrupo de $N-$torsión de un grupo cíclico multiplicativo. Sobre $E[N]$ podemos definir un producto a valores en las raíces enésimas de la unidad.

Definición 3.18. *Sean $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ con $w_1/w_2 \in \mathbb{H}$, $N \in \mathbb{N}_{\geq 1}$, P, $Q \in E[N]$ y $\mu_N = \{z \in \mathbb{C} : z^N = 1\}$. Entonces, definimos el emparejamiento de Weil como*

$$e_N : E[N] \times E[N] \to \mu_N \quad (P,Q) \mapsto e^{2\pi i det(\gamma)/N},$$

para algún $\gamma \in M_2(\mathbb{Z}/N\mathbb{Z})$ tal que

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \begin{pmatrix} w_1/N + \Lambda \\ w_2/N + \Lambda \end{pmatrix}.$$

Esta aplicación tiene sentido aunque el determinante está definido solo módulo N. Si P y Q generan Λ, por el Lema 3.3 existe una matriz $\gamma' \in SL_2(\mathbb{Z})$ que cumple la propiedad anterior, reduciendo sus coeficiente módulo N y calculando el determinante obtenemos que $e_N(P,Q)$ es una raíz enésima primitiva de la unidad. En la siguiente proposición daremos una serie de propiedades del emparejamiento de Weil.

Proposición 3.19. *Sean $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ con $w_1/w_2 \in \mathbb{H}$, $N \in \mathbb{N}_{\geq 1}$, $P, Q \in E[N]$ y $\mu_N = \{z \in \mathbb{C} : z^N = 1\}$. Entonces*

a) La imagen de la aplicación $e_N(P,Q)$ no depende de la base elegida de Λ.

b) El emparejamiento de Weil es una aplicación bilineal, alternada y no degenerada.

c) Sea $d \in \mathbb{N}_{\geq 1}$, $d(\cdot) : \mu_{dN} \to \mu_N$ dada por $d(z) = z^d$ y sea $d(\cdot,\cdot) : E[dN] \times E[dN] \to E[N] \times E[N]$ dada por $d(P,Q) = (dP, dQ)$. Entonces se tiene que

$$e_N(\cdot,\cdot) \circ d(\cdot,\cdot) = d(\cdot) \circ e_{dN}(\cdot,\cdot).$$

d) Sea Λ' otro retículo tal que existe $m \in \mathbb{C} \setminus \{0\}$ de forma que $\Lambda' = m\Lambda$. El isomorfismo de toros complejos que lleva $\mathbb{C}/\Lambda$ a $\mathbb{C}/\Lambda'$, conserva el emparejamiento de Weil.

Demostración. a) Se comprueba de forma directa por el Lema 3.3.

b) Tenemos que e_N es una aplicación bilineal y alternada porque el determinante también lo es. Dado $P \in E[N]$ siempre podemos encontrar $Q \in E[N]$ de forma que el $det(\gamma) \neq 0$, luego e_N es no degenerada.

c) Por un lado, sean P' y Q' dos puntos que pertenecen a $E[dN] \times E[dN]$, tenemos que $d\left(e_{dN}(P',Q')\right) = e^{2\pi i det(\gamma')/N}$ y por otro que $e_{dN}\left(d(P',Q')\right) = e^{2\pi i det(\gamma)/N}$, donde

$$\begin{pmatrix} P' \\ Q' \end{pmatrix} = \gamma' \begin{pmatrix} w_1/dN + \Lambda \\ w_2/dN + \Lambda \end{pmatrix} \text{ y } \begin{pmatrix} dP' \\ dQ' \end{pmatrix} = \gamma \begin{pmatrix} w_1/N + \Lambda \\ w_2/N + \Lambda \end{pmatrix}.$$

Por tanto si demostramos que $det(\gamma) = det(\gamma')$, hemos terminado. Para ello observamos la siguiente serie de igualdades

$$\begin{pmatrix} dP' \\ dQ' \end{pmatrix} = d \begin{pmatrix} P' \\ Q' \end{pmatrix} = d\gamma' \begin{pmatrix} w_1/dN + \Lambda \\ w_2/dN + \Lambda \end{pmatrix} = \gamma' \begin{pmatrix} w_1/N + \Lambda \\ w_2/N + \Lambda \end{pmatrix}.$$

Por ende, podemos concluir que se da la igualdad.

d) Tomando como base de Λ' el conjunto $\{mw_1, mw_2\}$ por el apartado c), comprobamos que se conserva el emparejamiento de Weil.

□

3.2. Funciones elípticas

En esta sección vamos a introducir la definición y algunas propiedades sobre las funciones elípticas. En particular, estudiaremos la función de Weierstrass, la cual nos permitirá en la Sección 3.3 relacionar los toros complejos con las curvas elípticas. En este apartado hemos seguido el libro "Complex functions. An algebraic and geometric viewpoint."de G. A. Jones y D. Singerman [6] como referencia fundamental.

Definición 3.20. *Una función meromorfa $f : \mathbb{C} \to \mathbb{C}$ es elíptica con respecto al retículo Λ si f es doblemente periódica con respecto a él, es decir, si para todo $z \in \mathbb{C}$ y para todo $w \in \Lambda$ se cumple que $f(z+w) = f(z)$.*

Teniendo en cuenta que el toro complejo es una superficie de Riemann podemos observar que toda función meromorfa de un toro complejo a $\mathbb{C}$ da lugar a una función elíptica y que toda función elíptica induce una función meromorfa de un toro complejo a $\mathbb{C}$.
Recordamos que dado un espacio topológico y un grupo que actúa sobre el, un dominio fundamental es un subconjunto del espacio topológico que contiene exactamente un punto de cada una de las órbitas generadas por la acción de grupo. Habitualmente se requiere que la descripción topológica de este conjunto sea sencilla, dado que se emplea para representar geométricamente el conjunto de órbitas. En concreto, estamos interesados en estudiar el dominio fundamental de la acción de un retículo Λ sobre $\mathbb{C}$.

Definición 3.21. *Sea $\mathbb{C}/\Lambda$ un toro complejo con $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$. Llamamos dominio fundamental de $\mathbb{C}/\Lambda$ al conjunto*

$$P = \{x_1 w_1 + x_2 w_2 : \ x_1, x_2 \in [0,1)\}.$$

Obsérvese que por el Teorema de Liouville toda función elíptica sin polos es constante. Como toda función meromorfa con llegada en $\mathbb{C}$ se puede ver como una función holomorfa con llegada en $\widehat{\mathbb{C}}$, empleamos esta notación para funciones elípticas cuando resulte conveniente. Recordamos algunas propiedades fundamentales de las funciones elípticas que emplearemos a lo largo del capítulo.

Proposición 3.22. *Sea $f : \mathbb{C} \to \widehat{\mathbb{C}}$ una función elíptica no constante con respecto al retículo Λ y con dominio fundamental P. Para cada $c \in \widehat{\mathbb{C}}$ el conjunto de soluciones contadas con su multiplicidad de $f(z) = c$ en P es finito.*
Denominamos al número de soluciones de $f(z) = c$ en P orden de c respecto a f.

Demostración. Como f es meromorfa y no constante, las soluciones de $f(z) = c$ en $\mathbb{C}$ están aisladas y cada solución tiene multiplicidad finita. Como P es relativamente compacto, f tiene una cantidad finita de soluciones $\{z_1, z_2, \ldots, z_r\}$ en P con multiplicidades respectivas $k_1, k_2, \ldots, k_r \in \mathbb{N}_{\geq 1}$. Por tanto, $f(z) = c$ tiene $N = k_1 + k_2 + \cdots + k_r$ soluciones de P. □

En las mismas condiciones de la Proposición 3.22, si denotamos por ∂P a la frontera del dominio fundamental P, como f tiene un número finito de polos y ceros en P, para todo $t \in \mathbb{R}$ excepto un conjunto discreto, se tiene que f no tiene ni ceros ni polos en $t + \partial P$.

Proposición 3.23. *Sea $f:\mathbb{C}\to\widehat{\mathbb{C}}$ una función elíptica respecto a Λ no constante. Dado $t\in\mathbb{R}$ tal que f no tiene ni ceros ni polos en $t+\partial P$, se tiene que*

a) $\frac{1}{2\pi i}\int_{t+\partial P} f(z)dz = 0.$

b) $\frac{1}{2\pi i}\int_{t+\partial P} \frac{f'(z)}{f(z)}dz = 0.$

Demostración. Teniendo en cuenta que ∂P es un paralelogramo, denominando sus lados como $\Gamma_1,\Gamma_2,\Gamma_3,\Gamma_4$, los cuales están formados respectivamente por los segmentos de t a $t+w_1$, de $t+w_1$ a $t+w_1+w_2$, de $t+w_1+w_2$ a $t+w_2$ y de $t+w_2$ a t, obtenemos que

$$\frac{1}{2\pi i}\int_{t+\partial P} f(z)dz = \frac{1}{2\pi i}\sum_{i=1}^{4}\int_{\Gamma_i} f(z)dz.$$

Por otro lado, como $f(z)=f(z+w_2)$ y por construcción $\Gamma_3=\Gamma_1+w_2$, pero recorridos en sentidos opuestos, podemos deducir que

$$\int_{\Gamma_3} f(z)dz = -\int_{\Gamma_1} f(z)dz.$$

De forma análoga, se puede deducir lo mismo para Γ_2 y Γ_4. Por tanto, podemos concluir que

$$\frac{1}{2\pi i}\sum_{i=1}^{4}\int_{\Gamma_i} f(z)dz = 0.$$

Como f es meromorfa, también lo es f'. Fijando $w\in\Lambda$ tenemos que $f(z+w)=f(z)$ para cada $z\in\mathbb{C}$ y derivando en esta expresión concluimos que f' es elíptica respecto a Λ. En consecuencia f'/f también es elíptica respecto a Λ. Como f no tiene polos en $t+\partial P$, empleando el desarrollo de Laurent, f' tampoco tiene polos y como f no se anula en $t+\partial P$, f'/f no tiene polos en $t+\partial P$. Además f'/f es no constante, si fuera constante, resolviendo la ecuación diferencial $f(z)=Ke^{cz}$, como f no tiene polos en $\mathbb{C}$ y es elíptica, entonces f debe de ser constante, es decir, $f(z)=K$ y $c=0$ lo que es imposible. Aplicando el apartado a) a $g=f'/f$ concluimos que la correspondiente integral es nula. □

Corolario 3.24. *El número de ceros de una función elíptica no constante, contando con su multiplicidad, coincide con el número de polos, contados con su multiplicidad, en su dominio fundamental.*

Demostración. Su demostración es inmediata aplicando el apartado b) de la proposición anterior y el principio del argumento. □

De hecho, el resultado anterior es más general y nos permite afirmar que el orden es independiente del punto.

Corolario 3.25. *Sea $f:\mathbb{C}\to\widehat{\mathbb{C}}$ una función elíptica no constante. Para todo $c\in\mathbb{C}$ el número de soluciones de $f(z)=c$ en P contadas con su multiplicidad es independiente de c y coincide con el número de polos contados con su multiplicidad en P.*

Demostración. Basta aplicar el Corolario 3.24 a $g_c=f(z)-c$ que es elíptica respecto al mismo retículo que f y tiene los mismos polos con las mismas multiplicidades que f. □

Definición 3.26. *Sea $f:\mathbb{C}\to\widehat{\mathbb{C}}$ una función elíptica no idénticamente infinito. Llamamos orden de f al orden de $c=\infty$ respecto a f, es decir, la suma de los ordenes de los polos de f en el correspondiente dominio fundamental.*

En realidad, toda función elíptica debe tomar cada valor al menos dos veces como muestra la siguiente propiedad.

Corolario 3.27. *Sea f una función elíptica con respecto a Λ no constante. Entonces f no puede tener orden* 1.

Demostración. Si f tiene orden 1 entonces tendría un único polo en $z=a$ dentro de $P+t$ y por tanto podríamos expresar f como

$$f(z)=\sum_{n=-1}^{\infty} a_n(z-a)^n$$

con $a_{-1}\neq 0$ en un entorno de a. Esto implica que la suma de sus residuos es igual a a_{-1}, lo cual es una contradicción con el apartado $a)$ de la Proposición 3.23. □

Hemos visto que los ceros y los polos de una función elíptica están sujetas a ciertas restricciones. Sin embargo, las condiciones no son tan restrictivas como para funciones racionales. Recordamos que una función racional $f:\widehat{\mathbb{C}}\to\widehat{\mathbb{C}}$ no idénticamente nula, tiene un conjunto finito de ceros $a_1, a_2, \ldots, a_r\in\widehat{\mathbb{C}}$ con multiplicidades $k_1, k_2, \ldots, k_r\in\mathbb{N}_{\geq 1}$ y un conjunto finito de polos $b_1, b_2, \ldots, b_s\in\widehat{\mathbb{C}}$ con multiplicidades $\ell_1, \ell_2, \ldots, \ell_s\in\mathbb{N}_{\geq 1}$. A la inversa eligiendo una serie finita de puntos de $\widehat{\mathbb{C}}$ y multiplicidades. Existe una función racional con esos ceros y esas multiplicidades siempre que

a) $\sum_{i=1}^{r} k_i=\sum_{i=1}^{s}\ell_i$.

b) Los conjuntos $\{a_1,\ldots,a_r\}$ y $\{b_1,\ldots,b_s\}$ sean disjuntos.

En el caso de las funciones elípticas, sabemos que la propiedad $a)$ es necesaria por el Corolario 3.25 cuando estudiamos ceros y polos en P. La segunda propiedad se podría cambiar por

$$\cup_{i=1}^{r}[a_i] \text{ y } \cup_{i=1}^{s}[b_i] \text{ conjuntos disjuntos.}$$

El siguiente teorema muestra que esto no es suficiente para que exista una función elíptica, al contrario que pasa con las funciones racionales.

Teorema 3.28. *Sean $\{[a_1],\ldots,[a_r]\}$ y $\{[b_1],\ldots,[b_s]\}$ las clases de congruencias de ceros y polos de f una función elíptica respecto a Λ con multiplicidades $k_1, k_2, \ldots, k_r$ y $\ell_1, \ell_2,\ldots, \ell_s\in\mathbb{N}_{\geq 1}$. Entonces*

$$\sum_{i=1}^{r} k_i a_i \equiv \sum_{i=1}^{s}\ell_i b_i \quad \text{mód } \Lambda.$$

Demostración. Sea P el dominio fundamental de Λ y t la traslación tal que $t+\partial P$ no contenga ni ceros ni polos de f. Podemos asumir sin perdida de generalidad que para todo $i\in\{1,\ldots,r\}$ y para todo $j\in\{1,\ldots,s\}$ se tiene que $a_i, b_j\in P+t$ dado que cambiar el representante de la clase elegido no altera la conclusión del teorema.
Considerando la función $g(z)=zf'(z)/f(z)$ es meromorfa y sin polos en $t+\partial P$. Los polos de $zf'(z)/f(z)$ en $t+P$ o bien provienen de ceros de $f(z)$ o bien de los polos de $f(z)$ dado que todo polo de f' es necesariamente polo de f.
Si $z=a$ es un cero con multiplicidad k de f, entonces $f(z)=(z-a)^k h(z)$ con $h(a)\neq 0$. Luego se tiene que

$$\frac{zf'(z)}{f(z)}=\frac{z}{(z-a)^k h(z)}\Big(k(z-a)^{k-1}h(z)+(z-a)^k h'(z)\Big)=\frac{kz}{z-a}+z\frac{h'(z)}{h(z)}.$$

Por tanto, como $zh'(z)/h(z)$ es holomorfa en un entorno de a, tenemos que el residuo de $zf'(z)/f(z)$ en $z=a$ es ka. De forma análoga, si f tiene un polo de multiplicidad ℓ en b, tenemos que el residuo de $zf'(z)/f(z)$ en $z=b$ es $-\ell b$. Por tanto, por el teorema de los residuos concluimos que

$$\sum_{i=1}^{r} k_i a_i-\sum_{i=1}^{s}\ell_i b_i=\frac{1}{2\pi i}\int_{\partial P+t}\frac{zf'(z)}{f(z)}dz.$$

Razonando como en la demostración de la Proposición 3.23, descomponemos $t+\partial P$ en cuatro caminos $\Gamma_1=[t,t+w_1]$, $\Gamma_2=[t+w_1,t+w_1+w_2]$, $\Gamma_3=[t+w_1+w_2,t+w_2]$ y $\Gamma_4=[t+w_2,t]$. Descomponiendo la integral respecto a Γ_2 en partes obtenemos que

$$\int_{\Gamma_2}\frac{zf'(z)}{f(z)}dz=\int_{\Gamma_2}\frac{(z-w_1)f'(z)}{f(z)}dz+\int_{\Gamma_2}\frac{w_1 f'(z)}{f(z)}dz.$$

Realizando un cambio de variables $z-w_1=u$ y teniendo en cuenta que f es una función elíptica obtenemos que

$$\int_{\Gamma_2}\frac{(z-w_1)f'(z)}{f(z)}dz+\int_{\Gamma_2}\frac{w_1f'(z)}{f(z)}dz=-\int_{\Gamma_4}\frac{uf'(u)}{f(u)}du+[w_1log(f(z))]_{\Gamma_2}=-\int_{\Gamma_4}\frac{zf'(z)}{f(z)}dz$$
$$+w_1log\left(\frac{f(t+w_1+w_2)}{f(t+w_1)}\right)=-\int_{\Gamma_4}\frac{zf'(z)}{f(z)}dz+2\pi in_1w_1,$$

para algún $n_1\in\mathbb{Z}$ adecuado. De forma similar obtenemos que

$$\int_{\Gamma_1}\frac{zf'(z)}{f(z)}dz=-\int_{\Gamma_3}\frac{zf'(z)}{f(z)}dz+2\pi in_2w_2,$$

para algún $n_2\in\mathbb{Z}$ adecuado. Por tanto podemos concluir que

$$\frac{1}{2\pi i}\sum_{i=1}^{4}\int_{\Gamma_i}\frac{zf'(z)}{f(z)}dz=n_1w_1+n_2w_2,$$

y que $\sum_{i=1}^{r}k_ia_i\equiv\sum_{i=1}^{s}\ell_ib_i \mod \Lambda$. □

Por tanto, para construir funciones elípticas necesitamos que se cumpla la condición del teorema anterior aparte de las dos mencionadas con anterioridad. Se puede probar [6, section 3.13] que estas tres condiciones son también suficientes.
Concluimos la sección presentando un ejemplo de una función elíptica no constante. Para completar los detalles de este ejemplo se ha seguido el libro "Modular functions and Dirichlet series in number theory."de T. M. Apostol [1].

Ejemplo 3.29. *Definimos la $\wp$−función de Weierstrass con respecto al retículo Λ como*

$$\wp(z)=\frac{1}{z^2}+\sum_{w\in\Lambda,w\neq0}\left(\frac{1}{(z-w)^2}-\frac{1}{w^2}\right)\quad\forall z\in\mathbb{C}\ y\ z\notin\Lambda.$$

Para demostrar que es una función elíptica hay que demostrar que es una función Λ−periódica y meromorfa. En primer lugar, observamos que cada uno de los sumandos del sumatorio cumple que

$$\left|\frac{1}{(z-w)^2}-\frac{1}{w^2}\right|=\left|\frac{z(2w-z)}{w^2(z-w)^2}\right|.$$

Para todo $w\in\mathbb{C}$ con $|w|>R>0$ y $z\in\mathbb{C}$ con $|z|\leq R$ se tiene que

$$\left|\frac{z-w}{w}\right|=\left|1-\frac{z}{w}\right|\geq1-\left|\frac{z}{w}\right|\geq1-\frac{R}{R+\varepsilon}$$

con $\varepsilon>0$. Luego se cumple que

$$\left|\frac{z-w}{w}\right|^2\geq\left(1-\frac{R}{R+\varepsilon}\right)^2.$$

Por tanto, dado $z\in\mathbb{C}$ con $|z|\leq R$ y $w\in\Lambda$ con $|w|>R$, se cumple que

$$\left|\frac{z(2w-z)}{w^2(z-w)^2}\right|\leq\frac{C\cdot R(2|w|+R)}{|w|^4}\leq\frac{3M\cdot R}{|w|^3}.$$

Por tanto, la serie

$$\sum_{w\in\Lambda,|w|>R}\left(\frac{1}{(z-w)^2}-\frac{1}{w^2}\right)$$

converge absolutamente y uniformemente en $|z|\leq R$ luego define una función analítica en el disco. El resto de sumandos que aparecen en la definición de $\wp(z)$ nos dan polos de orden 2 en cada uno de los puntos del

retículo dentro del disco de radio R. Por ende, $\wp(z)$ es meromorfa en $\mathbb{C}$ con polos de orden 2 en cada uno de los puntos de Λ. En segundo lugar, veamos que es $\Lambda-$periódica. Para ello trabajamos con su derivada

$$\wp'(z) = -2\sum_{w\in\Lambda}\left(\frac{1}{(z-w)^3}\right),$$

la cual es una función $\Lambda-$ periódica puesto que para cualquier $w_0 \in \Lambda$ la función $f_0 : \Lambda \to \Lambda$ dada por $f_0(w) = w + w_0$ es biyectiva, por tanto haciendo un cambio de variables $\wp'(z+w_0) = \wp'(z)$. Por otra parte, teniendo en cuenta que $(w-z)^2 = (z-w)^2$ y que si $w \in \Lambda$ entonces $-w \in \Lambda$, se puede comprobar de manera rutinaria que $\wp$ es una función par. Teniendo en cuenta estas propiedades, para cada $w_0 \in \Lambda$, consideramos la función auxiliar $g_0(z) = \wp(z+w_0) - \wp(z)$. Derivando obtenemos que $g_0'(z) = \wp'(z+w_0) - \wp'(z) = 0$, por tanto $\wp(z+w_0) - \wp(z) = c$ con c una constante. Ahora tomando $z = -w_0/2$ obtenemos que $\wp(w_0/2) - \wp(-w_0/2) = c$ y por tanto $c = 0$. Entonces, para todo $w_0 \in \Lambda$, $\wp(z+w_0) = \wp(z)$ y por ende $\wp$ es una función elíptica con respecto a Λ.

Resulta que $\wp$ y $\wp'$ son los únicos ejemplos básicos que necesitamos ya que el anillo de funciones meromorfas en $\mathbb{C}/\Lambda$ es $\mathbb{C}(\wp, \wp')$. Recordamos que $\mathbb{C}(\wp, \wp')$ es el conjunto de fracciones racionales en estas dos funciones, para más detalle ver [6, section 3.11]. En la siguiente sección mostraremos que las curvas elípticas se pueden parametrizar empleando la función de Weierstrass. Cuando queremos precisar el retículo escribimos $\wp_\Lambda(z)$ y $\wp'_\Lambda(z)$ y en el caso particular de un retículo de la forma Λ_τ, abusando de la notación, escribimos $\wp_\tau(z)$ y $\wp'_\tau(z)$.

3.3. Toros complejos como curvas elípticas

En esta sección definiremos las curvas elípticas, además mostraremos como identificar los toros complejos con curvas elípticas a través de un isomorfismo. Comenzamos con la definición de curva elíptica para un cuerpo $\mathbb{K}$ con característica distinta de 2 o 3.

Definición 3.30. *Sea $\mathbb{K}$ un cuerpo con $car(\mathbb{K}) \neq 2$ y $car(\mathbb{K}) \neq 3$. Llamamos curva elíptica al conjunto*

$$E = \left\{(x,y) \in \mathbb{K}^2 : \quad y^2 = x^3 + ax + b = 0\right\} \cup \{\infty\}.$$

Con $a, b \in \mathbb{K}$ tales que $4a^3 + 27b^2 \neq 0$.

La condición sobre los coeficientes garantiza que la curva es no singular. Cuando la característica del cuerpo es 2 o 3 esta condición no nos permite incluir todas las curvas no singulares. Coviene destacar que, aunque no hagamos uso de ella en este trabajo, existe una definición alternativa de curva elíptica validada para todo cuerpo: una curva elíptica es una curva algebraica proyectiva sobre $\mathbb{K}$ no singular y de género 1.

Para poder construir el isomorfismo entre toros complejos y curvas elípticas necesitamos obtener algunas propiedades adicionales de la función de Weierstrass. Para ello, necesitamos introducir las series de Eisenstein sobre un retículo.

Ejemplo 3.31. *Para cada $k \in \mathbb{N}_{\geq 3}$, k par y cada retículo Λ, definimos*

$$G_k(\Lambda) = \sum_{w\in\Lambda, w\neq 0} \frac{1}{w^k} \text{ con } k \geq 3.$$

Observamos que esta definición coincide con la definición del Ejemplo 2.15, en este caso la serie $G_k(\tau)$ se corresponde con la serie de Eisenstein evaluada en el retículo Λ_τ, es decir, $G_k(\Lambda_\tau) = G_k(\tau)$. Comprobamos que como función sobre el conjunto de retículos cumple la siguiente condición de homogeneidad para todo $m \in \mathbb{C} \setminus \{0\}$, se tiene que $G_k(m\Lambda) = m^{-k} G_k(\Lambda)$.

Empleamos esta función para establecer la relación fundamental entre $\wp$ y $\wp'$.

Proposición 3.32. *Sea $\wp$ la función de Weierstrass con respecto a Λ. Entonces*

a) El desarrollo de Laurent de $\wp$ es

$$\wp(z) = \frac{1}{z^2} + \sum_{n=2,\ npar}^{\infty} (n+1) G_{n+2}(\Lambda) z^n$$

para todo z tal que $0 < |z| < inf\{|w| : w \in \Lambda \setminus \{0\}\}$.

b) La función $\wp$ y $\wp'$ satisfacen la relación:

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

c) Sea $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ y $w_3 = w_1 + w_2$, entonces la ecuación cúbica dada por $\wp$ y $\wp'$ como $y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$ es

$$y^2 = 4(x-e_1)(x-e_2)(x-e_3) \ \ con\ e_i = \wp(w_i/2)\ \forall i \in \{1,2,3\}.$$

Esta ecuación es nosingular, lo cual significa que a su lado derecho tiene tres raíces distintas.

Demostración. a) Teniendo en cuenta que podemos desarrollar los sumandos que aparecen en la definición de $\wp$ para $|z| < |w|$ como

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

Luego podemos expresar $\wp$ como

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

Como hemos probado en el Ejemplo 3.29 la serie es absolutamente convergente, por tanto podemos cambiar el orden de los sumatorios y obtenemos que

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

para todo z tal que $0 < |z| < inf\{|w| : w \in \Lambda \setminus \{0\}\}$ y como $\wp$ es par los coeficientes de la forma G_{n+2} con n impar deben anularse.

b) Para demostrar esta parte de la proposición vamos a desarrollar la función $\wp$ empleando la expresión del apartado anterior, para todo z tal que $0 < |z| < inf\{|w| : w \in \Lambda \setminus \{0\}\}$ se tiene que

$$\wp(z) = \frac{1}{z^2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + O(z^6).$$

Gracias a esto podemos obtener las siguientes expresiones

$$\begin{aligned}
\wp'(z) &= \frac{-2}{z^3} + 6G_4(\Lambda)z + 20G_6(\Lambda)z^3 + O(z^5),\\
(\wp'(z))^2 &= \frac{4}{z^6} - \frac{24}{z^2}G_4(\Lambda) - 80G_6(\Lambda) + O(z^2),\\
4(\wp(z))^3 &= \frac{4}{z^6} + \frac{36}{z^2}G_4(\Lambda) + 60G_6(\Lambda) + O(z^2),\\
60G_4(\Lambda)\wp(z) &= \frac{60}{z^2}G_4(\Lambda) + O(z^2).
\end{aligned}$$

Por tanto considerando la función

$$f(z) = (\wp'(z))^2 - 4(\wp(z))^3 + 60G_4(\Lambda)\wp(z) + 140G_6(\Lambda),$$

es una función $\Lambda-$ periódica ya que $\wp$ y $\wp'$ lo son. Empleando las ecuaciones anteriores $f(z) = O(z^2)$, luego $f(0) = 0$. Por tanto, $f(w) = 0$ para todo $w \in \Lambda$. Sin embargo, por construcción f sólo puede tener polos en donde los tenían $\wp$ y $\wp'$, es decir, en Λ. En consecuencia, f es holomorfa y, por el teorema de Liouville, concluimos que es constante. Como $f(0) = 0$, deducimos que $f(z) \equiv 0$ para todo $z \in \mathbb{C}$ y las funciones $\wp$ y $\wp'$ cumplen la ecuación deseada.

c) Escribiendo $y = \wp'(z)$ y $x = \wp(z)$ por el apartado anterior se cumple la ecuación. Como $\wp'$ es impar, si $z \equiv -z \mod \Lambda$, entonces $\wp'(z) = \wp'(-z) = -\wp'(z)$ y por tanto $\wp'(z) = 0$. Gracias a esto podemos observar que tiene ceros en los puntos de orden 2 del grupo $\mathbb{C}/\Lambda$, los cuales son $w_1/2$, $w_2/2$, $w_3/2$. Sus valores asociados son $e_i = \wp(w_i/2)$. Por ende, como $y^2 = (\wp'(w_i/2))^2 = 0$ podemos expresar la ecuación como $y^2 = 4(x-e_1)(x-e_2)(x-e_3)$, puesto que es un polinomio de grado 3 y hemos obtenido sus soluciones. Para ver que son distintas observamos que como $\wp(z)$ es meromorfa en $\mathbb{C}$ y tiene polos de orden 2 en Λ por lo probado en el Ejemplo 3.29. Por el Corolario 3.25, tenemos que $\wp(z)$ toma en $\mathbb{C}/\Lambda$ exactamente cada valor de $\widehat{\mathbb{C}}$ dos veces contando con su multiplicidad. Sin embargo, como $\wp'(w_i/2) = 0$ tenemos que $w_i/2$ es un cero doble de $\wp(z) - e_i$, luego los valores e_1, e_2, e_3 son dos a dos distintos.

□

Gracias a esta proposición podemos construir una función biyectiva entre un toro complejo y una curva algebraica $\Theta : \mathbb{C}/\Lambda \to \mathbb{C}^2$ donde $\Theta(z+\Lambda) = (\wp_\Lambda(z), \wp'_\Lambda(z))$. Por el apartado b) de la proposición anterior

$$\mathrm{Im}(\Theta) \subseteq \left\{(x,y) \in \mathbb{C}^2 : y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)\right\}.$$

Como para todo $x \in \mathbb{C}$, $\wp$ toma el valor x dos veces en $\mathbb{C}/\Lambda$ el contenido es una igualdad. Para ver que Θ es inyectiva tenemos que si existen dos pares de elementos tal que la coordenada x es la misma, por la Proposición 3.32 y el Corolario 3.25, cada elemento solo puede ser obtenido dos veces por tanto como $\wp$ es par se tiene que $x = \wp(\pm z + \Lambda)$. Si nos fijamos en la derivada, como $\wp'$ es impar, $\wp'(-z+\Lambda) = -\wp'(z+\Lambda)$, por tanto la coordenada y será distinta si $y \neq 0$. Por otro lado si $y = 0$, sabemos que el valor obtenido es de orden 2, por tanto en ambos pares se obtiene la misma coordenada x. Por ende, Θ es una aplicación biyectiva entre el toro complejo $\mathbb{C}/\Lambda$ y la curva dada por la ecuación $y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$.

Para transformar esta aplicación biyectiva en un isomorfismo necesitamos definir una operación de grupo sobre la curva elíptica. De manera natural, definimos esta operación por $\Theta(z_1) + \Theta(z_2) := \Theta(z_1 + z_2)$ y se cumple que Θ es un isomorfismo. Cabe destacar que esta operación admite una interpretación geométrica. Dados $\Theta(z_1)$ y $\Theta(z_2)$ en la curva, trazamos la recta que une ambos puntos, si son el mismo punto, trazamos la tangente a la curva en dicho punto. Dicha recta tendrá una ecuación $ax + by + c = 0$. Consideramos la función $f(z) = a\wp(z) + b\wp'(z) + c = 0$ que es elíptica respecto a Λ. Si $b \neq 0$, es decir, la recta no es vertical, $f(z)$ tiene un polo triple en $0+\Lambda$ y ceros en $z_1+\Lambda$ y $z_2+\Lambda$. Por tanto, tiene que existir otro cero y, por el Teorema 3.28, se tiene que $z_1 + z_2 + z_3 + \Lambda = 0 + \Lambda$, luego $\Theta(z_1) + \Theta(z_2) = -\Theta(z_3)$. En consecuencia, para obtener la suma intersecamos la recta anterior con la curva obteniendo un tercer punto y después calculamos su simétrico. Este punto se corresponderá con la suma. Si $b = 0$, es decir, si la recta es vertical, entonces el tercer punto es $\Theta(z_1) + \Theta(z_2) = \infty$.

En la Sección 3.1 hemos demostrado que dos toros complejos $\mathbb{C}/\Lambda$ y $\mathbb{C}/\Lambda'$ son isomorfos si y solo si existe $m \in \mathbb{C} \setminus \{0\}$ tal que $\Lambda' = m\Lambda$. Observando los correspondientes toros complejos mediante sus curvas asociadas E_Λ y $E_{\Lambda'}$, podemos establecer un isomorfismo $\phi : E_\Lambda \to E_{\Lambda'}$ dado por $\phi((x,y)) = (m^{-2},\ m^{-3})$, el cual cambia la ecuación $y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$ en $y^2 = 4x^3 - 60m^{-4}G_4(\Lambda')x - 140m^{-6}G_6(\Lambda')$. Esta correspondencia se obtiene teniendo en cuenta la relación entre $\wp_{m\Lambda}$ y $\wp_\Lambda$ dada por $\wp_{m\Lambda}(mz) = m^{-2}\wp_\Lambda(z)$, la cual se deduce de la Proposición 3.32, y derivando y despejando $\wp'_{m\Lambda}$, obtenemos que $\wp'_{m\Lambda}(mz) = m^{-3}\wp'_\Lambda(z)$.
Hemos visto que la curva algebraica determinada por $\mathbb{C}/\Lambda$ es libre de cuadrados en x. Este hecho se puede caracterizar algebraicamente en términos del determinante. Recordamos que el discriminante de la curva de ecuación $y^2 = x^3 + ax + b$ es $\Delta = -4a^3 - 27b^2$. Si la curva tiene la forma $y^2 = 4x^3 - g_2x - g_3$, entonces realizando el cambio de variable correspondiente en la variable x el discriminante resulta $\Delta = g_2^3 - 27g_3^2$. Con los desarrollos anteriores, extendemos la definición del discriminante a retículos.

Definición 3.33. *Dado un retículo Λ llamamos discriminante de Λ a*

$$\Delta(\Lambda) = (g_2(\Lambda))^3 - 27(g_3(\Lambda))^2$$

con $g_2(\Lambda) = 60G_4(\Lambda)$ y $g_3(\Lambda) = 140G_6(\Lambda)$.

Dada la relación entre las raíces múltiples y el discriminante que se puede consultar en [6, section 6.2] tenemos el siguiente corolario.

Corolario 3.34. *Para todo retículo Λ, se tiene que $\Delta(\Lambda) \neq 0$.*

En el caso particular de Λ_τ el discriminante es una función del plano superior complejo

$$\Delta : \mathbb{H} \to \mathbb{C} \quad \tau \mapsto \Delta(\tau) = (g_2(\tau))^3 - 27(g_3(\tau))^2$$

donde $g_2(\tau) = 60G_4(\tau)$ y $g_3(\tau) = 140G_6(\tau)$. Por las propiedades demostradas para la serie de Eisenstein podemos comprobar que $\Delta \in S_{12}(SL_2(\mathbb{Z}))$. Del mismo modo podemos definir una función más relevante para nuestros propósitos en $\mathbb{H}$, que es invariante respecto a $SL_2(\mathbb{Z})$.

Definición 3.35. *Sea Λ un retículo. Definimos $j(\Lambda) = 1728g_2(\Lambda)^3/\Delta(\Lambda)$ y análogamente la función j dada por*

$$j : \mathbb{H} \to \mathbb{C} \quad \tau \mapsto 1728g_2(\tau)^3/\Delta(\tau).$$

Atención no se debe confundir la función $j : \mathbb{H} \to \mathbb{C}$ con el factor de automorfia $j(\gamma, \tau)$. Se ha decidido emplear la misma letra manteniendo la notación clásica dado que por el contexto se entiende que función interviene en cada caso.

Proposición 3.36. *Para todo $\gamma \in SL_2(\mathbb{Z})$ y para todo $\tau \in \mathbb{H}$, $j(\gamma(\tau)) = j(\tau)$.*

Demostración. La proposición se demuestra de forma sencilla utilizando que la serie de Eisenstein es una forma modular para $k \geq 3$ y que tanto el numerador como el denominador tienen el mismo peso. □

Queremos probar que dada una curva elíptica podemos construir un retículo de manera que al establecer la parametrización de la Proposición 3.32 recuperemos la curva de partida. Para ello, necesitamos demostrar que j es una función sobreyectiva.

Proposición 3.37. *Para todo $c \in \mathbb{C}$ existe un $\tau \in \mathbb{H}$ tal que $j(\tau) = c$.*

Demostración. Para demostrar está proposición razonaremos por reducción al absurdo. Suponemos que existe $c \in \mathbb{C}$ tal que para todo $\tau \in \mathbb{H}$, $c \neq j(\tau)$. Consideramos la integral

$$\frac{1}{2\pi i} \int_\gamma \frac{j'(\tau)}{j(\tau) - c} d\tau,$$

y consideramos los subconjuntos

$$\begin{aligned}
\Gamma_1 &= \left\{ \tau : \mathrm{Im}(\tau) \in [\sqrt{3}/2, \sqrt{3}/2 + 2] \text{ y } Re(\tau) = 1/2 \right\}, \\
\Gamma_2 &= \left\{ \tau : |\tau| = 1 \text{ y } Re(\tau) \in [-1/2, 1/2] \right\}, \\
\Gamma_3 &= \left\{ \tau : \mathrm{Im}(\tau) \in [\sqrt{3}/2, \sqrt{3}/2 + 2] \text{ y } Re(\tau) = -1/2 \right\}, \\
\Gamma_4 &= \left\{ \tau : Re(\tau) \in [-1/2, 1/2] \text{ y } \mathrm{Im}(\tau) = \sqrt{3}/2 + 2 \right\}.
\end{aligned}$$

donde γ es la curva que recorre el segmento Γ_1 en sentido descendente, después el arco de circunferencia Γ_2 en sentido anti-horario, luego el segmento Γ_3 en sentido ascendente y, por último, el segmento Γ_4 de izquierda a derecha. En primer lugar, observamos que $g(\tau) = j'(\tau)/(j(\tau) - c)$ es una función holomorfa ya que $j(\tau)$ y $j'(\tau)$ son holomorfas y el denominador nunca se anula. Por tanto, por el teorema integral de Cauchy se tiene que

$$\int_\gamma \frac{j'(\tau)}{j(\tau) - c} d\tau = 0.$$

Por otra parte, observamos que $j(\tau) = j(\tau + 1)$ por la Proposición 3.36 y teniendo en cuenta que $\Gamma_1 = \Gamma_3 + 1$ recorridos en sentidos contrarios obtenemos que

$$\frac{1}{2\pi i} \int_{\Gamma_1} \frac{j'(\tau)}{j(\tau) - c} d\tau = -\frac{1}{2\pi i} \int_{\Gamma_3} \frac{j'(\tau)}{j(\tau) - c} d\tau.$$

Razonando de forma análoga, teniendo en cuenta que $j(\tau) = j(-1/\tau) = j(-\bar{\tau})$ en Γ_2 puesto que $|\tau| = 1$, dividiendo el arco de circunferencia en dos partes iguales $\Gamma_{2,1}$ que va desde $e^{2\pi i/3}$ hasta i y $\Gamma_{2,2}$ desde i hasta $e^{\pi i/3}$. Observamos que $\Gamma_{2,2} = \overline{\Gamma_{2,1}}$ recorrido en forma opuesta por tanto obtenemos que

$$\frac{1}{2\pi i} \int_{\Gamma_2} \frac{j'(\tau)}{j(\tau) - c} d\tau = 0.$$

Por tanto, se cumple que

$$\frac{1}{2\pi i}\int_{\gamma}\frac{j'(\tau)}{j(\tau)-c}d\tau=\frac{1}{2\pi i}\int_{\Gamma_4}\frac{j'(\tau)}{j(\tau)-c}d\tau=[log(j(\tau)-c)]_{\Gamma_4}.$$

Haciendo el cambio de variable $q=e^{-2\pi i\tau}$ convirtiendo Γ_4 en una circunferencia C_4. Multiplicando y dividiendo dentro del logaritmo por q obtenemos que

$$[log(j(\tau)-c)]_{\Gamma_4}=[log(q(j(q)-c))-log(q)]_{C_4}.$$

Empleando las propiedades de las series de Eisenstein como se puede ver en [6, section 6.4], podemos obtener el desarrollo en serie de potencias de $j(q)$ dado por

$$j(q)=\frac{1}{q}+\sum_{n=0}^{\infty}c(n)q^n$$

donde los $c(n)\in\mathbb{Z}$. Teniendo esto en cuenta obtenemos que $log(q(j(q)-c))$ es una función analítica y por ende que

$$[log(q(j(q)-c))-log(q)]_{C_4}=[-log(q)]_{C_4}=2\pi i.$$

Por tanto, se cumple que $\frac{1}{2\pi i}\int_{\Gamma_4}\frac{j'(\tau)}{j(\tau)-c}d\tau=1$. Este hecho contradice la hipótesis inicial y, por ende, j es sobreyectiva. □

Previamente hemos demostrado que a partir de una transformación podemos convertir los toros complejos en curvas de la forma $y^2=4x^3-a_2x-a_3$ tal que $a_2^3-27a_3^2\neq 0$. Veamos que el recíproco es cierto.

Proposición 3.38. *Dada una curva $y^2=4x^3-a_2x-a_3$ tal que $a_2^3-27a_3^2\neq 0$ existe Λ tal que $g_2(\Lambda)=a_2$ y $g_3(\Lambda)=a_3$.*

Demostración. Por las propiedades de modularidad de las series de Eisestein podemos comprobar que $g_2(\Lambda_{\mu_3})=g_3(\Lambda_i)=j(\mu_3)=0$ y que $j(i)=1$ donde $\mu_3=e^{2\pi i/3}$. Dividimos la demostración en tres casos.

1. Si $a_2=0$ entonces $a_3\neq 0$ ya que $a_2^3-27a_3^2\neq 0$. Sea $\mu_3=e^{2\pi i/3}$, teniendo en cuenta que $g_2(\Lambda_{\mu_3})=0$ y que $g_3(m\Lambda_{\mu_3})=m^{-6}g_3(\Lambda_{\mu_3})$, elegimos un $m\in\mathbb{C}\setminus\{0\}$ tal que $a_3=g_3(m\Lambda_{\mu_3})$.

2. Si $a_3=0$, de forma análoga a la anterior pero con el retículo Λ_i, elegimos un $m\in\mathbb{C}\setminus\{0\}$ tal que $a_2=g_2(m\Lambda_i)$.

3. Si $a_2\neq 0$ y $a_3\neq 0$, como la función j por la Proposición 3.37, es una función sobreyectiva. Por tanto, para todo a_2 y a_3 existe un $\tau\in\mathbb{H}$ tal que

$$j(\tau)=\frac{1728g_2(\tau)^3}{g_2(\tau)^3-27g_3(\tau)^2}=\frac{1728a_2^3}{a_2^3-27a_3^2}.$$

Despejando se obtiene que $a_2^3/g_2(\tau)^3=a_3^2/g_3(\tau)^2$. Para $w_2\in\mathbb{C}\setminus\{0\}$, sea $w_1=w_2\tau$ y $\Lambda=w_1\mathbb{Z}\oplus w_2\mathbb{Z}$, entonces

$$g_2(\Lambda)=g_2(w_2\tau\mathbb{Z}\oplus w_2\mathbb{Z})=g_2(w_2\Lambda_\tau)=w_2^{-4}g_2(\Lambda_\tau).$$
$$g_3(\Lambda)=g_3(w_2\tau\mathbb{Z}\oplus w_2\mathbb{Z})=g_3(w_2\Lambda_\tau)=w_2^{-6}g_3(\Lambda_\tau).$$

Eligiendo $w_2\in\mathbb{C}\setminus\{0\}$ tal que $w_2^{-4}=a_2/g_2(\tau)$ entonces

$$w_2^{-12}=a_2^3/g_2(\tau)^3=a_3^2/g_3(\tau)^2.$$

Por tanto, se tiene que $w_2^{-6}=\pm a_3/g_3(\tau)$. Despejando se cumple que

$$a_2^3=\frac{a_3^2}{g_3(\tau)^2}g_2(\tau)^3=w_2^{-12}g_2(\tau)^3=(w_2^{-4}g_2(\tau))^3=(g_2(\Lambda))^3.$$

Por ende, cambiando w_2 por iw_2 si fuera necesario concluimos que $a_2=g_2(\Lambda)$ y $a_3=g_3(\Lambda)$.

□

Capítulo 4

Curvas modulares

Las curvas modulares son el engranaje que nos permite conectar las curvas elípticas y las formas modulares. En la primera sección, mostraremos la relación entre las curvas modulares y los espacios de moduli para clasificar curvas elípticas. Esta relación nos permitirá establecer una conexión entre las funciones homogeneas definidas sobre curvas elípticas y las funciones definidas en $\mathbb{H}$ que cumplen una condición de modularidad. En la segunda sección describimos algunos de los elementos fundamentales de la topología de las curvas modulares. En la última sección, estudiaremos las propiedades de los puntos elípticos de las curvas modulares.

4.1. Curvas modulares y espacios de moduli

Por lo visto en el Corolario 3.8 sabemos que dos toros $\mathbb{C}/\Lambda$ y $\mathbb{C}/\Lambda'$ son holomórficamente isomorfos como grupos si y solo si $m\Lambda = \Lambda'$ para algún $m \in \mathbb{C} \setminus \{0\}$. Gracias a la relación entre curvas elípticas y toros complejos podemos dividir el conjunto de curvas elípticas en clases de equivalencia. De forma similar, viendo dos puntos $\tau, \tau' \in \mathbb{H}$ como equivalentes si y solo si $\gamma(\tau) = \tau'$ para algún $\gamma \in SL_2(\mathbb{Z})$ podemos considerar el conjunto cociente también. En esta sección veremos que existe una biyección del primer conjunto cociente al segundo. Esto implica que el conjunto de clases de equivalencias de puntos de $\mathbb{H}$ bajo la acción del grupo modular, está descrito por las clases de isomorfía de los toros. De un modo más general, en lugar de considerar la acción del grupo modular sobre $\mathbb{H}$, podemos considerar la acción de alguno de los subgrupos de congruencias descritos en la Sección 2.3. Se demostrará que en este caso la relación de congruencia está descrita mediante curvas elípticas realzadas. Comenzaremos el capítulo introduciendo esta noción.

Definición 4.1. *Sea $N \in \mathbb{N}_{\geq 1}$. Se define una curva elíptica realzada para $\Gamma_0(N)$ como un par ordenado (E,C), donde E es una curva elíptica compleja y C es un subgrupo cíclico de E de orden N.*

Se considera que dos pares (E,C) y (E',C') son equivalentes, si existe algún isomorfismo de E a E' que lleva C en C'. El conjunto de clases de equivalencia es denotado por $S_0(N)$ y las clases correspondientes se denotan $[(E,C)]$.

Definición 4.2. *Sea $N \in \mathbb{N}_{\geq 1}$. S se define una curva elíptica realzada para $\Gamma_1(N)$ como un par ordenado (E,P), donde E es una curva elíptica compleja y P es un punto de E de orden N.*

De manera similar, se considera que dos pares (E,P) y (E',P') son equivalentes, si existe algún isomorfismo de E a E' que lleva P en P'. El conjunto de clases de equivalencia es denotado por $S_1(N)$ y las clases correspondientes se denotan $[(E,P)]$. Como cada punto de orden N genera un subgrupo cíclico de orden N, si (E,P) y (E',P') son equivalentes entonces $(E,\langle P\rangle)$ y $(E,\langle P'\rangle)$ son equivalentes.

Definición 4.3. *Sea $N \in \mathbb{N}_{\geq 1}$. Se define una curva elíptica realzada para $\Gamma(N)$ como un par ordenado $(E,(P,Q))$, donde E es una curva elíptica compleja y (P,Q) es un par de puntos de E que generan el subgrupo de $N-$torsión $E[N]$ y cuyo emparejamiento de Weil cumple que $e_N(P,Q) = e^{2\pi i/N}$.*

Análogamente, se considera que dos pares $(E,(P,Q))$ y $(E',(P',Q'))$ son equivalentes, si existe algún isomorfismo de E a E' que lleva P en P' y Q en Q'. El conjunto de clases de equivalencias es denotado por

$S(N)$ y las clases correspondientes se denotan $[(E,(P,Q)]$.
Cada uno de los conjuntos $S_0(N)$, $S_1(N)$, $S(N)$ es un espacio de moduli. En geometría algebraica se denomina espacio de moduli a un espacio geométrico cuyos puntos representan objetos matemáticos con una misma propiedad, en este caso ser isomorfos. Habitualmente, estos espacios aparecen en problemas de clasificación, por tanto, en este contexto la palabra módulo hace referencia al parámetro de clasificación no a la aritmética modular como ocurría con las formas modulares. Cuando $N = 1$, los tres espacios modulares se reducen al espacio de clases de isomorfismos de toros mencionado al principio de la sección.

Definición 4.4. *Para cualquier subgrupo de congruencias Γ de $SL_2(\mathbb{Z})$ actuando sobre $\mathbb{H}$, se define la curva modular $Y(\Gamma)$ como el espacio cociente $\mathbb{H}/\Gamma$ formado por las orbitas bajo la acción de Γ, es decir, dado por*

$$Y(\Gamma) = \{\Gamma\tau : \tau \in \mathbb{H}\}.$$

Las curvas modulares para $\Gamma_0(N)$, $\Gamma_1(N)$, $\Gamma(N)$, son denotadas respectivamente $Y_0(N)$, $Y_1(N)$, $Y(N)$. En el siguiente teorema se demuestra que existen aplicaciones biyectivas entre los espacios de moduli y las curvas modulares. Recordemos la notación introducida en la Sección 3.1, en la cual $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$. El siguiente teorema nos indica que los datos de torsión que definen los espacios de moduli coinciden con las condiciones que definen los grupos de congruencias. En otras palabras, las definiciones introducidas en la Sección 2.3 son las naturales en este problema.

Teorema 4.5. *Sea $N \in \mathbb{N}_{\geq 1}$.*

a) El espacio de moduli $\Gamma_0(N)$ es

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

donde dos puntos $[E_\tau, \langle 1/N+\Lambda_\tau\rangle] = [E_{\tau'}, \langle 1/N+\Lambda_{\tau'}\rangle]$ si y solo si $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. Por tanto, existe una aplicación biyectiva $\psi_0 : S_0(N) \to Y_0(N)$ tal que $\psi_0([E_\tau, \langle 1/N+\Lambda_\tau\rangle]) = \Gamma_0(N)\tau$.

b) El espacio de moduli $\Gamma_1(N)$ es

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

donde dos puntos $[E_\tau, 1/N+\Lambda_\tau] = [E_{\tau'}, 1/N+\Lambda_{\tau'}]$ si y solo si $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. Por tanto, existe una aplicación biyectiva $\psi_1 : S_1(N) \to Y_1(N)$ tal que $\psi_1([E_\tau, 1/N+\Lambda_\tau]) = \Gamma_1(N)\tau$.

c) El espacio de moduli $\Gamma(N)$ es

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

donde dos puntos $[E_\tau, (\tau/N+\Lambda_\tau, 1/N+\Lambda_\tau)] = [E_{\tau'}, (\tau'/N+\Lambda_{\tau'}, 1/N+\Lambda_{\tau'})]$ si y solo si $\Gamma(N)\tau = \Gamma(N)\tau'$. Por tanto, existe una aplicación biyectiva $\psi : S(N) \to Y(N)$ tal que $\psi([E_\tau, (\tau/N+\Lambda_\tau, 1/N+\Lambda_\tau)]) = \Gamma(N)\tau$.

Demostración. Empezaremos demostrando la parte *b*) del teorema. Para demostrar esta parte, cogemos cualquier punto $[E,Q] \in S_1(N)$. Comenzaremos probando que podemos elegir un representante de la clase $[E,Q]$ de la forma $[E_\tau, 1/N+\Lambda_\tau]$. Como E es isomorfo a $\mathbb{C}/\Lambda_{\tau'}$ para algún $\tau' \in \mathbb{H}$ por lo demostrado en el Corolario 3.8, podemos decir, abusando de notación que $E = \mathbb{C}/\Lambda_{\tau'}$. Por otra parte, como Q es un elemento de orden N de E, podemos escribir $Q = (c\tau' + d)/N + \Lambda_{\tau'}$ para algún c y d números enteros y tales que $mcd(c,d,N) = 1$. Por el algoritmo de Euclides, existen a, d, $k \in \mathbb{Z}$ tal que $ad - bc - kN = 1$. Construimos una matriz γ tal que

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}).$$

Como modificar las entradas de γ módulo N no cambia el punto Q, podemos transformar esta matriz en una matriz de $M_2(\mathbb{Z}/N\mathbb{Z})$ y como se cumple la condición $ad - bc - kN = 1$ podemos suponer sin perdida de generalidad que está en $SL_2(\mathbb{Z}/N\mathbb{Z})$. Como la aplicación de paso al cociente de $SL_2(\mathbb{Z})$ en $SL_2(\mathbb{Z}/N\mathbb{Z})$ es sobreyectiva asumimos que $\gamma \in SL_2(\mathbb{Z})$.
Denotamos por $\tau = \gamma(\tau')$ y por $m = c\tau' + d \neq 0$. Por consiguiente, se tiene que $m\tau = a\tau' + b$ y, por tanto, empleando el Corolario 3.8 y el Lema 3.3 para probar la última igualdad, se tiene que

$$m\Lambda_\tau = m(\tau\mathbb{Z} \oplus \mathbb{Z}) = (a\tau' + b)\mathbb{Z} \oplus (c\tau' + d)\mathbb{Z} = \Lambda_{\tau'},$$

además se cumple que $m(1/N+\Lambda_\tau) = (c\tau'+d)/N+\Lambda_{\tau'} = Q$. Esto muestra que $[E,Q] = [E_\tau, 1/N+\Lambda_\tau]$, siendo $E_\tau = \mathbb{C}/\Lambda_\tau$.
Para demostrar la segunda parte del apartado, primero suponemos que τ y $\tau' \in \mathbb{H}$, los cuales satisfacen $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. Este hecho implica que $\tau = \gamma(\tau')$ para algún $\gamma \in \Gamma_1(N)$. Tomando $m = c\tau'+d$ entonces como acabamos de mostrar se dan las siguientes igualdades

$$m\Lambda_\tau = \Lambda_{\tau'} \quad \text{y} \quad m(1/N+\Lambda_\tau) = (c\tau'+d)/N+\Lambda_{\tau'}.$$

Como $\gamma \in \Gamma_1(N)$ tenemos que $(c,d) \equiv (0,1) \mod N$, luego

$$m(1/N+\Lambda_\tau) = 1/N+\Lambda_{\tau'}.$$

Por tanto se tiene que $[E_\tau, 1/N+\Lambda_\tau] = [E_{\tau'}, 1/N+\Lambda_{\tau'}]$.
De forma recíproca, suponemos que $[E_\tau, 1/N+\Lambda_\tau] = [E_{\tau'}, 1/N+\Lambda_{\tau'}]$, entonces existe un isomorfismo entre E_τ y $E_{\tau'}$ que lleva $1/N+\Lambda_\tau$ en $1/N+\Lambda_{\tau'}$, teniendo en cuenta la forma de los isomorfismos entre toros, existe $m \in \mathbb{C}\setminus\{0\}$ tal que $m(1/N+\Lambda_\tau) = 1/N+\Lambda_{\tau'}$, además se sabe por el Lema 3.3 que existe un $\gamma \in SL_2(\mathbb{Z})$ tal que

$$\begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \begin{pmatrix} \tau' \\ 1 \end{pmatrix}.$$

Lo cual implica que $m = c\tau'+d$, pero como por hipótesis $m(1/N+\Lambda_\tau) = 1/N+\Lambda_{\tau'}$, se deduce que $(c,d) \equiv (0,1) \mod N$. Por tanto, como $\gamma \in SL_2(\mathbb{Z})$ tenemos que $a \equiv 1 \mod N$, luego $\gamma \in \Gamma_1(N)$ y, por ende, $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$.
Para demostrar el apartado $a)$ del teorema, podemos razonar de un modo similar. La demostración de que podemos encontrar un representante de la forma deseada es completamente análoga dado que en este punto no interviene el subgrupo de congruencias.
Razonando de manera parecida tenemos que dados τ, $\tau' \in \mathbb{H}$ tales que existe $\gamma \in SL_2(\mathbb{Z})$ con $\tau = \gamma(\tau')$ tenemos que

$$\langle m\left(\frac{1}{N}+\Lambda_\tau\right)\rangle = \langle \frac{c\tau'+d}{N}+\Lambda_{\tau'}\rangle.$$

Resulta que

$$\langle \frac{1}{N}+\Lambda_{\tau'}\rangle = \langle \frac{c\tau'+d}{N}+\Lambda_{\tau'}\rangle$$

si y solo si $c \equiv 0 \mod N$ y $mcd(d,N) = 1$, es decir, si y solo si, $\gamma \in \Gamma_0(N)$.
También podemos razonar de un modo análogo para demostrar el apartado $c)$. De manera similar escribimos

$$(P,Q) = \left(\frac{a\tau'+b}{N}+\Lambda_{\tau'}, \frac{c\tau'+d}{N}+\Lambda_{\tau'}\right).$$

Basta observar que P, Q generan $E[N]$ y su emparejamiento de Weil cumple que $e_N(P,Q) = e^{2\pi i/N}$ si y solo si la correspondiente matriz $\gamma \equiv I(\mod N)$, es decir, $\gamma \in \Gamma(N)$. □

Cuando $N = 1$ tenemos que $\Gamma_0(1) = \Gamma_1(1) = \Gamma(1) = SL_2(\mathbb{Z})$, luego $Y_0(1) = Y_1(1) = Y(1) = \{SL_2(\mathbb{Z})\tau : \tau \in \mathbb{H}\}$. Por tanto, cada $\tau \in \mathbb{H}$ determina una clase de isomorfía y a cada clase de isomorfía le podemos asignar $\tau \in \mathbb{H}$, único salvo por la acción de $SL_2(\mathbb{Z})$. Recordando que el invariante modular j de la Definición 3.35 es una función $SL_2(\mathbb{Z})-$invariante en $\mathbb{H}$, podemos definir el índice j para $SL_2(\mathbb{Z})\tau$ como $j(SL_2(\mathbb{Z})\tau) = j(\tau)$ y extender dicha definición a cualquier toro complejo.

Definición 4.6. *Sean E un toro complejo y $\tau \in \mathbb{H}$ tal que $E = \mathbb{C}/\Lambda_\tau$. Definimos $j(E_\tau) = j(SL_2(\mathbb{Z})\tau)$.*

El teorema de la modularidad que enunciaremos al final del trabajo afirma que las curvas elípticas con valores $j(E) = q \in \mathbb{Q}$ proceden de las formas modulares.
Las aplicaciones biyectivas entre espacios de moduli y curvas modulares nos dan más ejemplos de formas modulares. La idea fundamental es que podemos establecer una correspondencia entre curvas elípticas realzadas y funciones que cumplen la condición de modularidad de peso k respecto a un subgrupo de congruencias adecuado. Para precisar esta idea, necesitamos establecer primero una serie de conceptos.

Definición 4.7. *Sean $k \in \mathbb{Z}$ y $\Gamma \in \{\Gamma_0(N), \Gamma_1(N), \Gamma(N)\}$. Una función*

$$F : \{\textit{curvas elípticas realzada para } \Gamma\} \to \mathbb{C}$$

se dice que es homogénea de grado k con respecto a Γ si para todo $m \in \mathbb{C} \setminus \{0\}$, cumple que

$$\begin{aligned} F(\mathbb{C}/m\Lambda, mC) &= m^{-k}F(\mathbb{C}/\Lambda, C) && \textit{si } \Gamma = \Gamma_0(N) \\ F(\mathbb{C}/m\Lambda, mQ) &= m^{-k}F(\mathbb{C}/\Lambda, Q) && \textit{si } \Gamma = \Gamma_1(N) \\ F(\mathbb{C}/m\Lambda, (mP, mQ)) &= m^{-k}F(\mathbb{C}/\Lambda, (P,Q)) && \textit{si } \Gamma = \Gamma(N) \end{aligned}$$

Dada una función F como la anterior, podemos asociarle una función $f : \mathbb{H} \to \mathbb{C}$.

Definición 4.8. *Sea F una función homogénea de grado k con respecto a Γ, se dice que $f : \mathbb{H} \to \mathbb{C}$ es su función deshomogeneizada correspondiente si cumple que*

$$\begin{aligned} f(\tau) &= F(\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau \rangle) && \textit{si } \Gamma = \Gamma_0(N) \\ f(\tau) &= F(\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau) && \textit{si } \Gamma = \Gamma_1(N) \\ f(\tau) &= F(\mathbb{C}/\Lambda_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)) && \textit{si } \Gamma = \Gamma(N) \end{aligned}$$

Veamos que f cumple la condición de modularidad de peso k respecto a Γ.

Proposición 4.9. *Sea f una función deshomogeneizada correspondiente a F una función homogénea de grado k respecto a Γ, vemos que f cumple la condición de modularidad de peso k respecto a Γ.*

Demostración. Sin perdida de generalidad suponemos que $\Gamma = \Gamma_1(N)$, ya que para los otros dos subgrupos se prueba de forma muy similar. Sea $\gamma \in \Gamma$ y para todo $\tau \in \mathbb{H}$, sea $m = (c\tau + d)^{-1}$, usando la condición $(c,d) \equiv (0,1) \mod N$ y el Lema 3.3 podemos deducir que

$$\begin{aligned} f(\gamma(\tau)) &= F(\mathbb{C}/\Lambda_{\gamma(\tau)}, 1/N + \Lambda_{\gamma(\tau)}) = F(\mathbb{C}/m\Lambda_\tau, m(c\tau+d)/N + m\Lambda_\tau) \\ &= m^{-k}F(\mathbb{C}/\Lambda_\tau, (c\tau+d)/N + \Lambda_\tau) = m^{-k}F(\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau) = (c\tau+d)^k f(\tau). \end{aligned}$$

□

Por ejemplo, ver Ejemplo 3.31, las series de Eisenstein para retículos son funciones homogéneas de grado k y su función deshomogeneizada son las series de Eisestein en el semiplano superior. Recíprocamente dado f que cumple la condición de modularidad de peso k respecto a Γ podemos construir la correspondiente homogeneizada F.

Proposición 4.10. *Sea $f : \mathbb{H} \to \mathbb{C}$ una función que cumple la condición de modularidad de peso k respecto a $\Gamma \in \{\Gamma_0(N), \Gamma_1(N), \Gamma(N)\}$. Podemos definir una función F sobre el conjunto de curvas elípticas realzadas para Γ tal que F es homogénea de grado k y f es la correspondiente deshomogeneizada.*

Demostración. Vamos a probar esta proposición suponiendo que $\Gamma = \Gamma_1(N)$, para los otros dos casos se hace de manera similar. De manera natural, definimos F para las curvas realzadas del tipo $(\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau)$ por

$$F(\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau) = f(\tau).$$

Veamos que F está bien definida. Para ello veamos que sean $(\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau)$ y $(\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'})$ dos curvas elípticas realzadas equivalentes, entonces su imagen es la misma. Basta observar que si son equivalentes entonces existe un isomorfisfo entre Λ_τ y $\Lambda_{\tau'}$, por tanto existe una matriz invertible tal que

$$\begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau' \\ 1 \end{pmatrix},$$

por tanto $(c,d) = (0,1)$. Por otro lado, por el Teorema 4.5 sabemos que como se da la igualdad entre clases $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] = [\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}]$ entonces $\tau' = \gamma(\tau)$ con $\gamma \in \Gamma_1(N)$, por tanto $(a,b) = (1,b)$, siendo b cualquier número entero. Además como f cumple la condición de modularidad de peso k y que $(c\tau + d) = 1$ sabemos que

$$F(\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}) = f(\tau') = f(\gamma(\tau)) = f(\tau) = F(\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau),$$

por tanto está bien definida.
Veamos como extender F a una función sobre todas las curvas elípticas realzadas. Dada (E,Q) sabemos por el Teorema 4.5, que existen $\tau,\tau' \in \mathbb{H}$, $m \in \mathbb{C}\setminus\{0\}$, $c,d \in \mathbb{Z}$ con $mcd(c,d,N)=1$ tal que

$$E = \mathbb{C}/\Lambda_{\tau'}, \quad Q = \frac{c\tau'+d}{N} + \Lambda_{\tau'}, \quad m\Lambda_\tau = \Lambda_{\tau'} \quad \text{y} \quad [E,Q] = [\mathbb{C}/\Lambda_\tau, \frac{1}{N}+\Lambda_\tau].$$

Por consiguiente observamos que

$$m^{-k}F\left(\mathbb{C}/\Lambda_\tau, \frac{1}{N}+\Lambda_\tau\right) = m^{-k}f(\tau) = f(\tau') = F\left(\mathbb{C}/\Lambda_{\tau'}, \frac{1}{N}+\Lambda_{\tau'}\right).$$

De manera coherente, definimos

$$F(E,Q) := m^{-k}f(\tau).$$

La función F es homogénea de grado k y su deshomogeneizada coincide con f. □

En resumen, esta proposición muestra que las curvas modulares son el dominio de la definición natural de las funciones modulares de peso k.

4.2. Topología de las curvas modulares.

Recordamos que dado un subgrupo Γ de $SL_2(\mathbb{Z})$ la curva modular correspondiente ha sido definida como el espacio cociente $\mathbb{H}/\Gamma$ de $\mathbb{H}$ por la acción de Γ, es decir, es el conjunto de órbitas que denotamos por $Y(\Gamma) = \{\Gamma\tau : \tau \in \mathbb{H}\}$. En esta sección veremos como dotar a $Y(\Gamma)$ de estructura de superficie de Riemann. Comenzamos introduciendo las propiedades fundamentales de la topología natural de $\mathbb{H}$ e $Y(\Gamma)$. Primero de todo, cabe destacar que $\mathbb{H}$ hereda la topología euclídea como subespacio de $\mathbb{R}^2$. Por otra parte la proyección natural $\Pi : \mathbb{H} \to Y(\Gamma)$ dada por $\Pi(\tau) = \Gamma\tau$, dota a $Y(\Gamma)$ de la topología cociente, es decir, un subconjunto de $Y(\Gamma)$ es abierto si su contraimagen bajo la aplicación Π es un subconjunto abierto en $\mathbb{H}$. Dado $U \subseteq \mathbb{H}$ abierto tenemos que

$$\Pi^{-1}(\Pi(U)) = \{\gamma(u) : \gamma \in \Gamma, u \in U\} = \cup_{\gamma\in\Gamma}\gamma(U)$$

que es abierto por ser unión de abiertos, luego Π es una aplicación abierta. Además se cumple la siguiente equivalencia.

Proposición 4.11. *Sean U_1 y U_2, dos subconjuntos abiertos de $\mathbb{H}$ se cumple que*

$$\Pi(U_1)\cap\Pi(U_2) = \emptyset \text{ en } Y(\Gamma) \text{ si y solo si } \Pi(U_1)\cap U_2 = \emptyset \text{ en } \mathbb{H}.$$

Demostración. Basta con observar que $\Pi(U_1)\cap\Pi(U_2) = \emptyset$ si y solo si, para cualquier $\tau_1 \in U_1$ no existe ningún $\tau_2 \in U_2$ tal que $\Gamma\tau_1 = \Gamma\tau_2$, lo que significa que para cualquier $\tau_1 \in U_1$ no existe ninguna función $\gamma \in \Gamma$ tal que $\gamma(\tau_1) = \tau_2$ para algún $\tau_2 \in U_2$, esto ocurre si y solo si $\Pi(U_1)\cap U_2 = \emptyset$. □

Por otra parte, como Π es una aplicación continua y $\mathbb{H}$ es conexo, entonces $Y(\Gamma)$ es un espacio conexo también. En esta sección veremos que a parte de ser conexo $Y(\Gamma)$ es Hausdorff. La clave para demostrar esto, y para poder en secciones sucesivas dar coordenadas a los puntos en $Y(\Gamma)$, es la idea de que para dos puntos cualesquiera en $\mathbb{H}$ podemos encontrar entornos lo suficientemente pequeños de manera que cada transformación de $SL_2(\mathbb{Z})$ que aleja los puntos también aleja los correspondientes entornos. En este caso decimos que la acción de $SL_2(\mathbb{Z})$ sobre $\mathbb{H}$ es propiamente discontinua. Para poder probar esta propiedad necesitamos el siguiente lema auxiliar.

Lema 4.12. *Sean τ_1 y $\tau_2 \in \mathbb{H}$ y U_1 un entorno de τ_1 y U_2 un entorno de τ_2, tales que $\overline{U_1} \subseteq \mathbb{H}$ y $\overline{U_2} \subseteq \mathbb{H}$. Entonces para todo par de puntos $(c,d) \in \mathbb{Z}^2$ menos un conjunto finito, se cumple que*

$$sup\left\{Im(\gamma(\tau)) : \gamma = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \tau \in U_1\right\} < inf\{Im(\tau) : \tau \in U_2\}$$

Demostración. Consideramos

$$y_1 = inf\{\mathrm{Im}(\tau) : \tau \in U_1\}, \quad y_2 = inf\{\mathrm{Im}(\tau) : \tau \in U_2\}, \quad Y_1 = sup\{\mathrm{Im}(\tau) : \tau \in U_1\}$$

que son todos reales positivos porque $\overline{U_1} \subseteq \mathbb{H}$ y $\overline{U_2} \subseteq \mathbb{H}$. Por la Proposición 2.3 se tiene que $\mathrm{Im}(\gamma(\tau)) = \mathrm{Im}(\tau)/|c\tau+d|^2$ para todo $\gamma \in SL_2(\mathbb{Z})$, teniendo en cuenta que $|c\tau+d|^2 > (cRe(\tau)+d)^2$, observamos que $\mathrm{Im}(\gamma(\tau)) < Y_1/(cRe(\tau)+d)^2$. Por otra parte, observando que $|c\tau+d|^2 > c^2\mathrm{Im}(\tau)^2$, se obtiene que $\mathrm{Im}(\gamma(\tau)) < 1/(c^2\mathrm{Im}(\tau))$ y, por ende, que $\mathrm{Im}(\gamma(\tau)) < 1/(c^2 y_2)$. Por tanto, se cumple que

$$\mathrm{Im}(\gamma(\tau)) < inf\left\{1/(c^2 y_1),\ Y_1/(cRe(\tau)+d)^2\right\}.$$

Por otro lado, como y_1, y_2 son positivos podemos garantizar que existe $c_0 \in \mathbb{Z}$ tal que para todo $c \in \mathbb{Z}$ con $|c| \geq c_0$ se tiene que $1/(c^2 y_1) < y_2$. Por consiguiente, para todo $c \in \mathbb{Z}$ excepto quizás los del intervalo $(-c_0, c_0)$ se tiene la desigualdad buscada. Para $c \in (-c_0, c_0) \cap \mathbb{Z}$, podemos garantizar que existe $d_c \in \mathbb{Z}$ tal que para todo $|d| \geq d_c$ se cumple que $Y_1/(cRe(\tau)+d)^2 < y_2$. Por tanto, se cumple la propiedad para todos los $c, d \in \mathbb{Z}$ excepto un conjunto finito. □

Gracias a este lema, estamos en disposición de demostrar que la acción de grupo de $SL_2(\mathbb{Z})$ sobre $\mathbb{H}$ es propiamente discontinua, como establece la siguiente proposición.

Proposición 4.13. *Sean τ_1 y $\tau_2 \in \mathbb{H}$. Entonces existen entornos U_1 de τ_1 y U_2 de τ_2 en $\mathbb{H}$ tal que para todo $\gamma \in SL_2(\mathbb{Z})$ se tiene que*

$$si\ \gamma(U_1) \cap U_2 \neq \emptyset,\ entonces\ \gamma(\tau_1) = \tau_2.$$

Demostración. Sea U_1' un entorno de τ_1 cualquiera con clausura compacta en $\mathbb{H}$ y análogamente para U_2' de τ_2. Por el Lema 4.12, sabemos que dado un $\gamma \in SL_2(\mathbb{Z})$ si $\gamma(U_1') \cap U_2' \neq \emptyset$ entonces hay una cantidad finita de posibilidades para la fila inferior de γ. Ahora para cada una de estas posibilidades (c,d) que cumplen que la intersección es no vacía queremos saber cuantas matrices hay en $SL_2(\mathbb{Z})$ con ese par como segunda fila. Para ello, fijamos $\gamma \in SL_2(\mathbb{Z})$ con fila inferior (c,d) alguna de las posibilidades problemáticas. Observamos que

$$\left\{\gamma' \in SL_2(\mathbb{Z}) :\ \text{fila inferior de } \gamma' \text{ es } (c,d)\right\} = \left\{\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} : k \in \mathbb{Z}\right\}.$$

Para probar esta igualdad, basta resolver el sistema de ecuaciones

$$a' = a + kc \quad b' = b + kd.$$

Cuya solución es $k = ab' - a'b$. Esto significa que para cualquier $\gamma' \in SL_2(\mathbb{Z})$ se cumple

$$\gamma'(U_1') \cap U_2' = \left(\gamma(U_1') + k\right) \cap U_2'.$$

Por tanto, para cada par de puntos (c,d) que no cumplen la propiedad del Lema 4.12, solo hay un número finito de matrices tal que $\gamma'(U_1') \cap U_2' \neq \emptyset$ ya que para cualquiera de ellos existe un k_0 tal que para todo $|k| \geq k_0$, se tiene que $(\gamma(U_1') + k) \cap U_2' = \emptyset$. Denominamos $F = \{\gamma \in SL_2(\mathbb{Z}) : \gamma(U_1') \cap U_2' \neq \emptyset, \gamma(\tau_1) \neq \tau_2\}$, el cual es un conjunto finito por ser la unión finita de conjuntos finitos. Para cada $\gamma \in F$, como $\gamma(\tau_1) \neq \tau_2$, existen entornos disjuntos $U_{1,\gamma}$ de $\gamma(\tau_1)$ y $U_{2,\gamma}$ de τ_2 en $\mathbb{H}$. A partir de ellos definimos

$$U_1 = U_1' \cap \left(\cap_{\gamma \in F} \gamma^{-1}\left(U_{1,\gamma}\right)\right) \text{ un entorno de } \tau_1 \in \mathbb{H}.$$
$$U_2 = U_2' \cap \left(\cap_{\gamma \in F} U_{2,\gamma}\right) \text{ un entorno de } \tau_2 \in \mathbb{H}.$$

Sea $\gamma \in SL_2(\mathbb{Z})$ tal que$\gamma(U_1) \cap U_2 \neq \emptyset$. Para mostrar que $\gamma(\tau_1) = \tau_2$ es suficiente ver que $\gamma \notin F$. Suponemos que $\gamma \in F$, entonces $U_1 \subseteq \gamma^{-1}\left(U_{1,\gamma}\right)$ y $U_2 \subseteq U_{2,\gamma}$, por tanto $\gamma(U_1) \cap U_2 \subseteq U_{1,\gamma} \cap U_{2,\gamma}$. Esto es una contradicción con la hipótesis $U_{1,\gamma} \cap U_{2,\gamma} = \emptyset$ ya que $\gamma(U_1) \cap U_2 \neq \emptyset$. Concluimos que $\gamma \notin F$. □

Corolario 4.14. *Para cada subgrupo de congruencias Γ de $SL_2(\mathbb{Z})$. La curva modular $Y(\Gamma)$ es Hausdorff, es decir, puntos distintos poseen entornos disjuntos.*

Demostración. Sea $\Pi(\tau_1)$ y $\Pi(\tau_2)$ distintos puntos de $Y(\Gamma)$. Elegimos U_1 y U_2 entornos de τ_1, τ_2 como los definidos en la Proposición 4.13. Como $\gamma(\tau_1) \neq \tau_2$ para todo $\gamma \in \Gamma$, puesto que hemos elegido puntos distintos, la Proposición 4.13 nos garantiza que existen entornos U_1 y U_2 tales que $\gamma(U_1) \cap U_2 = \emptyset$. Por la Proposición 4.11 se obtiene que $\Pi(U_1)$ y $\Pi(U_2)$ son conjuntos disjuntos que contienen a $\Pi(\tau_1)$ y a $\Pi(\tau_2)$ respectivamente. Como Π es una aplicación abierta entonces $\Pi(U_1)$ y $\Pi(U_2)$ son entornos disjuntos de los puntos. □

4.3. Puntos elípticos de una curva modular

Para poder enunciar el teorema de la modularidad necesitamos dotar a $Y(\Gamma)$ de una estructura de variedad diferencial. Por consiguiente, necesitamos definir coordenadas locales en cada punto $\Pi(\tau) \in Y(\Gamma)$. Si para el punto $\Pi(\tau)$ podemos encontrar un entorno U de τ en $\mathbb{H}$ de forma que $\Pi_{|_U} : U \to \Pi(U)$ es homeomorfismo, entonces podríamos tomar la inversa local como la carta correspondiente.
Sin embargo, existen puntos de $\mathbb{H}$ para los cuales no es posible construir la correspondiente carta de esta forma. Por ejemplo, tomando $\Gamma = SL_2(\mathbb{Z})$ y $\tau = i$, tenemos que la transformación $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ fija el punto i. Cerca de $\tau = i$, esta γ actúa casi como un giro de 180 grados centrado en i. Por tanto, todo entorno U de i en $\mathbb{H}$ contiene puntos $\gamma-$equivalentes distintos, luego no podemos construir la carta empleando $\Pi_{|_U} : U \to \Pi(U)$ dado que no es inyectiva.
Este fenómeno ocurre porque para estos puntos, que denominaremos puntos elípticos, el estabilizador respecto a la acción de Γ es no trivial.

Definición 4.15. *Sea Γ un subgrupo de congruencias de $SL_2(\mathbb{Z})$. Para cada $\tau \in \mathbb{H}$ definimos Γ_τ el subgrupo estabilizador de Γ respecto a τ como*

$$\Gamma_\tau = \{\gamma \in \Gamma : \quad \gamma(\tau) = \tau\}.$$

Diremos que τ es elíptico para Γ si Γ_τ es no trivial como grupo de transformaciones, es decir, si $\{\pm I\}$ es un subgrupo propio de Γ_τ. El correspondiente punto $\Pi(\tau) \in Y(\Gamma)$ se llama también punto elíptico en $Y(\Gamma)$.

Nuestro objetivo en esta sección es probar que aun que Γ_τ no sea trivial podemos garantizar que es cíclico y finito en los puntos elípticos, lo que es suficiente para construir cartas.
Comenzamos estudiando lo que ocurre para el caso particular $Y(1) = \mathbb{H}/SL_2(\mathbb{Z})$ y después lo extenderemos a un subgrupo de congruencias cualquiera. Consideramos la región de $\mathbb{H}$ definida por

$$D = \{\tau \in \mathbb{H} : |Re(\tau)| \leq 1/2, \ |\tau| \geq 1\}.$$

Vamos a probar que podemos identificar $Y(1)$ con D. Por tanto, por lo probado en la Sección 4.1, D representará el espacio de moduli de las curvas elípticas, identificando cada punto $\tau \in D$ con la clase de $\mathbb{C}/\Lambda_\tau$.

Lema 4.16. *La aplicación $\Pi : D \to Y(1)$, dada por $\Pi(\tau) = SL_2(\mathbb{Z})\tau$, es sobreyectiva.*

Demostración. Dado $\tau \in \mathbb{H}$, basta probar que es $SL_2(\mathbb{Z})-$equivalente a un punto en D. Dado un punto $\tau = x + iy$ sabemos que existe $N \in \mathbb{Z}$ tal que $N - 1/2 \leq x \leq N + 1/2$. Por tanto, empleando la transformación

$$\begin{pmatrix} 1 & -N \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$$

trasladamos el punto τ a τ' con $|Re(\tau')| \leq 1/2$. Si $|\tau'| \geq 1$ hemos terminado, si $|\tau'| < 1$ utilizando la transformación

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

trasladamos τ' a $-1/\tau'$, donde $\mathrm{Im}(-1/\tau') = \mathrm{Im}(\tau')/|\tau|^2 > \mathrm{Im}(\tau')$. Si al aplicar la transformación resulta que $|Re(-1/\tau')| > 1/2$, entonces volvemos a aplicar la traslación para obtener un punto de la banda. Podemos iterar este procedimiento obteniendo a cada paso un elemento de la banda con parte imaginaria cada vez mayor. Sin embargo, solo hay una cantidad finita de puntos $(c,d) \in \mathbb{Z}^2$ tales que $|c\tau + d| < 1$. Por la Proposición 2.3, tenemos que

$$Im(\gamma(\tau)) = \frac{Im(\tau)}{|c\tau + d|^2} \ \text{ con } \ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Razonando como en la demostración de la Proposición 4.13 como dos transformaciones con la misma fila inferior se diferencian en una traslación, podemos concluir que solo existe una cantidad finita de $\gamma \in SL_2(\mathbb{Z})$ que mantengan a τ en la banda y aumenten el tamaño de su parte real. Por tanto, podemos garantizar que el algoritmo termina en algún momento y transformamos τ en un punto de D. □

Se puede observar que la aplicación Π no es inyectiva en D, ya que la transformación que lleva τ a $\tau+1$ identifica los puntos de los bordes de la banda y la transformación que lleva τ a $-1/\tau$ identifica los puntos del arco de circunferencia. El siguiente lema muestra que solo existen estas identificaciones.

Lema 4.17. *Sean τ_1 y τ_2 dos puntos distintos de D y tal que $\gamma(\tau_1)=\tau_2$ para algún $\gamma\in SL_2(\mathbb{Z})$. Entonces se cumple una de las dos condiciones*

a) $Re(\tau_1)=\pm 1/2$ *y* $\tau_2=\tau_1\mp 1$.

b) $|\tau_1|=1$ *y* $\tau_2=-1/\tau_1$.

Demostración. Sin pérdida de generalidad, asumimos que $\mathrm{Im}(\tau_2)\geq \mathrm{Im}(\tau_1)$. Como $\tau_1\in D$, entonces tenemos que $\mathrm{Im}(\tau_1)\geq \sqrt{3}/2$, en caso contrario, como $|Re(\tau_1)|\leq 1/2$, tendríamos que $|\tau_1|<1$ lo que es imposible. Escribimos

$$\gamma=\begin{pmatrix} a & b\\ c & d\end{pmatrix},$$

entonces $|c\tau_1+d|\leq 1$ dado que $\mathrm{Im}(\tau_2)\geq \mathrm{Im}(\tau_1)$. Por tanto, por la Proposición 2.3 se cumple la siguiente desigualdad

$$|c|\sqrt{3}/2\leq |c|\mathrm{Im}(\tau_1)=|\mathrm{Im}(c\tau_1+d)|\leq |c\tau_1+d|\leq 1.$$

En consecuencia, como $c\in\mathbb{Z}$, entonces $|c|\in\{0,1\}$. Ahora trataremos cada caso de forma independiente.

(I) Si $c=0$, entonces

$$\gamma=\pm\begin{pmatrix} 1 & b\\ 0 & 1\end{pmatrix},$$

por tanto $\tau_2=\tau_1+b$. Dado que tenemos que $Re(\tau_2)=Re(\tau_1)+b$ y como $\tau_1,\ \tau_2\in D$ se cumple que $|Re(\tau_2)|\leq 1/2$ y $|Re(\tau_1)|\leq 1/2$. Como $\tau_1\neq\tau_2$ necesariamente $b\neq 0$, luego la única posibilidad es $b=\pm 1$ y $|Re(\tau_2)|=\pm 1/2$.

(II) Si $c=|1|$, entonces la condición inicial de $|c\tau_1\pm d|\leq 1$ se reduce a $|\tau_1\pm d|\leq 1$. Por tanto, $(Re(\tau_1)\pm d)^2+\mathrm{Im}(\tau_1)^2\leq 1$ y se da la siguiente desigualdad

$$(Re(\tau_1)\pm d)^2\leq 1-\mathrm{Im}(\tau_1)^2\leq 1-3/4\leq 1/4.$$

Por ende, $|(Re(\tau_1)\pm d)|\leq 1/2$ y como $|Re(\tau_1)|\leq 1/2$, se deduce que $|d|\leq 1$, por tanto $d\in\{-1,0,1\}$.

(1) Si $|d|=1$, entonces se cumple que $|Re(\tau_1)\pm d|=|Re(\tau_1)\pm 1|\leq 1/2$. Por tanto, despejando para cada valor de d tenemos dos opciones, por un lado $-3/2\leq Re(\tau_1)\leq -1/2$ cuando $d=1$, por otro lado $1/2\leq Re(\tau_1)\leq 3/2$ cuando $d=-1$. Como sabemos por hipótesis que $\tau_1\in D$, entonces la única posibilidad es que $|Re(\tau_1)|=1/2$. Entonces despejando $\mathrm{Im}(\tau_1)$ de $(Re(\tau_1)+d)^2+\mathrm{Im}(\tau_1)^2\leq 1$ se obtiene que $\mathrm{Im}(\tau_1)\leq\sqrt{3}/2$, pero por las hipótesis iniciales sabíamos que $\mathrm{Im}(\tau_1)\geq\sqrt{3}/2$, por lo que se puede concluir que $\mathrm{Im}(\tau_1)=\sqrt{3}/2$. Una vez obtenido esto, se puede deducir que entonces $|c\tau_1+d|^2=|\tau_1|^2=1$ y por tanto que $\mathrm{Im}(\tau_2)=\sqrt{3}/2$, además como $\tau_1\neq\tau_2$ y solo hay dos puntos en D cuya parte imaginaria es $\sqrt{3}/2$, los cuales son τ_1 y $-1/\tau_1$, se cumple que $|\tau_1|=1$ y $\tau_2=-1/\tau_1$.

(2) Si $|d|=0$, entonces la condición inicial de $|c\tau_1\pm d|\leq 1$ se reduce a $|\tau_1|\leq 1$, como $\tau_1\in D$ entonces $|\tau_1|=1$, gracias a esto se puede deducir que $\mathrm{Im}(\gamma(\tau_1))=\mathrm{Im}(\tau_1)/|c\tau_1+d|^2=\mathrm{Im}(\tau_1)$. En resumen, tenemos que $|\tau_1|=1$ y $\mathrm{Im}(\tau_1)=\mathrm{Im}(\tau_2)$. Por tanto, como

$$\gamma^{-1}=\begin{pmatrix} a & \pm 1\\ \mp 1 & 0\end{pmatrix}^{-1}=\begin{pmatrix} 0 & \mp 1\\ \pm 1 & a\end{pmatrix}$$

y como $\mathrm{Im}(\tau_1)=\mathrm{Im}(\tau_2)$, razonando de manera análoga para τ_2 tenemos que $|a|\leq 1$. Tanto en el caso (1) como en el caso (2) esto nos permite concluir que $|\tau_2|=1$. Como $\mathrm{Im}(\tau_1)=\mathrm{Im}(\tau_2)$, se tiene que $Re(\tau_1)=-Re(\tau_2)$, es decir, $\tau_2=-1/\tau_1$.

□

En conclusión, identificando los puntos de la frontera de D de manera adecuada, el conjunto resultante es un dominio fundamental de la acción de $SL_2(\mathbb{Z})$ sobre $\mathbb{H}$. Emplearemos esta representación en el estudio de los puntos elípticos. Comenzamos obteniendo información sobre el polinomio característico de las transformaciones no triviales que fijan algún punto.

Proposición 4.18. *Sean $\tau \in \mathbb{H}$ y $\gamma \in SL_2(\mathbb{Z})$, con $\gamma \neq \pm I$ tal que $\gamma(\tau) = \tau$, entonces el polinomio característico de γ es x^2+1 ó $x^2 \pm x + 1$.*

Demostración. Con la notación habitual si $\gamma(\tau) = \tau$, entonces $a\tau + b = c\tau^2 + d\tau$. Como $\tau \in \mathbb{H}$, $\tau \notin \mathbb{Q}$ y como $\gamma \neq \pm I$, podemos asegurar que $c \neq 0$. Por la Proposición 2.3, como $\mathrm{Im}(\gamma(\tau)) = \mathrm{Im}(\tau)$ deducimos que $|c\tau + d|^2 = 1$. Por otro lado, como $\tau \notin \mathbb{R}$, el discriminante de la ecuación de segundo grado es $(d-a)^2 + 4bc < 0$. Como $\gamma \in SL_2(\mathbb{Z})$, $bc = ad - 1$ luego sustituyendo obtenemos que $(d+a)^2 - 4 < 0$. En conclusión, se tiene que $|d+a| < 2$, lo que nos permite diferenciar en dos casos

1. Si $a + d = 0$, entonces $a = -d$, luego la traza de γ es nula y, como $det(\gamma) = 1$, el polinomio característico viene dado por $x^2 + 1$.
2. Si $|a+d| = 1$, entonces la traza de γ es ± 1 y, como $det(\gamma) = 1$, el polinomio característico viene dado por $x^2 \pm x + 1$.

□

Corolario 4.19. *Sean $\tau \in \mathbb{H}$ y sea $\gamma \in SL_2(\mathbb{Z})$, con $\gamma \neq \pm I$ tal que $\gamma(\tau) = \tau$, entonces $\gamma^4 = I$ ó $\gamma^3 = I$ ó $\gamma^6 = I$.*

Demostración. Para realizar esta demostración basta con sustituir γ en su polinomio característico y operar hasta obtener la identidad. □

Se puede observar que por tanto si $\gamma \in SL_2(\mathbb{Z})$ deja fijo a un punto de $\mathbb{H}$ entonces, tiene orden $1, 2, 3, 4, 6$ como matriz. Las matrices de órdenes 1 y 2 se corresponden con las transformaciones triviales, para las no triviales tenemos la siguiente proposición.

Proposición 4.20. *Sean $\gamma \in SL_2(\mathbb{Z})$,con $\gamma \neq \pm I$ y $\tau \in \mathbb{H}$ tal que $\gamma(\tau) = \tau$. Entonces*

a) Si γ tiene orden 3, entonces γ es una conjugación de $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}^{\pm 1}$ en $SL_2(\mathbb{Z})$.

b) Si γ tiene orden 4, entonces γ es una conjugación de $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}^{\pm 1}$ en $SL_2(\mathbb{Z})$.

c) Si γ tiene orden 6, entonces γ es una conjugación de $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{\pm 1}$ en $SL_2(\mathbb{Z})$.

Recordamos que γ y γ' son conjugadas en $SL_2(\mathbb{Z})$ si existe $\delta \in SL_2(\mathbb{Z})$ tal que $\gamma = \delta\gamma'\delta^{-1}$.

Demostración. Vamos a empezar probando el caso c). Como $\gamma^6 = I$ podemos dotar al retículo $L = \mathbb{Z}^2$ de estructura de $\mathbb{Z}[\mu_6]-$módulo donde $\mu_6 = e^{2\pi i/6}$ definiendo el producto por escalares como

$$(a + b\mu_6)v := (aI + b\gamma)v$$

donde $a,\ b \in \mathbb{Z}$ y en el lado derecho considerando el producto de matrices.
El anillo $\mathbb{Z}[\mu_6]$ es un dominio de ideales principales, una prueba de este hecho clásico se puede encontrar en [9], aunque se puede demostrar de manera directa de un modo similar a la prueba para $\mathbb{Z}[i]$. Como L es un $\mathbb{Z}[\mu_6]-$módulo finitamente generado, el teorema de descomposición de módulos sobre un dominio de ideales principales garantiza que L es isomorfo a una suma de la forma $\oplus_k \mathbb{Z}[\mu_6]/I_k$ donde I_k es un ideal de $\mathbb{Z}[\mu_6]$. Tenemos que, como grupo abeliano, L es libre de grado 2. Por otro lado, todo ideal I_k no nulo también es un grupo abeliano libre de rango 2, luego el cociente $\mathbb{Z}[\mu_6]/I_k$ es un grupo de torsión. En consecuencia, en la suma no pueden aparecer sumandos de esta forma, es decir, la suma se limita a los sumandos de la forma $\mathbb{Z}[\mu_6]$. De hecho, podemos garantizar que solo aparece un único sumando porque $\mathbb{Z}[\mu_6]$ es isomorfo a $\mathbb{Z} \times \mathbb{Z}$ como grupo abeliano. En conclusión, existe un isomorfismo de $\mathbb{Z}[\mu_6]-$módulos $\Phi_\gamma : \mathbb{Z}[\mu_6] \to L$.

Denotamos por $u = \Phi_\gamma(1)$ y $v = \Phi_\gamma(\mu_6)$ y por $[u\ v]$ la matriz con columnas los vectores u, v. Entonces $L = \mathbb{Z}^2 = \mathbb{Z}u + \mathbb{Z}v$ lo que implica que la matriz $[u\ v]$ tiene $det([u\ v]) = \pm 1$. Teniendo en cuenta que

$$\gamma u = (0I + 1\gamma)u = \mu_6 u = \mu_6 \Phi_\gamma(1) = \Phi_\gamma(\mu_6) = v,$$
$$\gamma v = (0I + 1\gamma)v = \mu_6 v = \mu_6 \Phi_\gamma(\mu_6) = \Phi_\gamma(\mu_6^2) = \Phi_\gamma(-1 + \mu_6) = -u + v,$$

obtenemos que

$$\gamma[u\ v] = [v\ \ -u+v] = [u\ v]\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad \text{entonces} \quad \gamma = [u\ v]\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}[u\ v]^{-1}.$$
$$\gamma[v\ u] = [-u+v\ \ v] = [v\ u]\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \quad \text{entonces} \quad \gamma = [v\ u]\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{-1}[v\ u]^{-1}.$$

Una de las dos matrices $[v\ u]$ ó $[u\ v] \in SL_2(\mathbb{Z})$. Por tanto, queda probado el apartado.
La parte b) se demuestra de forma análoga cambiando $\mathbb{Z}[\mu_6]$ por $\mathbb{Z}[i]$. Para la parte a), observamos que si γ tiene orden 3, entonces $-\gamma$ tiene orden 6 y, por tanto, concluimos utilizando el caso c). □

Una vez conocida la forma de las matrices que dejan fijos los puntos de $\mathbb{H}$, podemos calcular los puntos elípticos y los correspondientes subgrupos estabilizadores respecto a la acción de $SL_2(\mathbb{Z})$.

Corolario 4.21. *Los puntos elípticos en $SL_2(\mathbb{Z})$ son $SL_2(\mathbb{Z})i$ y $SL_2(\mathbb{Z})\mu_3$, siendo $\mu_3 = e^{2\pi i/3}$. La curva modular $Y(1)$ tiene dos puntos elípticos distintos. Los estabilizadores respectivos de i y μ_3 son*

$$SL_2(\mathbb{Z})_i = \langle \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \rangle \ \ y \ \ SL_2(\mathbb{Z})_{\mu_3} = \langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \rangle.$$

Para cada punto elíptico τ de $SL_2(\mathbb{Z})$, el estabilizador $SL_2(\mathbb{Z})_\tau$ es cíclico finito.

Demostración. Resolviendo la ecuación $\gamma(\tau) = \tau$ con las matrices principales de la Proposición 4.20, obtenemos que los puntos fijos de esas matrices son i e μ_3. Por otro lado para cualquier matriz conjugada γ', si $\gamma(i) = i$, entonces la matriz $\gamma'\gamma\gamma'^{-1}$ deja fijo a $\gamma'(i)$ y de forma análoga pasa con las matrices conjugadas de aquellas que dejan fijo a μ_3, por tanto, los puntos elípticos en $SL_2(\mathbb{Z})$ son $SL_2(\mathbb{Z})i$ y $SL_2(\mathbb{Z})\mu_3$.

Para demostrar que la curva modular $Y(1)$ tiene dos puntos elípticos distintos, basta con ver que no existe ninguna trasformación $\gamma \in SL_2(\mathbb{Z})$ tal que $\gamma(i) = \mu_3$. Resolviendo la ecuación obtenemos que $2a = -c + d\sqrt{3}$ y que $2b = -d - c\sqrt{3}$ y, por tanto, no existe una solución con números enteros.

Por otra parte, resolviendo la ecuación $\gamma(i) = i$, obtenemos que las únicas dos transformaciones no triviales que dejan i fijo son

$$\pm \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix},$$

por tanto, es fácil deducir que su estabilizador es

$$SL_2(\mathbb{Z})_i = \langle \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \rangle.$$

Resolviendo la ecuación para μ_3 y teniendo en cuenta que $|c\mu_3 + d|^2 = 1$, obtenemos que las matrices resultantes son aquellas que tienen la forma

$$\begin{pmatrix} a & b \\ -b & a-b \end{pmatrix} \text{ tal que } (2a-b)^2 + 3b^2 = 4.$$

Por tanto $|2a-b| < 2$ y $|b| < 2$, además como sabemos que $a, b \in \mathbb{Z}$, obtenemos que las matrices que dejan fijo a μ_3 son:

$$\pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \ \pm \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Por tanto, se puede comprobar que el estabilizador de μ_3 es

$$SL_2(\mathbb{Z})_{\mu_3} = \langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \rangle.$$

Dado $\tau \in \mathbb{H}$, sin pérdida de generalidad, suponemos que existe $\gamma \in SL_2(\mathbb{Z})$ tal que $\gamma(i) = \tau$. Por ende, $\Gamma_\tau = \gamma\Gamma_i\gamma^{-1}$ que es también subgrupo cíclico. □

Nótese que cuando estudiábamos los puntos que anulaban a_2 y a_3 en la Proposición 3.38, también encontrábamos los puntos i y μ_3.

Corolario 4.22. *Sea Γ un subgrupo de congruencias de $SL_2(\mathbb{Z})$. La curva modular $Y(\Gamma)$ tiene una cantidad finita de puntos elípticos. Para cada punto elíptico τ de Γ el estabilizador Γ_τ es cíclico y finito.*

Demostración. Como Γ es un subgrupo de congruencias entonces $\Gamma(N) \subseteq \Gamma$ para algún $N \in \mathbb{N}_{\geq 1}$. Por tanto, por la Proposición 2.25 sabemos que $[SL_2(\mathbb{Z}) : \Gamma]$ es finito y por ende se puede descomponer $SL_2(\mathbb{Z}) = \cup_{j=1}^{d} \Gamma\gamma_j$.
Por consiguiente, el conjunto de puntos elípticos de la curva modular $Y(\Gamma)$ es un subconjunto del conjunto $E_\Gamma = \{\Gamma\gamma_j(i), \Gamma\gamma_j(\mu_3) : 1 \leq j \leq d\}$ y, por tanto, finito. Para cada punto elíptico τ, se cumple que $\Gamma_\tau \subseteq SL_2(\mathbb{Z})_\tau$ el cual es cíclico y finito, por tanto será un subgrupo cíclico y finito. □

Capítulo 5

Teorema de la modularidad vía superficies de Riemann

El objetivo del último capítulo es enunciar una versión del teorema de la modularidad entendiendo todos los elementos que intervienen en la misma. Para poder enunciar esta versión es necesario dotar a $Y(\Gamma)$ de estructura de superficie de Riemann y construir la compactificación de dicha superficie añadiendo las cúspides de Γ. Esta curva modular compacta se denota por $X(\Gamma)$ y es la que aparece en el enunciado del teorema de la modularidad.

5.1. Curvas modulares como superficies de Riemann.

En esta sección se va a estudiar como dotar de coordenadas locales a una curva modular $Y(\Gamma)$. Para ello necesitamos encontrar para cada punto $\Pi(\tau) \in Y(\Gamma)$, un entorno U' y un homeomorfismo $\varphi' : U' \to V \in \mathbb{C}$ tal que si tenemos φ'_1 y φ'_2 con $U'_1 \cap U'_2 \neq \emptyset$ entonces $\varphi'_2 \circ \varphi'^{-1}_1 : U'_1 \cap U'_2 \to U'_1 \cap U'_2$ sea holomorfa.

En primer lugar, como se mencionó en la Sección 4.3 cabe destacar que la complejidad viene dada por los puntos $\Pi(\tau)$ elípticos, es decir, puntos para los cuales existe una transformación no trivial de Γ que los fija. Observamos que si $\Pi(\tau)$ no es un punto elíptico, por la Proposición 4.13 aplicada a τ, existen U_1, U_2 entornos de τ tal que para todo $\gamma \in SL_2(\mathbb{Z})$

$$\text{Si } \gamma(U_1) \cap U_2 \neq \emptyset, \text{ entonces } \gamma(\tau) = \tau.$$

Como $\Pi(\tau)$ no es elíptico dado $\gamma \in \Gamma$, con $\gamma \neq \pm I$, se tiene que $\gamma(U_1) \cap U_2 = \emptyset$. Tomando $U = U_1 \cap U_2$ tenemos que $\gamma(U) \cap U = \emptyset$, luego $\Gamma U \cap U = \emptyset$ y concluimos que $\Pi_{|_U} : U \to \Pi(U)$ es biyectiva luego podemos definir $\varphi : \Pi(U) \to U$ una carta para $\Pi(\tau)$.
Sin embargo, este razonamiento no se puede repetir para los puntos elípticos. Recordemos que $\tau \in \mathbb{H}$, o $\Pi(\tau) \in Y(\Gamma)$, es elíptico si el estabilizador respecto a Γ dado por

$$\Gamma_\tau = \{\gamma \in \Gamma : \quad \gamma(\tau) = \tau\}$$

es no trivial.
Por el Corolario 4.22, sabemos que aunque este subgrupo puede no ser trivial se trata siempre de un grupo cíclico finito, lo que nos permite trabajar con puntos elípticos. Empleando el estabilizador de $\tau \in \mathbb{H}$ respecto a Γ, podemos asociar a cada punto un entero positivo que mide en cierta forma la dificultad para construir las cartas de $\Pi(\tau)$.

Definición 5.1. *Dado Γ un subgrupo de congruencias, para cada $\tau \in \mathbb{H}$ se define su periodo h_τ como*

$$h_\tau = |\{\pm I\}\Gamma_\tau / \{\pm I\}|,$$

el cual es $|\Gamma_\tau|/2$ si $-I \in \Gamma$ o $|\Gamma_\tau|$ si $-I \notin \Gamma$.

Observamos que tanto I como $-I$ actúan trivialmente sobre $\mathbb{H}$. Sin embargo, puede ser que para un subgrupo $\Gamma \subseteq SL_2(\mathbb{Z})$ no se cumpla que $-I \in \Gamma$. Considerando $\{\pm I\}\Gamma_\tau / \{\pm I\}$ nos aseguramos que estamos contando

el periodo de manera homogénea para todos los grupos independientemente de si $-I$ está o no en Γ.
La siguiente proposición nos muestra que el periodo es estable por conjugación.

Proposición 5.2. *sean $\tau \in \mathbb{H}$ y $\gamma \in SL_2(\mathbb{Z})$. Entonces el periodo de $\gamma(\tau)$ respecto al subgrupo de congruencias $\gamma\Gamma\gamma^{-1}$ es el mismo que el periodo de τ respecto al subgrupo de congruencias Γ.*

Demostración. Para demostrar esta proposición hay que probar que para cualquier $\beta \in \Gamma$ tal que $\beta(\tau) = \tau$, entonces $\gamma\beta\gamma^{-1}$ fija a $\gamma(\tau)$, lo cual se hace de forma directa aplicando la composición de aplicaciones. Por otra parte, hay que probar que si $-I \notin \Gamma$ entonces $-I \notin \gamma\Gamma\gamma^{-1}$, lo cual se cumple ya que $-I = \gamma - I\gamma^{-1}$. □

En particular, h_τ depende solo de Γ, haciendo que el periodo esté bien definido en $Y(\Gamma)$. Si Γ es un subgrupo normal de $SL_2(\mathbb{Z})$, entonces el periodo de τ sobre Γ es el mismo que el periodo de $\gamma(\tau)$ sobre Γ, es decir, si Γ es normal el periodo es el mismo para todos los puntos de $SL_2(\mathbb{Z})\tau$.
Antes de poder dar cartas a los puntos elípticos de una curva modular, necesitaremos el siguiente corolario.

Corolario 5.3. *Sea Γ un subgrupo de congruencias de $SL_2(\mathbb{Z})$. Para cada $\tau \in \mathbb{H}$ existe un entorno U contenido en $\mathbb{H}$ tal que para todo $\gamma \in \Gamma$ se cumple que*

$$\text{si } \gamma(U) \cap U \neq \emptyset, \text{ entonces } \gamma \in \Gamma_\tau.$$

Demostración. Este corolario es una consecuencia directa de la Proposición 4.13. Tomando $\tau_1 = \tau$, $\tau_2 = \tau$, obtenemos U_1, U_2 entornos de τ y basta tomar $U = U_1 \cap U_2$. □

Ahora nos disponemos a construir una aplicación que cumpla las propiedades necesarias para poder considerar cartas en los puntos elípticos, para ello para cada punto elíptico consideraremos la siguiente matriz.

Definición 5.4. *Sea $\tau \in \mathbb{H}$. Consideraremos la matriz*

$$\delta_\tau = \begin{pmatrix} 1 & -\tau \\ 1 & -\bar{\tau} \end{pmatrix} \in GL_2(\mathbb{C}).$$

Observando la correspondiente transformación $\delta_\tau = (z-\tau))/(z-\bar{\tau})$ tenemos que $\delta_\tau(\tau) = 0$ y $\delta_\tau(\bar{\tau}) = \infty$.

Gracias a esta matriz podemos deducir una serie de propiedades sobre los puntos elípticos.

Proposición 5.5. *El estabilizador del 0 en el grupo de transformaciones conjugado $\left(\delta_\tau \{\pm I\} \Gamma \delta_\tau^{-1}\right)_0 / \{\pm I\}$, es el conjugado del estabilizador de τ, es decir, $\delta_\tau \left(\{\pm I\}\Gamma_\tau / \{\pm I\}\right) \delta_\tau^{-1}$.*

Demostración. Basta observar que dado $\gamma \in \Gamma$ se tiene que $\gamma(\tau) = \tau$ si y solo si $\delta_\tau \gamma \delta_\tau^{-1}(0) = 0$ y que $-I \in \Gamma_\tau$ si y solo si $-I \in \left(\delta_\tau \Gamma \delta_\tau^{-1}\right)_0$. □

Gracias a este resultado y al Corolario 4.22 sabemos que el estabilizador del 0 en $\delta_\tau\Gamma\delta_\tau^{-1}$ es un grupo cíclico de orden h_τ. Recordamos que $\gamma \in SL_2(\mathbb{Z})$ fija a τ si y solo si fija a $\bar{\tau}$ es decir $\Gamma_\tau = \Gamma_{\bar{\tau}}$. Por tanto, dada $\lambda \in \left(\delta_\tau \Gamma \delta_\tau^{-1}\right)_0 / \{\pm I\}$ tenemos que $\lambda = \delta_\tau \gamma \delta_\tau^{-1}$ con $\gamma \in \Gamma_\tau$ luego

$$\lambda(\infty) = \delta_\tau \gamma(\delta_\tau^{-1}(\infty)) = \delta_\tau(\gamma(\bar{\tau})) = \delta_\tau(\bar{\tau}) = \infty.$$

En consecuencia, los elementos de $\left(\delta_\tau \Gamma \delta_\tau^{-1}\right)_0 / \{\pm I\}$ fijan a 0 y a ∞. Este hecho nos permite probar que la aplicación δ_τ separa los puntos $\Gamma-$equivalentes.

Proposición 5.6. *Sean $\tau \in \mathbb{H}$, U un entorno de τ y $\delta_\tau : U \to \mathbb{C}$. Entonces dados $\tau_1, \tau_2 \in U$ con $\tau_1 \neq \tau_2$ se cumple que existe $\gamma \in SL_2(\mathbb{Z})$ con $\gamma(\tau_1) = \tau_2$ si y solo si $\delta_\tau(\tau_1) = e^{(2\pi i m)/h_\tau}\delta_\tau(\tau_2)$ con $m \in \{1,\ 2,\ \ldots,\ h_\tau - 1\}$.*

Demostración. Como los elementos de $\left(\delta_\tau \Gamma \delta_\tau^{-1}\right)_0 / \{\pm I\}$ son transformaciones fraccionales lineales que fijan a 0 y a ∞ luego necesariamente son de la forma $\lambda(z) = az$. Como además sabemos que es un grupo cíclico finito de orden h_τ necesariamente es el grupo generado por $\lambda_{h_\tau}(z) = e^{(2\pi/h_\tau)i}z$.
Por otra parte, sabemos que $\gamma(\tau_1) = \tau_2$, por el Corolario 5.3, $\gamma \in \Gamma_\tau$. Componiendo con δ_τ y δ_τ^{-1}, obtenemos que $\delta_\tau\gamma\delta_\tau^{-1}(\delta_\tau(\tau_1)) = \delta_\tau(\tau_2)$, y observando que $\delta_\tau\gamma\delta_\tau^{-1}$ pertenece al estabilizador del 0, obtenemos que $\delta_\tau(\tau_1)$ es igual a una rotación de $(2\pi m)/h_\tau$ de $\delta_\tau(\tau_2)$. Finalmente como $\gamma \neq \pm I$ podemos asegurar que $m \in \{1,\ 2,\ ...,\ h_\tau - 1\}$. Recíprocamente, si $\delta_\tau(\tau_1) = e^{2\pi i m/h_\tau}\delta_\tau(\tau_2) = \lambda_{2\pi i m/h_\tau}(\delta_\tau(\tau_2))$, luego, por la Proposición 5.5, existe $\gamma \in \Gamma_\tau$ tal que $\lambda_{2\pi i m/h_\tau} = \delta_\tau\gamma\delta_\tau^{-1}$. En consecuencia $\delta_\tau(\tau_1) = \delta_\tau\gamma(\tau_2)$, es decir, $\gamma(\tau_2) = \tau_1$. □

De una forma más coloquial, podemos decir que δ_τ lleva entornos de τ a entornos de 0, en los cuales sabemos dónde están los puntos equivalentes. Por tanto, podemos identificar esos sectores circulares y crear una aplicación que asocie los entornos de $\Pi(\tau)$ en $Y(\Gamma)$ un sector circular, en el cual no habrá puntos equivalentes. Para escribir esto de manera precisa, necesitamos definir una serie de aplicaciones.

Definición 5.7. *Sean $\tau \in \mathbb{H}$, $\rho : \mathbb{C} \to \mathbb{C}$ la aplicación dada por $\rho(z) = z^h$ con $h = h_\tau$, $\delta = \delta_\tau$ y U un entorno de τ, Definimos*

$$\Psi = \Psi_\tau : U \to \mathbb{C}\,, \quad \tau' \mapsto \rho(\delta(\tau')).$$

Considerando $V = \Psi(U)$, observamos que es un entorno abierto en $\mathbb{C}$ ya que Ψ es una aplicación abierta por ser composición de aplicaciones abiertas.

Por otra parte, se puede observar que Ψ es continua, dado que tanto δ como ρ son aplicaciones continuas. Para comprobar que a través de Ψ podemos construir una carta para un entorno de $\Pi(\tau)$, primero veremos que Π y Ψ identifican los mismos puntos, para ello enunciamos la siguiente proposición.

Proposición 5.8. *Sean U un entorno de τ, τ_1 y τ_2 son dos puntos distintos de U. Entonces $\Pi(\tau_1) = \Pi(\tau_2)$ si y solo si $\Psi(\tau_1) = \Psi(\tau_2)$.*

Demostración. Observamos que $\Pi(\tau_1) = \Pi(\tau_2)$ si y solo si existe $\gamma \in \Gamma$ tal que $\gamma(\tau_2) = \tau_1$. Gracias a la Proposición 5.6, sabemos que entonces $\delta(\tau_1) = e^{(2\pi i m)/h}\delta(\tau_2)$. Por ende, significa que $\Psi(\tau_1) = (\delta(\tau_1))^h$ es igual a $(e^{(2\pi i m)/h}\delta(\tau_2))^h$ y por tanto igual a $(\delta(\tau_2))^h$, por lo que podemos concluir que $\Psi(\tau_1) = \Psi(\tau_2)$. El recíproco se prueba de forma análoga. □

Estamos en disposición de construir la aplicación de la carta.

Proposición 5.9. *Sean τ un punto de $\mathbb{H}$, U un entorno de τ sin puntos elípticos excepto τ, Ψ_τ de la Definición 5.7 y $V = \Psi(U)$. Definimos $\varphi : \Pi(U) \to V$ por $\varphi((\Pi(\tau')) = \Psi(\tau')$. Entonces la aplicación φ es un homeomorfismo.*

Demostración. Gracias la Proposición 5.8, observamos dos cosas, la primera que esta bien definida la aplicación, por otra parte que la aplicación es inyectiva, al ser una equivalencia. Esta aplicación es sobreyectiva por construcción, por ende podemos concluir que es una aplicación biyectiva.
Veamos que φ es continua, tomamos $V' \subseteq V$ abierto, entonces $\varphi^{-1}(V') = \Pi(\Psi^{-1}(V'))$ que es un abierto por que Ψ es continua y Π es abierta. Análogamente φ^{-1} es continua porque Π es continua y Ψ es abierta. Por tanto, tenemos que φ es un homeomorfismo. □

Sabiendo que es un homeomorfismo, lo último que nos falta por comprobar es que los cambios de cartas son holomorfos.

Proposición 5.10. *Sean $\varphi_1 : \Pi(U_1) \to V_1$ y $\varphi_2 : \Pi(U_2) \to V_2$, definidas en la Proposición 5.9. Entonces $\varphi_2 \circ \varphi_1^{-1} : \varphi_1(\Pi(U_1) \cap \Pi(U_2)) \to \varphi_2(\Pi(U_1) \cap \Pi(U_2))$ es una aplicación holomorfa.*

Demostración. Para empezar consideramos $x \in \Pi(U_1) \cap \Pi(U_2)$, entonces $x = \Pi(\tau_1) = \Pi(\tau_2)$ con $\tau_1 \in U_1$ y $\tau_2 \in U_2$ de tal manera que $\tau_2 = \gamma(\tau_1)$ con $\gamma \in \Gamma$. Consideramos $U_{1,2} = U_1 \cap \gamma^{-1}(U_2)$. Entonces $\Pi(U_{1,2})$ es un entorno de x en $\Pi(U_1) \cap \Pi(U_2)$ ya que $\Pi(U_{1,2}) \subseteq \Pi(U_1)$ y $\Pi(U_{1,2}) \subseteq \Pi(\gamma^{-1}(U_2))$ y como $\gamma^{-1} \in \Gamma$, entonces $\Pi(\gamma^{-1}(U_2)) = \Pi(U_2)$. Por tanto, consideramos $V_{1,2} = \varphi_1(\Pi(U_{1,2}))$ que es un entorno de $\varphi_1(x)$ en V_1. Trataremos de probar la holomorfia de $\varphi_2 \circ \varphi_1^{-1}$ en $V_{1,2}$. Dividiremos la demostración en tres casos, los cuales el primero y el segundo son simétricos.

Caso A: $\varphi_1(x) = 0$. Por tanto, si $x = \Pi(\tau_1)$, como $\varphi_1(x) = 0$, la aplicación δ_1 en la definición de φ_1 resulta ser $\delta_1 = \delta_{\tau_1}$. Por ende, un punto de $V_{1,2}$ será de la forma $q = \varphi_1(x') = \Psi_1(\tau') = (\delta_1(\tau'))^{h_1}$ para algún $\tau' \in U_{1,2}$, donde h_1 es el periodo de τ_1.

Denotamos por $\tilde{\tau_2} \in U_2$ el elemento tal que $\delta_2 = \delta_{\tilde{\tau_2}}$, es decir, $\Psi_2(\tilde{\tau_2}) = 0$ y denotamos por h_2 su correspondiente periodo. Como $x' = \Pi(\tau')$ con $\tau' \in U_{1,2}$, tenemos que $\gamma(\tau') \in U_2$ y podemos escribir

$$\varphi_2(x') = \varphi_2(\Pi(\gamma(\tau')) = \Psi_2(\gamma(\tau')) = (\delta_2(\gamma(\tau')))^{h_2} = (\delta_2\gamma\delta_1^{-1}(\delta_1(\tau')))^{h_2} = (\delta_2\gamma\delta_1^{-1}(q^{1/h_1}))^{h_2}.$$

El único caso donde el cambio de cartas podría no ser holomorfo es si $h_1 > 1$, es decir, si τ_1 es elíptico dado que la aplicación que lleva z a $z^{1/h}$ no tiene porque ser holomorfa.

Por otro lado, recordamos que U_2 solo tiene un punto elíptico, por construcción. Como τ_1 es elíptico entonces $\gamma(\tau_1) = \tau_2$ también es elíptico en U_2 ya que para cualquier $\beta \in \Gamma_{\tau_1}$, como $\gamma \in \Gamma$ entonces $\gamma\Gamma\gamma^{-1} = \Gamma$ entonces $\gamma\beta\gamma^{-1} \in \Gamma_{\tau_2}$ y con el mismo periodo que τ_1, por la Proposición 5.2. Por ende, $\tilde{\tau_2} = \tau_2$ y $h_1 = h_2 = h$. Además podemos deducir que $\delta_2\gamma\delta_1^{-1}$ es una aplicación que deja fijo al punto 0 y a ∞ por tanto

$$\delta_2\gamma\delta_1^{-1} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},$$

con a y $b \in \mathbb{C} \setminus \{0\}$. Por tanto, se tiene que

$$(\delta_2\gamma\delta_1^{-1}(q^{1/h_1}))^{h_2} = \left(\frac{a}{b}\right)^h q,$$

que es una aplicación holomorfa.

Caso B: $\varphi_2(x) = 0$. Basta con considerar la aplicación inversa a la definida anteriormente, la cual es holomorfa dado que la aplicación inversa de una aplicación biyectiva holomorfa también es holomorfa.

Caso C: $\varphi_1(x) \neq 0$ y $\varphi_2(x) \neq 0$. En este caso, construimos la correspondiente carta $\varphi_3 : \Pi(U_3) \to V_3$ tal que $\varphi_3(x) = 0$. Resulta razonando como en los casos anteriores $\varphi_3 \circ \varphi_1^{-1}$ y $\varphi_2 \circ \varphi_3^{-1}$ son holomorfas y como $\varphi_2 \circ \varphi_1^{-1} = \varphi_2 \circ \varphi_3^{-1} \circ \varphi_3 \circ \varphi_1^{-1}$ concluimos que el correspondiente cambio de cartas también es holomorfo.

□

5.2. Compactificación de $Y(\Gamma)$ mediante cúspides

En la Sección 4.3 vimos que la curva modular $Y(1)$ tenía como dominio fundamental el conjunto $D = \{\tau \in \mathbb{H} : |Re(\tau)| \leq 1/2,\ |\tau| \geq 1\}$ que no es compacto. Sin embargo, empleando la proyección estereográfica podemos situar D sobre la esfera de Riemann obteniendo un triangulo sin el vértice superior. Podemos compactificar dicho triangulo añadiendo el punto en el infinito. El hecho de que podamos compactificar $Y(1)$ con un solo punto está relacionado con que $(\mathbb{Q} \cup \{\infty\})/SL_2(\mathbb{Z})$ tiene una única clase de equivalencia.

En general, dado un subgrupo de congruencias Γ de $SL_2(\mathbb{Z})$, recordamos que cada una de las clases de equivalencia de $\mathbb{Q} \cup \{\infty\}$ por la acción de Γ se denomina cúspide, ver Definición 2.30. El objetivo de esta sección es mostrar que podemos añadir las cúspides a $Y(\Gamma)$ construyendo las correspondientes cartas de manera que obtengamos una superficie de Riemann compacta que denotamos por $X(\Gamma)$. Emplearemos algunas de las propiedades de la acción de $SL_2(\mathbb{Z})$ sobre $\mathbb{Q} \cup \{\infty\}$. Recordamos que por el Lema 2.31 $SL_2(\mathbb{Z})$ actúa de manera transitiva sobre $\mathbb{Q} \cup \{\infty\}$. Desde un punto de vista geométrico, si $\gamma \in SL_2(\mathbb{Z})$ lleva ∞ a $s \in \mathbb{Q}$ entonces transforma el dominio fundamental D en una región que se estrecha hacia la cúspide s, al igual que la contraimagen de la proyección estereográfica de D se estrecha hacia la cúspide ∞ en la esfera de Riemann.

Proposición 5.11. *El estabilizador de ∞ respecto a $SL_2(\mathbb{Z})$ es*

$$SL_2(\mathbb{Z})_\infty = \left\{ \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} : m \in \mathbb{Z} \right\}.$$

Demostración. Basta tener en cuenta que las matrices que dejan fijo al infinito son aquellas en las que $c = 0$. □

Una vez visto como actúa $SL_2(\mathbb{Z})$ respecto al ∞, podemos añadir las cúspides a $Y(\Gamma)$ considerando la acción de Γ sobre el conjunto unión de $\mathbb{H}$ y $\mathbb{Q} \cup \{\infty\}$.

Definición 5.12. *Sea $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ y $\Gamma \subseteq SL_2(\mathbb{Z})$ un subgrupo de congruencias. Definimos la curva modular extendida por*

$$X(\Gamma) = \mathbb{H}^*/\Gamma = Y(\Gamma) \cup ((\mathbb{Q} \cup \{\infty\})/\Gamma).$$

Por simplicidad, llamaremos $X(\Gamma)$ curva modular y a los puntos $\Gamma s \in (\mathbb{Q} \cup \{\infty\})/\Gamma$ cúspides de $X(\Gamma)$.

Definición 5.13. *Sea $s \in \mathbb{Q} \cup \{\infty\}$ una cúspide de $X(\Gamma)$ llamamos γ_s a $\gamma \in SL_2(\mathbb{Z})$ tal que $\gamma(\infty) = s$.*

Lema 5.14. *La curva modular $X(1) = \mathbb{H}^*/SL_2(\mathbb{Z})$ tiene una única cúspide. En general. para cualquier subgrupo de congruencias Γ de $SL_2(\mathbb{Z})$, la curva modular $X(\Gamma)$ tiene un conjunto finito de cúspides.*

Demostración. La primera parte del lema es una consecuencia del Lema 2.31, ya que implica que ∞ es $SL_2(\mathbb{Z})-$equivalente a cualquier $s \in \mathbb{Q}$. Por tanto $SL_2(\mathbb{Z})\infty = SL_2(\mathbb{Z})s$, lo cual nos dice que solo existe una única cúspide. Para la segunda parte, basta con conocer el número de clases de $(\mathbb{Q} \cup \{\infty\})/\Gamma$. Si dos elementos $\Gamma\gamma = \Gamma\gamma'$ son de la misma clase lateral de $SL_2(\mathbb{Z})$ módulo Γ tenemos que

$$s = \gamma(\infty) = \beta(\gamma'(\infty)) = \beta(s').$$

Luego los puntos s y s' están en la misma cúspide. Por tanto, el número de cúspides es a lo sumo el número de clases de equivalencia de $SL_2(\mathbb{Z})$ módulo Γ como probamos en la Proposición 2.25 este número es finito. □

El siguiente paso, para poder construir nuestras coordenadas locales en las cúspides, es dotar a $\mathbb{H}^*$ de una topología. Podríamos tratar de considerar la topología que resulta de intersecar $\mathbb{H}^*$, incluyendo los discos de forma $\{z : |z| > r\} \cup \{\infty\}$. Sin embargo, con esta topología $X(\Gamma)$ no es Hausdorff porque cada entorno de Γs contiene una cantidad infinita de puntos de $\mathbb{Q} \cup \{\infty\}$. En consecuencia, necesitamos definir los entornos de un modo más laborioso.

Definición 5.15. *Sea $M > 0$. Definimos N_M como*

$$N_M = \{\tau \in \mathbb{H} : Im(\tau) > M\}.$$

Ahora podemos definir la topología en $\mathbb{H}^*$ como la construida a partir de los conjuntos abiertos de $\mathbb{H}$, añadiéndole para todo $M > 0$ y todo $\gamma \in SL_2(\mathbb{Z})$ los conjuntos $\gamma(N_M \cup \{\infty\})$ que actúan como una base de entornos de las cúspides. Cabe destacar que dado $s \in \mathbb{Q}$ si tomamos $\gamma \in SL_2(\mathbb{Z})$ tal que $\gamma(\infty) = s$, entonces γ transforma $N_M \cup \{\infty\}$ en un disco tangente al eje real en el punto s.
Veamos qué propiedades tiene la topología que acabamos de definir sobre $\mathbb{H}^*$.

Proposición 5.16. *La curva modular $X(\Gamma)$ con la topología construida anteriormente, es un espacio topológico Hausdorff,conexo y compacto.*

Demostración. Primero vamos a demostrar que cumple la condición para ser Hausdorff. Esta demostración la dividiremos en tres casos dependiendo de donde esten situados los puntos.

1. Si $x_1 = \Gamma\tau_1$ y $x_2 = \Gamma\tau_2$ con $\tau_1, \tau_2 \in \mathbb{H}$, está demostrado en el Corolario 4.14.

2. Si $x_1 = \Gamma s_1$ y $x_2 = \Gamma\tau_2$ con $s_1 \in \mathbb{Q} \cup \{\infty\}$ y $\tau_2 \in \mathbb{H}$, entonces $s_1 = \gamma_{s_1}(\infty)$ con $\gamma_{s_1} \in SL_2(\mathbb{Z})$. Sea U_2 un entorno de τ_2 tal que $K = \overline{U_2}$ es compacta y $K \subseteq \mathbb{H}$. Entonces por la Proposición 2.3 existe un M suficientemente grande tal que $SL_2(\mathbb{Z})K \cap N_M = \emptyset$. Eligiendo $U_1 = \gamma_{s_1}(N_M \cup \{\infty\})$, entonces $\Pi(U_1) \cap \Pi(U_2) = \emptyset$. Por tanto, se cumple la propiedad para ser Hausdorff.

3. Por último, si $x_1 = \Gamma s_1$ y $x_2 = \Gamma s_2$ con $s_1, s_2 \in \mathbb{Q} \cup \{\infty\}$, $x_1 \neq x_2$, entonces $s_1 = \gamma_{s_1}(\infty)$ y $s_2 = \gamma_{s_2}(\infty)$ con $\gamma_{s_2} \in SL_2(\mathbb{Z})$. Consideramos $U_1 = \gamma_{s_1}(N_2 \cup \{\infty\})$ y $U_2 = \gamma_{s_2}(N_2 \cup \{\infty\})$. Veamos que se puede concluir por reducción al absurdo que $\Pi(U_1) \cap \Pi(U_2) = \emptyset$. En caso contrario, existiría $\gamma \in \Gamma$ tal que $\gamma(\gamma_{s_1}(\tau_1)) = \gamma_{s_2}(\tau_2)$ con $\tau_1, \tau_2 \in N_2$. Por lo tanto, tenemos que

$$\gamma_{s_2}^{-1} \cdot \gamma \cdot \gamma_{s_1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

lleva τ_1 a τ_2, razonando como en la demostración del Lema 4.17, suponiendo que $\mathrm{Im}(\tau_2) \geq \mathrm{Im}(\tau_1)$ tenemos que

$$|c|^2 \leq |c|\mathrm{Im}(\tau_1) = |\mathrm{Im}(c\tau_1 + d)| \leq |c\tau_1 + d| \leq 1$$

luego $c = 0$. Por tanto, existe $m \in \mathbb{Z}$ tal que

$$\gamma_{s_2}^{-1} \cdot \gamma \cdot \gamma_{s_1} = \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix},$$

por la Proposición 5.11, $\gamma_{s_2}^{-1}\gamma\gamma_{s_1}$ deja fijo a ∞. En consecuencia, se cumple que $\gamma(s_1) = \gamma(\gamma_{s_1}(\infty)) = \gamma_{s_2}(\infty) = s_2$, contradiciendo que $s_1 \neq s_2$.

Por tanto, se puede deducir que $X(\Gamma)$ es un espacio topológico Hausdorff.
Veamos que $X(\Gamma)$ es conexo. Suponemos que existen O_1, O_2 abiertos no vacíos tal que $\mathbb{H}^* = O_1 \cup O_2$ y $O_1 \cap O_2 = \emptyset$. Por tanto como $\mathbb{H}$ es conexo, $\mathbb{H} \subseteq O_1$ ó $\mathbb{H} \subseteq O_2$. Supongamos sin perdida de generalidad que $\mathbb{H} \subseteq O_1$, entonces $O_2 \subseteq \mathbb{Q} \cup \{\infty\}$ pero esto contradice la hipótesis de que O_2 es un abierto no vacío. Por tanto $\mathbb{H}^*$ es conexo y por ende $X(\Gamma)$ también ya que es la imagen de $\mathbb{H}^*$ por la aplicación continua de paso al cociente.
Por último, veamos que $X(\Gamma)$ es compacto. Para ello, veamos que

$$D^* = D \cup \{\infty\} = \{\tau \in \mathbb{H} : |Re(\tau)| \leq 1/2,\ |\tau| \geq 1\} \cup \{\infty\}$$

es compacto en $\mathbb{H}^*$. Dado un recubrimiento $D^* \subseteq \cup_{i \in J} U_i$ con U_i abiertos de $\mathbb{H}^*$, tenemos que existe $j \in J$ tal que $\infty \in U_j$. Por tanto, existe $M \in \mathbb{N}_{\geq 2}$ tal que $N_M \cup \{\infty\} \subseteq U_j$. Como $D^* \setminus N_M \subseteq \mathbb{H}$ es compacto existe un subrecubrimiento $\cup_{i=1}^n U_i \cap \mathbb{H}$ que lo contiene. En consecuencia, se cumple que

$$D^* \subseteq (\cup_{i=1}^n U_i) \cup U_j.$$

Por consiguiente D^* es compacto en $\mathbb{H}^*$.
Resulta que D^* es un dominio fundamental de la acción de $SL_2(\mathbb{Z})$ sobre $\mathbb{H}^*$, luego

$$\mathbb{H}^* = SL_2(\mathbb{Z})D^* = \cup_{i=1}^d \Gamma \gamma_j(D^*)$$

porque $[SL_2(\mathbb{Z}) : \Gamma] < \infty$ por la Proposición 2.25. En consecuencia, se tiene que $X(\Gamma) = \cup_{i=1}^d \Pi(\gamma_j(D^*))$, como Π y γ_j son continuas $\Pi(\gamma_j(D^*))$ es compacto luego $X(\Gamma)$ es compacto. □

Una vez demostrado que $X(\Gamma)$ es compacta, vamos a dotarla de cartas para ver que es una superficie de Riemann. Para ello nos falta construir cartas para las cúspides de $X(\Gamma)$ que sean compatibles con las que hemos definido en la Sección 5.1 para $Y(\Gamma)$. Introducimos la noción de anchura de una cúspide.

Definición 5.17. *Sean Γ un subgrupo de congruencias, $s \in \mathbb{Q} \cup \{\infty\}$ una cúspide de $X(\Gamma)$ y $\gamma_s \in SL_2(\mathbb{Z})$ tal que $\gamma_s(\infty) = s$. Se define la anchura de s respecto a Γ como*

$$h_{s,\Gamma} = \left| SL_2(\mathbb{Z})_\infty / \left(\gamma_s^{-1} \{\pm I\} \Gamma \gamma_s \right)_\infty \right|.$$

Cabe destacar que suprimiremos el subíndice Γ cuando el contexto lo permita. La anchura de una cúspide es una noción análoga al periodo de un punto elíptico. Recordamos que el periodo de un punto elíptico representa el número de sectores que se identifican por la acción del subgrupo en un disco centrado en el punto. En la cúspide, tenemos una cantidad numerable de sectores que se identifican bajo la acción de subgrupo. Llevando la cúspide a ∞ estos sectores son bandas verticales de amplitud uno, y la anchura representa el número de bandas que son distintas bajo la acción de grupo.
Antes de pasar a construir las cartas, estableceremos una serie de propiedades importantes sobre h_s.

Proposición 5.18. *Sean Γ un subgrupo de congruencias, $s \in \mathbb{Q} \cup \{\infty\}$ una cúspide de $X(\Gamma)$ y h_s su anchura. Entonces*

a) h_s es finito.

b) $h_s = |SL_2(\mathbb{Z})_s / \{\pm I\} \Gamma_s|$.

c) $h_s = min \left\{ h \in \mathbb{N}_{\geq 1} : \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \gamma_s^{-1} \Gamma \gamma_s \right\}$.

Demostración. a) Como Γ es un subgrupo de congruencias entonces existe $N \in \mathbb{N}_{\geq 1}$ tal que $\Gamma(N) \subseteq \Gamma$. Por la Proposición 2.29, sabemos que $\Gamma(N) \subseteq \gamma_s^{-1} \Gamma \gamma_s$ por tanto podemos deducir que

$$h_{s,\Gamma} = \left| SL_2(\mathbb{Z})_\infty / \left(\gamma_s^{-1} \{\pm I\} \Gamma \gamma_s \right)_\infty \right| \leq |SL_2(\mathbb{Z})_\infty / \Gamma(N)_\infty| \leq [SL_2(\mathbb{Z}) : \Gamma(N)],$$

luego, $h_{s,\Gamma}$ es finito.

b) Para demostrar esta segunda parte, construimos isomorfismo $g : SL_2(\mathbb{Z})_\infty \to (\gamma_s SL_2(\mathbb{Z}) \gamma_s^{-1})_s$ donde $g(\gamma) = \gamma_s \gamma \gamma_s^{-1}$. Primero, vemos que esta bien definido ya que si $\gamma(\infty) = \infty$ entonces

$$\gamma_s \gamma \gamma_s^{-1}(s) = \gamma_s(\gamma(\infty)) = \gamma_s(\infty) = s.$$

Se puede comprobar de forma directa que es biyectiva.
De una manera análoga, se puede comprobar que $\Gamma_s \cong \left(\gamma_s^{-1}\Gamma\gamma_s\right)_\infty$. Por ende, concluimos que

$$SL_2(\mathbb{Z})_\infty / \left(\gamma_s^{-1}\{\pm I\}\Gamma\gamma_s\right)_\infty \cong SL_2(\mathbb{Z})_s / \{\pm I\}\Gamma_s$$

lo cual implica que $h_s = |SL_2(\mathbb{Z})_s / \{\pm I\}\Gamma_s|$.

c) Basta observar que $SL_2(\mathbb{Z})_\infty = \{\pm I\}\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$. Luego existe $h \in \mathbb{N}_{\geq 1}$ tal que

$$\{\pm I\}\left(\gamma_s^{-1}\Gamma\gamma_s\right)_\infty = \{\pm I\}\langle \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \rangle$$

y resulta que $h = h_s$.

□

En particular, la proposición anterior muestra que h_s es independiente de la transformación $\gamma_s \in SL_2(\mathbb{Z})$ elegida para la definición.

Proposición 5.19. *Sean Γ un subgrupo de congruencias, $s \in \mathbb{Q} \cup \{\infty\}$ una cúspide y $\gamma \in SL_2(\mathbb{Z})$. Entonces $h_{s,\Gamma} = h_{\gamma(s),\gamma\Gamma\gamma^{-1}}$.*

Demostración. Vamos a dividir la prueba en dos partes distintas.
Si $\gamma(s) = \infty$, entonces $\gamma = \gamma_s^{-1}$ y por la Proposición 5.18 obtenemos que

$$h_{\gamma(s),\gamma\Gamma\gamma^{-1}} = \left|SL_2(\mathbb{Z})_\infty / \{\pm I\}\left(\gamma_s^{-1}\Gamma\gamma_s\right)_\infty\right|.$$

Por tanto, por definición de $h_{s,\Gamma}$ tenemos que son iguales.
Si $\gamma(s) = q \in \mathbb{Q}$, entonces podemos construir $f : SL_2(\mathbb{Z})_s \to SL_2(\mathbb{Z})_q$ dada por $f(\beta) = \gamma\beta\gamma^{-1}$. Se puede comprobar de manera sencilla que es un isomorfismo. De forma análoga, se construye el correspondiente isomorfismo entre Γ_s y $(\gamma\Gamma\gamma^{-1})_q$ y por tanto, haciendo el cociente y viendo que son espacios isomorfos, se puede deducir que $h_{s,\Gamma} = h_{\gamma(s),\gamma\Gamma\gamma^{-1}}$. □

Por último, veamos que h_s solo depende de Γs.

Proposición 5.20. *Sean Γ un subgrupo de congruencias, $s \in \mathbb{Q} \cup \{\infty\}$ una cúspide. Entonces $h_{s,\Gamma}$ solo depende de Γs y, por tanto, está bien definida en $X(\Gamma)$.*

Demostración. Si $\Gamma s = \Gamma q$, entonces existe $\gamma \in \Gamma$ tal que $q = \gamma(s)$ y, por la Proposición 5.19 $h_{s,\Gamma} = h_{q,\gamma\Gamma\gamma^{-1}}$. Como $\gamma \in \Gamma$ y Γ es un subgrupo $\gamma\Gamma\gamma^{-1} = \Gamma$ y, por tanto, se cumple que $h_{s,\Gamma} = h_{q,\Gamma}$. □

Emplearemos estas propiedades sobre la anchura para construir las cartas para las cúspides. Para ello, empezamos definiendo una aplicación auxiliar.

Definición 5.21. *Sean Γ un subgrupo de congruencias, $s \in \mathbb{Q} \cup \{\infty\}$ una cúspide de $X(\Gamma)$, $h = h_{s,\Gamma}$ y $U = U_s = \gamma_s(N_2 \cup \{\infty\})$. Definimos $\Psi : U \to V$ como $\Psi = \phi \circ \gamma_s^{-1}$ donde $\phi : \mathbb{C} \to \mathbb{D}$ dada por $\phi(z) = e^{2\pi i z/h}$ y $V = \Psi(U)$.*

Desde el punto de vista geométrico, lo que hacemos con esta aplicación es coger un entorno de nuestra cúspide, trasladarlo a ∞ empleando γ_s^{-1} y, por medio de ϕ, identificando los puntos a distancia mh con $m \in \mathbb{Z}$. Ahora veamos que los puntos identificados por la aplicación Ψ son los mismos que los identificados por la aplicación Π.

Proposición 5.22. *Sean Γ un subgrupo de congruencias, $s \in \mathbb{Q} \cup \{\infty\}$ una cúspide de $X(\Gamma)$, $h = h_{s,\Gamma}$,$U = U_s = \gamma_s(N_2 \cup \{\infty\})$ y $\tau_1, \tau_2 \in U$. Entonces*

$$\Pi(\tau_1) = \Pi(\tau_2) \text{ si y solo si } \Psi(\tau_1) = \Psi(\tau_1).$$

Demostración. Tenemos que $\Pi(\tau_1)=\Pi(\tau_2)$ si y solo si existe $\gamma\in\Gamma$ tal que $\tau_1=\gamma(\tau_2)$. Por tanto aplicando γ_s^{-1} podemos deducir que $\gamma_s^{-1}(\tau_1)=\left(\gamma_s^{-1}\gamma\gamma_s\right)\gamma_s^{-1}(\tau_2)$. Razonando como en el apartado 3 de la demostración de la Proposición 5.16 $\gamma_s^{-1}\gamma\gamma_s$ debe ser una traslación, luego deja fijo a ∞. Por otra parte sabemos que

$$\gamma_s^{-1}\gamma\gamma_s\in\gamma_s^{-1}\Gamma\gamma_s\cap SL_2(\mathbb{Z})_\infty=\left(\gamma_s^{-1}\Gamma\gamma_s\right)_\infty.$$

Por tanto, por la Proposición 5.11 es una traslación en la dirección mh con $m\in\mathbb{Z}$ y $h\in\mathbb{N}_{\geq 1}$. Por ende, $\Pi(\tau_1)=\Pi(\tau_2)$ si y solo si $\gamma_s^{-1}(\tau_1)=\gamma_s^{-1}(\tau_2)+mh$ lo que equivale a $\Psi(\tau_1)=\Psi(\tau_2)$. □

Empleando el resultado anterior, dado U entorno de s queremos encontrar un homeomorfismo entre $\Pi(U)$ y $V=\Psi(U)$ de un modo similar a las cartas construidas en $Y(\Gamma)$.

Proposición 5.23. *Sean Γ un subgrupo de congruencias, $s\in\mathbb{Q}\cup\{\infty\}$ una cúspide, el conjunto $U=U_s=\gamma_s(N_2\cup\{\infty\})$ y $V=\Psi(U)$. Definimos $\varphi:\Pi(U)\to V$ como $\varphi(\Pi(\tau))=\Psi(\tau)$ para todo $\tau\in U$. Entonces φ es un homeomorfismo.*

Demostración. Por la Proposición 5.22, φ está bien definida y es inyectiva. La sobreyectividad es directa por construcción. Como Π y Ψ son continuas tenemos que φ y φ^{-1} son continuas, luego φ es un homeomorfismo. □

Nos falta comprobar que la aplicación transición es una aplicación holomorfa. Para probar esta afirmación necesitamos demostrar un lema previo.

Lema 5.24. *El conjunto N_2 no contiene puntos elípticos en $SL_2(\mathbb{Z})$.*

Demostración. Dado $\tau=\gamma(i)$ ó $\tau=\gamma(\mu_3)$ con $\gamma\in SL_2(\mathbb{Z})$ tenemos que, por la Proposición 2.3, la parte imaginaria $\mathrm{Im}(\tau)=\mathrm{Im}(i)/|ci+d|^2$ ó $\mathrm{Im}(\tau)=\mathrm{Im}(\mu_3)/|c\mu_3+d|^2$. Como $|ci+d|\geq 1$ y $|c\mu_3+d|\geq 1$ para todos los pares $(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\}$ y como $\mathrm{Im}(i)=1$ y $\mathrm{Im}(\mu_3)<1$, concluimos que $\mathrm{Im}(\tau)\leq 1$, luego $\tau\notin N_2$. □

Proposición 5.25. *Sea $\varphi_1:\Pi(U_1)\to V_1$ y $\varphi_2:\Pi(U_2)\to V_2$, definidas en la Proposición 5.23 o Proposición 5.9. Entonces $\varphi_2\circ\varphi_1^{-1}:\varphi_1(\Pi(U_1)\cap\Pi(U_2))\to\varphi_2(\Pi(U_1)\cap\Pi(U_2))$ es una aplicación holomorfa.*

Demostración. En esta demostración consideramos dos casos diferentes.

1. Suponemos que $U_1\subseteq\mathbb{H}$ es un entorno de $\tau_1\in\mathbb{H}$ sin puntos elípticos, excepto quizás τ_1 y el subconjunto $U_2=\gamma_{s_2}(N_2\cup\{\infty\})$ es un entorno de $s_2\in\mathbb{Q}\cup\{\infty\}$. Para cada $x\in\Pi(U_1)\cap\Pi(U_2)$ escribimos $x=\Pi(\tilde{\tau_1})=\Pi(\tau_2)$ con $\tilde{\tau_1}\in U_1$ y $\tau_2\in U_2$ luego existe $\gamma\in\Gamma$ con $\tau_2=\gamma(\tilde{\tau_1})$. Consideramos $U_{1,2}=U_1\cap\gamma^{-1}(U_2)$ que es un entorno de $\varphi_1(x)$ en $V_{1,2}=\varphi_1(\Pi(U_1)\cap\Pi(U_2))$. Tomamos $\varphi_1(x')\in V_{1,2}$ con $x'=\Pi(\tau')$ y $\tau'\in U_{1,2}$ y escribimos $q=(\delta_1(\tau'))^{h_1}$ con $\delta_1=\delta_{\tau_1}$, como en la Definición 5.4. Tenemos que

$$\varphi_2\circ\varphi_1^{-1}(\varphi_1(x'))=\varphi_2(x')=\varphi_2(\Pi(\gamma(\tau')))=\Psi_2(\gamma(\tau'))=e^{2\pi i\gamma_{s_2}^{-1}\gamma(\tau')/h_2}=e^{2\pi i\gamma_{s_2}^{-1}\gamma\delta_1^{-1}(q^{1/h_1})/h_2}$$

que es una aplicación holomorfa excepto si $h_1>1$ y, además, $0\in\varphi_1(\Pi(U_{1,2}))$.

Sin embargo, si $h_1>1$, es decir, si τ_1 es un punto elíptico, entonces podemos probar que $\tau_1\notin U_{1,2}$. En caso contrario, tendríamos que $\gamma_{s_2}^{-1}(\gamma(\tau_1))\in N_2$ lo que es imposible porque N_2 no contiene puntos elípticos por el Lema 5.24. Por tanto, si $h_1>0$ entonces $0\notin\varphi_1(\Pi(U_{1,2}))$ y $\varphi_2\circ\varphi_1^{-1}$ es holomorfa.

2. Suponemos que $U_1=\gamma_1(N_2\cup\{\infty\})$ y $U_2=\gamma_2(N_2\cup\{\infty\})$ con $s_1=\gamma_1(\infty)$ y $s_2=\gamma_2(\infty)$ en $\mathbb{Q}\cup\{\infty\}$. Si $\Pi(U_1)\cap\Pi(U_2)\neq\emptyset$ entonces existe $\gamma\in\Gamma$ tal que $\gamma(\gamma_1(N_2\cup\{\infty\}))\cap\gamma_2(N_2\cup\{\infty\})\neq\emptyset$. Por tanto, se tiene que $\gamma_2^{-1}\gamma\gamma_1$ lleva un punto de $N_2\cup\{\infty\}$ en otro punto de $N_2\cup\{\infty\}$. Por ende, razonando como en la demostración de la Proposición 5.16, tenemos que $\gamma_2^{-1}\gamma\gamma_1$ es una traslación, luego deja fijo a ∞. Entonces, se tiene que
$$\gamma(s_1)=\gamma(\gamma_1(\infty))=\gamma_2(\infty)=s_2.$$
Aplicando la Proposición 5.20, tenemos que $h_1=h_2=h$. Tomamos un punto $\tau\in U_{1,2}=U_1\cap\gamma^{-1}(U_2)$ con $q=\Psi_1(\tau)=e^{2\pi i\gamma_1^{-1}(\tau)/h}$ y vemos que

$$\varphi_2\circ\varphi_1^{-1}(q)=\Psi_2(\gamma(\tau))=e^{2\pi i\gamma_2^{-1}\gamma(\tau)/h}=e^{2\pi i\gamma_2^{-1}\gamma\gamma_1(\gamma_1^{-1}(\tau))/h}=e^{2\pi i(\gamma_1^{-1}(\tau)+m)/h}=qe^{2\pi im/h}.$$

Por tanto $\varphi_2\circ\varphi_1^{-1}$ es una aplicación holomorfa.

□

En conclusión, hemos probado que podemos dotar a $X(\Gamma)$ de una estructura de superficie de Riemann compacta compatible con la dada para $Y(\Gamma)$.

5.3. Teorema de la modularidad

Los conceptos y los resultados de las secciones anteriores nos permiten presentar una versión del teorema de la modularidad comprendiendo todas las nociones que intervienen en el enunciado. Recordemos que, por lo visto en la Sección 4.1, toda curva elíptica E tiene un invariante $j(E)$ bien definido. Del mismo modo, recordamos que el subgrupo de congruencias $\Gamma_0(N) \subseteq SL_2(\mathbb{Z})$, definido en la Sección 2.3, tiene asociada la curva modular $X_0(N)$ definida en la Sección 5.2 y tanto E como $X_0(N)$ tienen estructura de superficie de Riemann. Con esta notación podemos enunciar la versión analítico-compleja del teorema.

Teorema 5.26. *Sea E una curva elíptica compleja con $j(E) \in \mathbb{Q}$. Entonces existen $N \in \mathbb{N}_{\geq 1}$ y una aplicación holomorfa y sobreyectiva entre superficies de Riemann compactas desde la curva modular $X_0(N)$ a la curva elíptica E,*

$$X_0(N) \to E.$$

A esta función se le conoce como parametrización modular de E.

En otras palabras, esta versión nos dice que todas las curvas elípticas con invariante racional provienen de las curvas modulares vía aplicaciones holomorfas, cuando consideramos ambas curvas como superficies de Riemann.

En los resultados previos hemos visto que las curvas modulares son en cierta forma el dominio natural de definición de las curvas elípticas. Sin embargo, en la versión más difundida del teorema de la modularidad aparece una conexión explícita entre formas modulares y curvas elípticas. Con intención de completar la información del trabajo presentamos otras dos versiones del teorema de la modularidad. En esta ocasión, no describiremos en detalle todos los elementos que intervienen en el enunciado y nos limitaremos a mostrar la relación que guardan entre ellos. Los pormenores y las pruebas se pueden encontrar en el libro de F. Diamond y J.Shurman [4] que hemos empleado como referencia principal de este trabajo.

En primer lugar, daremos una versión algebraico-racional del teorema. Para poder pasar de la versión analítico-compleja a este otro enfoque debemos estudiar el cuerpo de funciones meromorfas sobre una curva modular. En el caso de $X_0(N)$, se puede probar que el cuerpo de funciones meromorfas sobre esta curva es $\mathbb{C}(j, j_N)$ donde j es el invariante modular, ver la Definición 3.35 y $j_N(\tau) = j(N\tau)$ para todo $\tau \in \mathbb{H}$. Realizando el camino inverso, podemos partir del cuerpo de fracciones racionales $\mathbb{Q}(j, j_N)$ y tratar de buscar una curva algebraica cuyo cuerpo de funciones sea este cuerpo. Con las adaptaciones pertinentes, tenemos la posibilidad de construir dicha curva que denotamos por $X_0(N)_{alg}$. De esta manera, somos capaces de establecer una versión del teorema donde la curva elíptica compleja es remplazada por una curva elíptica racional, la curva modular $X_0(N)$ por su versión racional algebraica $X_0(N)_{alg}$ y la aplicación holomorfa sobreyectiva entre superficies de Riemann compactas por un morfismo de curvas algebraicas sobre $\mathbb{Q}$.

Teorema 5.27. *Sea E una curva elíptica sobre $\mathbb{Q}$. Entonces existen $N \in \mathbb{N}_{\geq 1}$ y un morfismo sobreyectivo de curvas algebraicas sobre $\mathbb{Q}$ desde la curva modular $X_0(N)_{alg}$ a la curva elíptica E,*

$$X_0(N)_{alg} \to E.$$

Aunque ambas versiones son equivalentes la prueba de A. Wiles se centró en este segundo enfoque. Además, esta versión nos permite introducir un nuevo invariante que es necesario para enunciar la tercera versión del teorema de la modularidad.

Definición 5.28. *Sea E una curva elíptica sobre $\mathbb{Q}$. El menor valor de $N \in \mathbb{N}_{\geq 1}$ que satisface el Teorema 5.27 es llamado el conductor analítico de E.*

La versión más popular del teorema de la modularidad relaciona las soluciones módulo p de la ecuación dada por una curva elíptica con los coeficientes de Fourier de una forma modular, definidos en la Sección 2.2. Precisaremos estas ideas.

Definición 5.29. *Sea E una curva elíptica sobre $\mathbb{Q}$. Asumimos que E está en forma reducida. Sean p un número primo y $\widetilde{E}$ la reducción de E módulo p. Entonces, definimos*

$$a_p(E) = p + 1 - |\widetilde{E}(\mathbf{F}_p)|.$$

Por otro lado, a partir de $X_0(N)_{alg}$ podemos construir una forma modular cuspidal f de manera que los coeficientes del desarrollo de Fourier de f coincidan con los valores correspondientes de la curva elíptica sobre los primos.

Teorema 5.30. *Sea E una curva elíptica sobre $\mathbb{Q}$ con conductor N_E. Entonces existe una forma modular $f \in S_2(\Gamma_0(N_E))$ tal que para todo primo p se tiene que*

$$a_p(f) = a_p(E).$$

Recordamos que para las sucesiones definidas en términos de una ecuación de recurrencia, como la sucesión de Fibonacci, podemos calcular la serie de potencias formal cuyos coeficientes son los términos de la sucesión. Cuando dicha serie de potencias es convergente representa una función, por lo que se denomina en todos los casos función generatriz. Por ejemplo, la sucesión de Fibonacci dada por la recurrencia $F_0 = F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$ para cada $n \in \mathbb{N}$ tiene por función generatriz $F(q) = q/1 - q - q^2$.
Por sorprendente que parezca, el teorema de la modularidad afirma que, en cierta forma, las formas modulares actúan como funciones generatrices de la sucesión $a_p(E)$. Por ejemplo, para la curva elíptica

$$E = \left\{(x,y) \in \mathbb{Q} : y^2 = x^3 - 4x^2 + 16\right\}$$

la función generatriz es la forma modular

$$f(q) = q\prod_{k=1}^{\infty}(1-q^k)^2(1-q^{11k})^2 = q(1-q)^2(1-q^{11})^2(1-q^2)^2(1-q^{22})^2(1-q^3)^2(1-q^{33})^2\ldots.$$

Cabe reseñar que este ejemplo con el que concluimos la memoria es uno de los presentados por M.Eichler y que inspiró la conjetura de Taniyama-Shimura-Weil. Los detalles pueden encontrarse en [7].

Bibliografía

[1] Apostol, T.M.; Modular functions and Dirichlet series in number theory. Graduate Texts in Mathematics, No. 41. Springer-Verlag, New York-Heidelberg, 1976

[2] Conrad,K.; Modular Forms. Connecticut Summer School in Number Theory, 2016. URL: https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016/02/CTNTmodularforms.pdf.

[3] Clarkson,C.; Riemann Surfaces. VIGRE REU, University of Chicago, 2007. URL: https://www.math.uchicago.edu/ may/VIGRE/VIGRE2007/REUPapers/INCOMING/clarkson.pdf.

[4] Diamond, F.; Shurman, J.; A first course in modular forms. Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005.

[5] Frenkel, E.; Amor y Matemáticas. Basic Books, New York, 2013.

[6] Jones, G.A.; Singerman, D.; Complex functions. An algebraic and geometric viewpoint. Cambridge University Press, Cambridge, 1987.

[7] Silverman, J.H.; Tate, J.T.; Rational points and elliptic curves. Undergrad. Text Math, Springer-Verlag. New York,1992.

[8] Taylor, R.; Modular Arithmetic: Driven by Inherent Beauty and Human Curiosity. Institute for Advance Study, 2012. URL: https://www.ias.edu/ideas/2012/taylor-modular-arithmetic.

[9] Washington, L.C.; Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997.