Pontificia Universidad Católica del Perú
Escuela de Posgrado

Formas Modulares

Tesis para optar el Grado de
Magíster en Matemáticas

Alex Junior Gomez Saltachin

Asesor

Alfredo Bernardo Poirier Schmitz

Jurado

Jaime Cuadros Valle

Rudy José Rosas Bazan

Lima - Perú

Julio 2019

FORMAS MODULARES

Alex Junior Gomez Saltachin

Tesis presentada a consideración del cuerpo docente de la Escuela de Posgrado, de la PUCP, como parte de los requisitos para obtener el grado académico de Magíster en Matemáticas.

Miembros del jurado:

Dr. Alfredo Bernardo Poirier Schmitz (asesor)

Dr Rudy Rosas Bazan (presidente)

Dr. Jaime Cuadros Valle (miembro)

Lima - Perú

Julio 2019

Resumen

En este trabajo presentamos una moderna introducción a las formas modulares cuyo contexto de desarrollo es principalmente analítico. Esto último lo aprovechamos sobremanera para evidenciar la naturaleza aritmética de las formas modulares, la cual emplearemos para demostrar completamente la conjetura de Bachet y parcialmente la conjetura de Ramanujan.

Palabras Claves: Grupo Modular. Formas Modulares. Dominio Fundamental. Conjetura de Ramanujan. Conjetura de Bachet.

… para mi mamá Irma.

Índice

Resumen . . . iii

Agradecimientos . . . vi

Introducción . . . 7

1 El Grupo modular **8**

1.1 $SL_2(\mathbb{Z})$ . . . 8

1.2 Subgrupos de congruencia . . . 11

1.3 Dominio fundamental . . . 18

2 Formas modulares I **24**

2.1 Primeras definiciones . . . 24

2.2 Series de Eisenstein . . . 30

2.3 La fórmula $k/12$ . . . 35

3 Operadores de Hecke I **46**

3.1 El enésimo operador de Hecke . . . 46

3.2 La conjetura de Ramanujan . . . 54

4 Formas modulares II **58**

4.1 Formas modulares de niveles altos . . . 58

4.2 El teorema de los cuatro cuadrados . . . 64

5 Operadores de Hecke II **75**

5.1 Operadores de Hecke de niveles altos . . . 75

5.2 Producto interno de Petersson . . . 79

Agradecimientos

Expreso mi mayor gratitud a mi asesor de tesis Dr. Alfredo Poirier cuya paciencia permitió el desarrollo de este trabajo. Además, quiero manifestar mi aprecio a los profesores de la sección Matemáticas de la PUCP de los cuales tuve el gran privilegio aprender lo que ahora es mi profesión. Finalmente, me gustaría agradecer a mi familia; aunque su colaboración directa haya sido minúscula en este proyecto de tesis, esta fue indispensable.

Introducción

El objetivo principal de este trabajo consiste en brindar una exposición moderna e introductoria a las formas modulares. Por un lado, es moderna, pues abandona completamente el lenguaje clásico de retículos sobre $\mathbb{C}$. Por otro lado, es introductoria, ya que desea presentarse como material inicial para temas más avanzados como lo son el programa de Langlands o la teoría de varidades de Shimura.

En el primer capítulo discutimos aspectos algebraicos y geométricos de $\mathrm{SL}_2(\mathbb{Z})$.

En el segundo capítulo definimos las formas modulares, las cuales presentan una estructura de $\mathbb{C}$-espacio vectorial. Por este motivo, las preguntas naturales de álgebra lineal brotan y es aquí donde determinamos las correspondientes dimensiones.

En el tercer capítulo definimos operadores lineales para los espacios vectoriales de formas modulares, conocidos como operadores de Hecke. Estos fueron usados por Mordell para probar parcialmente la conjetura de Ramanuajan, cuya prueba presentamos en este capítulo.

En el cuarto capítulo extendemos nuestra definición de formas modulares para subgrupos de congruencia, las cuales también presentan estructura de $\mathbb{C}$-espacio vectorial finito dimensional. Además, usamos un ejemplo de formas modulares para probar el teorema de la suma de los cuatro cuadrados.

El quinto capítulo es esencialmente una continuación del tercero. Acá definimos el producto de Petterson, el cual nos permite mostrar que los operadores Hecke son hermitianos. Asimismo, construimos operadores lineales para los espacios vectoriales de las formas modulares de niveles altos.

Capítulo 1

El Grupo modular

En este capítulo pondremos en relieve información sobre los principales aspectos algebraicos y geométricos del grupo modular. Gran parte de los resultados puede ser consultado en [2], [12], [15] y [19].

1.1 $\mathrm{SL}_2(\mathbb{Z})$

En el conjunto de las matrices enteras 2×2, los elementos invertibles son aquellos que tienen como determinante una unidad de $\mathbb{Z}$. En particular, aquellos elementos de determinante 1 forman un subgrupo con la multiplicación usual. Este objeto algebraico es conocido como el **grupo modular** y es denotado por $\mathrm{SL}_2(\mathbb{Z})$.

El grupo modular es en apariencia un ente tan elemental que para exhibir algún elemento es suficiente tomar dos enteros relativamente primos y usar la **identidad de Bézout**. Entre los elementos más resaltantes de $\mathrm{SL}_2(\mathbb{Z})$, aparte de la identidad, se encuentran

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{y} \quad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

El grupo modular es finitamente generado y curiosamente lo está por este par de matrices. El siguiente teorema pone en evidencia la veracidad de esta afirmación.

Teorema 1.1. *El grupo modular está generado por las matrices S y T.*

Prueba. La verificación de esta afirmación consiste en brindar a cada elemento del grupo modular un aspecto familiar respecto al grupo $\langle S, T\rangle$. En otras palabras, a cada elemento $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ de $\mathrm{SL}_2(\mathbb{Z})$ se le multiplicará de manera sucesiva otros de $\langle S, T\rangle$ hasta que el producto sea un elemento fácilmente reconocible de $\langle S,T\rangle$. Para ello consideremos dos casos: c vale 0 o no.

Si c vale 0, evidentemente se cumple $ad=1$ y con ello obtenemos $a=d=\pm1$, pues son enteros los que están discusión. En consecuencia, tenemos que γ es una matriz de la forma $\begin{bmatrix}\pm1 & b\\ 0 & \pm1\end{bmatrix}$. Por lo cual, en esta situación no es necesario multiplicarle una matriz a γ, pues tanto T^b como S^2T^{-b} son elementos de $\langle S,T\rangle$.

Si c es diferente de 0, entonces buscamos un entero n_1 tal que la matriz $\gamma T^{n_1}S$, igual a $\begin{bmatrix}an_1+b & -a\\ cn_1+d & -c\end{bmatrix}$, satisface la condición $|cn_1+d|\leq\frac{|c|}{2}$. Si cn_1+d es 0, entonces $\gamma T^{n_1}S$ es igual T^{-a} o a T^aS^2. De lo contrario, existe un entero n_2 tal que la matriz $\gamma T^{n_1}ST^{n_2}S$ es igual a $\begin{bmatrix}n_2(an_1+b)-a & -an_1-b\\ n_2(cn_1+d)-c & -cn_1-d\end{bmatrix}$ con la condición $|n_2(cn_1+d)-c|\leq\frac{|cn_1+d|}{2}\leq\frac{|c|}{2^2}$.

Claramente, si continuamos repitiendo los argumentos del párrafo anterior conseguiremos un elemento de $\langle S,T\rangle$ tal que al multiplicarlo con γ obtendremos una matriz de la forma $\begin{bmatrix}\pm1 & b'\\ 0 & \pm1\end{bmatrix}$ con $b'\in\mathbb{Z}$. De hecho, la cantidad de repeticiones necesarias es a lo más k, donde este es el menor entero positivo que satisface $|c|<2^k$. □

El teorema anterior revela que todo elemento de $\mathrm{SL}_2(\mathbb{Z})$ se identifica con alguna palabra del alfabeto $\{S,T,T^{-1}\}$. De hecho, nos describe el procedimiento a seguir para lograr este cometido.

Ejemplo 1.2. Usemos el algoritmo descrito en el teorema 1.1 para mostar cómo la matriz $A=\begin{bmatrix}3 & 1\\ 5 & 2\end{bmatrix}$ se representa como una palabra del alfabeto $\{S,T,T^{-1}\}$.

Como no estamos en el primer caso del algoritmo, el entero n_1 que buscamos para nuestra primera iteración es 0, ya que satisface $|5n_1+2|\leq\frac{5}{2}$. Por lo cual, la nueva matriz a considerar es $AS=\begin{bmatrix}1 & -3\\ 2 & -5\end{bmatrix}$.

Nuevamente no estamos en el primer caso, por lo que el entero n_2 que buscamos para la segunda iteración es 2, pues satisface $|2n_2-5|\leq\frac{2}{2}$. Así tenemos que la nueva matriz a considerar es $AST^2S=\begin{bmatrix}-1 & -1\\ -1 & -2\end{bmatrix}$.

Otra vez no estamos en el primer caso por lo que el entero n_3 que buscamos para esta tercera y última iteración es -2 debido a que satisface $|-n_3-2|\leq\frac{1}{2}$. En este caso, obtenemos $AST^2ST^{-2}S=T$. Por lo tanto, A se escribe como $TSSSTTSSST^{-1}T^{-1}SSS$.

En resumen, $\mathrm{SL}_2(\mathbb{Z})$ es un ejemplo de un grupo infinito finitamente generado no abeliano. No obstante, su estructura aún es un enigma, ya que preguntas como: ¿cuáles son sus automorfismos?, ¿cómo se comporta el grupo modular en alguno otro que lo contiene? o ¿cuáles son sus subgrupos? no se han respondido.

Con respecto a la primera pregunta, podemos afirmar que todos los automorfismos de $\mathrm{SL}_2(\mathbb{Z})$ son de la forma $\gamma \mapsto \alpha\gamma\alpha^{-1}$ o de la forma $\gamma \mapsto \epsilon(\gamma)\alpha\gamma\alpha^{-1}$, donde α es un elemento de $\mathrm{SL}_2(\mathbb{Z})$ y ϵ es una función cuya imagen está en $\{-I, I\}$. Todos los detalles de este resultado se encuentran en [10] y tienen como prerrequisito básico el teorema 1.1.

Con respecto a la segunda pregunta, si vemos a $\mathrm{SL}_2(\mathbb{Z})$, que es $\mathrm{GL}_2^+(\mathbb{Z})$, como subgrupo de $\mathrm{GL}_2(\mathbb{Z})$, existen dos únicas clases laterales, las cuales están representas por las matrices

$$I = I^{(+)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{y} \quad I^{(-)} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Esto implica que $\mathrm{SL}_2(\mathbb{Z})$ es un subgrupo normal de $\mathrm{GL}_2(\mathbb{Z})$ con índice finito y donde la identificación $\mathrm{SL}_2(\mathbb{Z})\mathrm{GL}_2(\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z})\mathrm{SL}_2(\mathbb{Z})$ es válida.

En virtud de lo mencionado en el párrafo anterior, la segunda pregunta puede ser más específica. ¿Existe alguna descomposición de $\mathrm{GL}_2^+(\mathbb{Q})$ con elementos de $\mathrm{SL}_2(\mathbb{Z})$? ¿El índice de $\mathrm{SL}_2(\mathbb{Z})$ en $\mathrm{GL}_2^+(\mathbb{Q})$ es finito? La siguiente proposición da respuesta a la primera de estas preguntas.

Proposición 1.3. *Para todo elemento de* $\mathrm{GL}_2^+(\mathbb{Q})$ *existe un múltiplo racional positivo de la matriz identidad y un elemento de* $\mathrm{SL}_2(\mathbb{Z})$ *tales que el producto de los tres es una matriz entera triangular superior.*

Prueba. No hay duda de que el enunciado asegura ser válido sin importar el orden para la multiplicación. Sin embargo, probaremos dicha afirmación para un orden específico, los casos restantes son similares.

Sea $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$. Supongamos inicialmente que α es una matriz entera. En este caso, para a y c tendríamos enteros a', c' y k tales que se cumple $a = a'k$, $c = c'k$ y $k = \mathrm{mcd}(a, c)$. Como a' y c' son primos relativos, existen enteros m y n tales que la matriz $\gamma = \begin{bmatrix} m & n \\ -c' & a' \end{bmatrix}$ es un elemento de $\mathrm{SL}_2(\mathbb{Z})$. Por lo cual, los objetos buscados en caso para α son γ y la matriz identidad, pues $\gamma\alpha$ es una matriz entera triangular superior.

Para el caso general podemos repetir los argumentos del párrafo anterior ya que existen $\alpha' \in \mathrm{M}_2(\mathbb{Z})$ y n' entero positivo para los cuales se satisface $n'\alpha = \alpha'$. □

De la proposición anterior se desprende la siguiente identificación conocida como la **descomposición de Bruhat** $\mathrm{GL}_2(\mathbb{Q}) = \mathrm{SL}_2(\mathbb{Z})B_2$ donde B_2 es el grupo formado por las matrices triangulares superiores en $\mathrm{GL}_2(\mathbb{Q})$.

Para finalizar esta sección, atendamos ahora la pregunta con respecto a la finitud del índice del grupo modular en $\mathrm{GL}_2(\mathbb{Q})$ (o bien para $\mathrm{GL}_2^+(\mathbb{Q})$). Para distintos primos p y q las matrices

$$\begin{bmatrix} p & 0 \\ 0 & p^{-1} \end{bmatrix} \quad y \quad \begin{bmatrix} q & 0 \\ 0 & q^{-1} \end{bmatrix}$$

son representantes de clases laterales distintas de $\mathrm{GL}_2(\mathbb{Q})/\mathrm{SL}_2(\mathbb{Z})$. Es decir, el índice del grupo modular en $\mathrm{GL}_2(\mathbb{Q})$ es finito.

En la siguiente sección, la discusión se centrará en los subgrupos de $\mathrm{SL}_2(\mathbb{Z})$ y en especial nos enfocaremos en aquellos de índice finito.

1.2 Subgrupos de congruencia

El estudio de los subgrupos de un grupo permite mejorar la compresión de la estructura algebraica, ya que los herederos nos mostrarán qué es lo más valioso del ancestro estudiado. Tal labor se inicia con el análisis de un puñado de sus subgrupos, en nuestra particular situación tenemos a $\langle -I\rangle, \langle S^3T\rangle, \langle S\rangle, \langle ST\rangle$ y $\langle T\rangle$, donde el primero es el centro de $\mathrm{SL}_2(\mathbb{Z})$, los primeros cuatro son subgrupos finitos de órdenes 2, 3, 4 y 6, respectivamente, y último es de orden e índice infinito.

La forma como hemos obtenido los subgrupos cíclicos, antes mencionados, ha sido apenas vía manipulaciones sucesivas de los elementos generadores de $\mathrm{SL}_2(\mathbb{Z})$. No obstante, si queremos conseguir otros subgrupos menos elementales, debemos usar alguna sofisticación de la teoría de grupos.

Para cada natural N, la proyección $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ induce un homomorfismo que va de $\mathrm{SL}_2(\mathbb{Z})$ a $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, el cual está dado por $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix}$. Cada núcleo de estos homomorfismos, a los que denotaremos por $\Gamma(N)$, es un subgrupo normal de $\mathrm{SL}_2(\mathbb{Z})$ de índice finito. A estos subgrupos del grupo modular se les conoce como **subgrupos de congruencia principal** de nivel N y cuya definición alternativa dada por

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}$$

nos permite deducir que la inclusión $\Gamma(M) \subset \Gamma(N)$ es válida si N divide a M.

A los subgrupos de $\mathrm{SL}_2(\mathbb{Z})$ que contienen algún subgrupo de congruencia principal se les conoce como **subgrupos de congruencia**. Adicionalmente, se dice que **tienen nivel** N si el subgrupo de congruencia principal más grande que yace dentro de ellos tiene nivel N. Evidentemente, todos los subgrupos de congruencia tienen índice finito y ello nos obliga a preguntarnos: ¿son todos los subgrupos de índice finito de $\mathrm{SL}_2(\mathbb{Z})$ subgrupos de congruencia? La respuesta es no y se remonta a los tiempos de Klein, cuyo contraejemplo brindado por aquel entonces lo encontramos en [16].

El siguiente teorema revela las principales cualidades de los subgrupos de congruencia y además presenta nuevos subgrupos de congruencias a los cuales se les conoce como **subgrupos de Hecke**.

Teorema 1.4. *Las siguientes propiedades se cumplen.*

a. Cualquier conjugación de un subgrupo de congruencia por un elemento de $\mathrm{SL}_2(\mathbb{Z})$ *es un subgrupo de congruencia. Más aún, el nivel no varía.*

b. La intersección de dos subgrupos de congruencia principal es un subgrupo de congruencia principal cuyo nivel es el mínimo común múltiplo de los niveles de los subgrupos intersectados.

c. El producto de dos subgrupos de congruencia principal es un subgrupo de congruencia principal cuyo nivel es máximo común divisor de los niveles de los subgrupos multiplicados.

d. Los subgrupos de $\mathrm{SL}_2(\mathbb{Z})$ *dados por*

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N} \right\},$$

$$\Gamma^1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} \pmod{N} \right\},$$

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N} \right\} \; y$$

$$\Gamma^0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & 0 \\ * & * \end{bmatrix} \pmod{N} \right\}$$

son subgrupos de congruencia (acá "$*$" significa sin especificar). Más aún, se verifican las cadenas de inclusiones

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z}) \quad y \quad \Gamma(N) \subset \Gamma^1(N) \subset \Gamma^0(N) \subset \mathrm{SL}_2(\mathbb{Z}).$$

Prueba. Los items a, b y d son fáciles de verificar, por lo cual los dejaremos como ejercicio para el lector.

Con respecto al item c, claramente se cumple

$$\Gamma(M)\Gamma(N) \subset \Gamma(\mathrm{mcd}(M,N))$$

para cualesquiera par de naturales M y N. Por lo tanto, es suficiente probar

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(M)\Gamma(N)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(\mathrm{mcd}(M,N))].$$

En efecto, por el segundo teorema de isomorfismos tenemos

$$[\Gamma(M)\Gamma(N) : \Gamma(N)] = [\Gamma(M) : \Gamma(M) \cap \Gamma(N)]$$

y al aplicar las reglas de la torre a $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(M)\Gamma(N)]$ obtenemos

$$\begin{aligned}
[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(M)\Gamma(N)] &= \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]}{[\Gamma(M)\Gamma(N) : \Gamma(N)} \\
&= \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]}{[\Gamma(M) : \Gamma(M) \cap \Gamma(N)]} \\
&= \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(M)][\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(M) \cap \Gamma(N)]}.
\end{aligned}$$

Para finalizar la prueba de este item usaremos el siguiente hecho (ver teorema 1.8): el índice de todo subgrupo de congruencia principal vale

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p \mid N} \left(1 - \frac{1}{p^2}\right).$$

Gracias a ello, conseguimos

$$\begin{aligned}
[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(M)\Gamma(N)] &= \mathrm{mcd}(M,N)^3 \prod_{p \mid \mathrm{mcd}(M,N)} \left(1 - \frac{1}{p^2}\right) \\
&= [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(\mathrm{mcd}(M,N))],
\end{aligned}$$

pues por el item b se cumple

$$\Gamma(M) \cap \Gamma(N) = \Gamma(\mathrm{mcm}(M,N)). \qquad \square$$

La finitud de los índices de los subgrupos congruencia junto con el teorema 1.1, nos asegura que los subgrupos de congruencia son finitamente generados por el lema de Schreier para subgrupos (véase el lema 4.2.1 de [18]). Más aún, este último resultado nos indica que de tener algún **subconjunto tranversal** (subconjunto formado por un único representante de cada clase lateral) de un subgrupo de congruencia en $\mathrm{SL}_2(\mathbb{Z})$, un conjunto de generadores para tal subgrupo congruencia estaría determinado de manera canónica.

Como los valores de los índices de los subgrupos de congruencia principal delimita los valores de los índices de los subgrupos de congruencia, los únicos subconjuntos transversales en $\mathrm{SL}_2(\mathbb{Z})$ a especificar serían aquellos correspondientes a los subgrupos de congruencia principal. Para esta tarea podemos implementar una búsqueda exhaustiva que terminaría si el cardinal del subconjunto tranversal en $\mathrm{SL}_2(\mathbb{Z})$ buscado es igual al índice del subgrupo de congruencia principal correspondiente. Debido a ello, es indispensable calcular es valor exacto de los índices de todos los subgrupos de congruencia principal. En lo que resta de esta sección nos enfocaremos en conseguir esto.

El siguiente teorema nos indica que el valor del índice de un subgrupo de congruencia principal de nivel N coincide con el cardinal del grupo $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Teorema 1.5. *El homomorfismo inducido* $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ *es sobreyectivo.*

Para demostrar este teorema es necesario probar el siguiente lema técnico.

Lema 1.6. *Para cualesquiera a, b y N enteros primos entre sí, existen enteros u y v para los cuales $a + uN$ y $b + vN$ son coprimos.*

Prueba. La afirmación es evidente si N es un elemento invertible de $\mathbb{Z}$. Por lo cual, es suficiente brindar detalles para $N \neq \pm 1$. En esta circunstancia en particular, se cumpliría $\mathrm{mcd}(a, N) \neq N$ o bien $\mathrm{mcd}(b, N) \neq N$, Por ello, sin pérdida de generalidad podemos asumir que se cumple $\mathrm{mcd}(a, N) \neq N$,

Al descomponer a como $a_1 a_2$ de tal manera que a_2 sea igual a $\mathrm{mcd}(a, N)$, se cumple que a_1 y N son coprimos. De este modo, existen enteros s y t para los cuales se verifica la identidad $sa_1 + tN = 1$, de donde obtenemos $b + t(1-b)N \equiv 1 \pmod{a_1}$.

Los enteros u y v buscados son entonces 0 y $t(1-b)$. En efecto, si p es un primo que divide mutuamente a a y $b + vN$, entonces se cumple $p \mid a_1$ o $p \mid a_2$. La primera de estas condiciones jamás ocurrirá, pues $b + vN$ no es divisible por factores de a_1. Tampoco tiene lugar la segunda, ya que de lo contrario a, b y N no serían coprimos pues todos serían divisible por p. De este modo, hemos verificado que $a + uN$ y $b + vN$ son coprimos. $\square$

Un comentario interesante respecto al lema 1.6 es que puede ser reformulado de manera distinta. Específicamente, el lema anterior puede ser enunciado como un problema de dinámica discreta asociado a la aplicación $f_N : \mathbb{Z} \to \mathbb{Z}$ dada por $x \mapsto x + N$ donde N es un entero. Es decir, ¿bajo qué condiciones dos órbitas distintas de f_N contienen puntos coprimos entre sí?

Prueba del teorema 1.5. Sea $\begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix}$ un elemento de $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. De este hecho se desprende la igualdad modular $ad - bc \equiv 1 \pmod{N}$, la cual confirma que a, b y N son coprimos. En concordancia, el lema 1.6 asegura la existencia de a' y b' enteros coprimos tales que se verifica $\begin{bmatrix} \overline{a'} & \overline{b'} \\ \overline{c} & \overline{d} \end{bmatrix} = \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix}$.

Para constatar que $\begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix}$ tiene una preimagen en $\mathrm{SL}_2(\mathbb{Z})$, es suficiente exhibir enteros u y v para los cuales la matriz $\begin{bmatrix} a' & b' \\ c + uN & d + vN \end{bmatrix}$ tenga determinante 1. Esto último está justificado debido a que los valores de $(a'v - b'u)N$ recorren todos los múltiplos de N, pues a' y b' son coprimos. Por lo tanto, hemos verificado que el homomorfismo inducido $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ es sobreyectivo. $\square$

Como consecuencia del teorema 1.5, calcular el índice de un subgrupo de congruencia principal de nivel N es igual a determinar el cardinal de $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Lema 1.7. *Para todo primo p y entero positivo n, se tiene*

$$\left|\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})\right| = \prod_{k=0}^{n-1} (p^n - p^k).$$

Prueba. Notemos que el cardinal de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ coincide con el número de bases ordenadas de $(\mathbb{Z}/p\mathbb{Z})^n$. Por ello, debemos calcular de cuántas maneras diferentes podemos colocar n vectores de $(\mathbb{Z}/p\mathbb{Z})^n$ de manera que la matriz generada por ellos tenga todos sus vectores columna linealmente independientes entre sí.

La primera columna tiene $p^n - 1$ opciones diferentes pues no debemos considerar el vector nulo. La segunda tiene $p^n - p$ porque debemos eliminar las p combinaciones lineales de la primera columna. La tercera tiene $p^n - p^2$ ya que en este caso debemos descartar las p^2 combinaciones lineales generados por la primera y segunda columna. Siguiendo este razonamiento, concluimos que la k-ésima columna tiene $p^n - p^k$ opciones diferentes. Por lo tanto, el número de bases ordenadas de $(\mathbb{Z}/p\mathbb{Z})^n$ es precisamente $(p^n - 1)(p^n - p)(p^n - p^2)\dots(p^n - p^{n-1})$. □

El lema anterior puede ser generalizado para cualquier cuerpo finito $\mathbb{F}_q$. Es decir, el tamaño de $\mathrm{GL}_n(\mathbb{F}_q)$ es $\prod_{k=0}^{n-1}(q^n - q^k)$.

El siguiente resultado determina el valor exacto del cardinal de $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Teorema 1.8. *Para todo subgrupo de congruencia principal se verifica*

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N}\left(1 - \frac{1}{p^2}\right).$$

Prueba. Iniciemos la prueba considerando el caso cuando N es un primo p. En vista de que $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ es un subgrupo de $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, es suficiente estimar la cantidad de elementos de determinante 1 dentro de este grupo de elementos con determinante no nulo. En otras palabras, debemos hallar el cardinal del núcleo del homormorfismo sobreyectivo $\det : \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^*$, el cual en este caso es

$$\frac{|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|}{|(\mathbb{Z}/p\mathbb{Z})^*|} = |\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})|.$$

El lema 1.7 nos indica entonces que $|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})|$ vale $p^3\left(1 - \frac{1}{p^2}\right)$.

Ahora, resolvamos el caso cuando N es igual a p^n. Para esto, usemos inducción. El caso base $n = 1$ ya fue verificado, por lo cual, supongamos que hasta cierto $n \geq 1$ se verifica $|\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})| = (p^n)^3\left(1 - \frac{1}{p^2}\right)$. Lo que resta es verificar lo análogo para $n + 1$.

La proyección natural $\mathrm{SL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ es un homomorfismo sobreyectivo, pues el teorema 1.5 nos permite levantar cualquier elemento de $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ en alguno de $\mathrm{SL}_2(\mathbb{Z})$ para luego reducirlo módulo p^{n+1}. Notemos que el núcleo de la proyección natural está conformado por las matrices de la forma

$$\begin{bmatrix} 1 + t_1 p^n & t_2 p^n \\ t_3 p^n & 1 + t_4 p^n \end{bmatrix}$$

con $0 \leq t_i \leq p - 1$. Como todas estas son de determinante 1 módulo p^{n+1}, necesariamente se cumple $t_1 + t_4 \equiv 0 \mod p$. De este modo, el núcleo tiene p^3 elementos y, por lo tanto, $|\mathrm{SL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})|$ es igual a $p^3|\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})|$, lo cual corrobora el caso $n+1$.

Finalmente, el caso general se cumple, pues del teorema fundamental de la aritmética y del teorema chino del resto deducimos

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \simeq \mathrm{SL}_2(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) \times \ldots \times \mathrm{SL}_2(\mathbb{Z}/p^{n_r}\mathbb{Z}). \qquad \square$$

Ilustremos lo conseguido en el siguiente ejemplo.

Ejemplo 1.9. Las matrices T, S^2 y $S^3T^{-4}S$ forman un subconjunto minimal de generadores de $\Gamma_0(4)$. En efecto, el teorema 1.5 nos brinda un algoritmo para determinar un subconjunto transversal de $\Gamma(4)$ en $\mathrm{SL}_2(\mathbb{Z})$ el cual tiene consigo a otro subconjunto que corresponde a un sistema de distintos representantes de $\Gamma_0(4)$ en $\mathrm{SL}_2(\mathbb{Z})$. En este caso, consideremos al subconjunto transversal de $\Gamma_0(4)$ en $\mathrm{SL}_2(\mathbb{Z})$ dado por las matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 3 \end{bmatrix} \text{ y } \begin{bmatrix} 0 & -1 \\ 1 & 4 \end{bmatrix}.$$

Al aplicar el lema de Scheier para subgrupos a este subconjunto conseguimos un subconjunto de generadores para $\Gamma_0(4)$. No obstante, en este caso el subconjunto obtenido no es minimal, pues lleva consigo muchas redundancias. Para asegurarnos de que tenemos un conjunto minimal de generadores, usamos el algoritmo presentado en el teorema 1.1, ya que este nos brindará una representación simbólica de cada una de estas matrices. Como cada una de las representaciones son palabras de $\{S, T, T^{-1}\}$ es muy fácil hacer simplificaciones. De esto modo, luego de hacer las cuentas correspondientes tenemos que las matrices

$$T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad S^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{y} \quad S^3T^{-4}S = \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}$$

forman un subconjunto minimal de generadores de $\Gamma_0(4)$.

Finalicemos esta sección determinando los índices de los subgrupos de Hecke.

Teorema 1.10. *Todo subgrupo de congruencia principal $\Gamma(N)$ es normal en $\Gamma_1(N)$ y este a su vez lo es en $\Gamma_0(N)$. Adicionalmente, los índices de estos grupos cocientes son*

$$[\Gamma_1(N) : \Gamma(N)] = N,$$

$$[\Gamma_0(N):\Gamma_1(N)] = N\prod_{p|N}\left(1-\frac{1}{p}\right).$$

Prueba. Consideremos los homomorfismos sobreyectivos

$$\begin{aligned} \Gamma_1(N) &\to (\mathbb{Z}/N\mathbb{Z},+) & \qquad \Gamma_0(N) &\to (\mathbb{Z}/N\mathbb{Z})^* \\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} &\mapsto b\,(\text{mód}\,N), & \begin{bmatrix} a & b \\ c & d \end{bmatrix} &\mapsto d\,(\text{mód}\,N). \end{aligned}$$

Notemos que el núcleo del primer homomorfismo es $\Gamma(N)$ y del segundo $\Gamma_1(N)$. Por lo tanto, $\Gamma(N)$ y $\Gamma_1(N)$ son subgrupos normales en $\Gamma_1(N)$ y $\Gamma_0(N)$ respectivamente y los índice están determinados por $|\mathbb{Z}/N\mathbb{Z}|$ y $|(\mathbb{Z}/N\mathbb{Z})^*|$. □

El siguiente corolario nos brinda los índices en $\mathrm{SL}_2(\mathbb{Z})$ de los subgrupos de Hecke.

Corolario 1.11. *Para todo entero positivo N, se verifica*

$$\begin{aligned} [\Gamma_0(N):\Gamma(N)] &= N^2\prod_{p|N}\left(1-\frac{1}{p}\right), \\ [\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(N)] &= N\prod_{p|N}\left(1+\frac{1}{p}\right) \text{ y} \\ [\mathrm{SL}_2(\mathbb{Z}):\Gamma_1(N)] &= N^2\prod_{p|N}\left(1-\frac{1}{p^2}\right). \end{aligned}$$ □

En la siguiente sección discutiremos cuestiones geométricas del grupo modular. Concretamente, discutiremos la acción de $\mathrm{SL}_2(\mathbb{Z})$ sobre $\mathbb{H}$, el semiplano superior de $\mathbb{C}$.

1.3 Dominio fundamental

En esta sección desarrollaremos los aspectos geométricos de $\mathrm{SL}_2(\mathbb{Z})$. Específicamente, brindaremos una "buena" identificación del espacio cociente determinado por la acción de $\mathrm{SL}_2(\mathbb{Z})$ sobre el semiplano superior de $\mathbb{C}$.

El **semiplano de Poincaré** (o semiplano superior de $\mathbb{C}$) es el subconjunto $\mathbb{H}$ dado por

$$\mathbb{H} = \left\{z\in\mathbb{C} : \mathrm{Im}(z) > 0\right\}.$$

Las **transformaciones de Möbius** asociadas a $\mathrm{GL}_2^+(\mathbb{R})$ son automorfimos de $\mathbb{H}$, los cuales están dadas por las aplicaciones de la forma

$$z\mapsto \frac{az+b}{cz+d},$$

donde $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ es un elemento de $\mathrm{GL}_2^+(\mathbb{R})$. Más aún, se cumple

$$\mathrm{Im}(\frac{az+b}{cz+d}) = \frac{(ad-bc)\mathrm{Im}(z)}{|cz+d|^2}$$

para todo z en $\mathbb{H}$ (ver lema 5 del capítulo 26 de [15]). Por lo tanto, se deduce que todo subgrupo de $\mathrm{GL}_2^+(\mathbb{R})$ actúa de manera continua sobre $\mathbb{H}$. Para ser precisos, la aplicación considerada es

$$(\gamma, z) \mapsto \gamma z = \frac{az+b}{cz+d},$$

donde $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ es un matriz de $\mathrm{GL}_2^+(\mathbb{R})$ y z un punto de $\mathbb{H}$. Notemos que γz es una aplicación conforme con derivada igual a

$$(\gamma z)' = \frac{d\gamma z}{dz} = \frac{ad-bc}{(cz+d)^2}.$$

La acción de $\mathrm{GL}_2^+(\mathbb{R})$ sobre $\mathbb{H}$ presenta muchas redundancias debido a que para cualquier $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$ se cumple

$$\frac{az+b}{cz+d} = \frac{\dfrac{a}{\sqrt{ad-bc}}z + \dfrac{b}{\sqrt{ad-bc}}}{\dfrac{c}{\sqrt{ad-bc}}z + \dfrac{d}{\sqrt{ad-bc}}}.$$

En consecuencia, las acciones de grupos sobre $\mathbb{H}$ que examinaremos serán las de los subgrupos de $\mathrm{SL}_2(\mathbb{R})$. Observemos que aún así existen redundancias adicionales debido a la presencia de $-I$, pues para todo $\gamma \in \mathrm{SL}_2(\mathbb{R})$, se cumple

$$(-\gamma)z = \gamma z.$$

Cada subgrupo $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ sobre $\mathbb{H}$ nos ofrece un espacio de órbitas $\Gamma\backslash\mathbb{H}$, el cual está dotado de una estructura analítica natural. Estos espacios cocientes tienen un sinfín de identificaciones en $\mathbb{H}$. El siguiente ejemplo advierte que es necesario depurar algunos subgrupos $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ con el proposito de no discutir cuestiones triviales.

Ejemplo 1.12. El espacio $\mathrm{SL}_2(\mathbb{R})\backslash\mathbb{H}$ consiste en un solo punto (o bien consta de una sola órbita), pues cualquier punto $z = x + yi \in \mathbb{H}$ puede ser descrito como

$$z = \begin{bmatrix} \sqrt{y} & x\sqrt{y}^{-1} \\ 0 & \sqrt{y}^{-1} \end{bmatrix} i.$$

En otras palabras, la acción de este grupo es transitiva.

Antes de precisar qué cualidades deben cumplir las identificaciones que buscamos de los espacio de órbitas de $\mathbb{H}$, veamos dos ejemplos de "buenas" identificaciones.

Ejemplo 1.13. Todo elemento de $\langle S\rangle\backslash\mathbb{H}$ tiene un representante en el conjunto

$$F_S = \{z \in \mathbb{H} : |z| \geq 1\}.$$

En efecto, la semicircunferencia $|z| = r$ con $r \leq 1$ en $\mathbb{H}$ es transformada vía S en la semicircunferencia $|z| = \frac{1}{r}$. En particular, la semicircunferencia $|z| = 1$ es dejada invariante por S. Adicionalmente, el conjunto F_S no contiene redundancias en su interior, pues la órbita de $z \in \mathbb{H}$ consta solo de z y Sz. Finalmente, F_S es un subconjunto cerrado de $\mathbb{H}$ y su frontera consiste de una curva suave.

Ejemplo 1.14. Todo elemento de $\langle T\rangle\backslash\mathbb{H}$ tiene un representante en el conjunto

$$F_T = \{z \in \mathbb{H} : \mathrm{Re}(z) \leq \frac{1}{2}\}.$$

En efecto, toda semirrecta vectical $\mathrm{Re}(z) = r$ en $\mathbb{H}$ con $|r| \geq \frac{1}{2}$ es transformada en una semirrecta vertical dentro de F_T vía T^n para algún conveniente entero n. En particular, la semirrecta $\mathrm{Re}(z) = -\frac{1}{2}$ se transforma en la semirrecta $\mathrm{Re}(z) = \frac{1}{2}$ vía a T. Adicionalmente, el conjunto F_T no tiene redundancias en su interior, pues los elementos de la órbita $\langle T\rangle z$ con $z \in \mathbb{H}$ comparten igual parte imaginaria y distan entre sí en por lo menos 1. Finalmente, F_T es un subconjunto cerrado de $\mathbb{H}$ y su frontera consiste en una curva suave.

Sean $w, z \in \mathbb{H}$ y $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ un subgrupo. Se dice que w y z son **Γ-equivalentes** o que **pertenecen a la misma Γ-órbita** si existe $\gamma \in \Gamma$ tal que se cumple $\gamma w = z$.

Ejemplo 1.15. Denotemos por ρ a la raíz cúbica de la unidad $e^{\frac{\pi i}{3}}$. Por un lado tenemos que ρ y ρ^2 son $\mathrm{SL}_2(\mathbb{Z})$-equivalentes, pues se cumple $S\rho = \rho^2$. Por otro lado, ρ y i no son $\mathrm{SL}_2(\mathbb{Z})$-equivalentes. Pues, de existir $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ que cumpla $\gamma i = \rho$, daría como consecuencia que $\sqrt{3}$ sea un racional, lo cual es falso.

Sean un subgrupo $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ y $F \subset \mathbb{H}$ un conjunto cerrado y conexo. Se dice que F es un **dominio fundamental** para Γ (o bien para el espacio de órbitas $\mathbb{H}/\Gamma$) si se satisfacen las siguientes condiciones:

- todo elemento de $\mathbb{H}$ es Γ-equivalente a uno F;
- ningún par de puntos interiores de F son Γ-equivalentes;
- la frontera de F es una unión finita de curvas suaves.

Como ejemplo notemos que la regiones F_S y F_T son dominios fundamentales para los subgrupos $\langle S \rangle$ y $\langle T \rangle$ respectivamente

Para hallar un dominio fundamental para $\mathrm{SL}_2(\mathbb{Z})$ necesitamos de un lema técnico.

Lema 1.16. *Dado $z \in \mathbb{H}$, el conjunto formado por los pares $(c, d) \in \mathbb{Z}^2$ diferentes a $(0, 0)$ y que satisfacen $|cz + d| \leq 1$ es no vacío y finito.*

Prueba. El conjunto es claramente no vacío, pues $(0, 1)$ satisface lo requerido. Ahora, al escribir z como $x + iy$, se nota que un par $(c, d) \in \mathbb{Z}^2$ satisface $|cz + d| \leq 1$ si y solo si se cumple $(cx + d)^2 + c^2y^2 \leq 1$. Esto implica que $c^2y^2 \leq 1$ debe satisfacerse, lo cual es equivalentemente a $|c| \leq \frac{1}{y}$. Es decir, c tiene una cantidad finita de opciones sobre $\mathbb{Z}$. Y como $|cx + d| \leq 1$ debe satisfacerse también, se obtiene $-1 - cx \leq d \leq 1 - cx$. De esta manera se puede concluir que d admite como máximo una cantidad finita de opciones sobre $\mathbb{Z}$. El conjunto en cuestión resulta entonces finito. $\square$

El siguiente teorema muestra un dominio fundamental para $\mathrm{SL}_2(\mathbb{Z})$ en $\mathbb{H}$, el cual es conocido como la **región modular**.

Teorema 1.17. *Un dominio fundamental para $\mathrm{SL}_2(\mathbb{Z})$ en $\mathbb{H}$ está dado por el dominio*

$$F_{\mathrm{SL}_2(\mathbb{Z})} = \left\{ z \in \mathbb{H} : |\mathrm{Re}(z)| \leq \frac{1}{2}, |z| \geq 1 \right\}.$$

Prueba. Primero verifiquemos que todo $z \in \mathbb{H}$ es $\mathrm{SL}_2(\mathbb{Z})$-equivalente a un punto del conjunto $F_{\mathrm{SL}_2(\mathbb{Z})}$. En virtud del lema 1.16, existe γ_0 elemento de $\mathrm{SL}_2(\mathbb{Z})$ tal que para

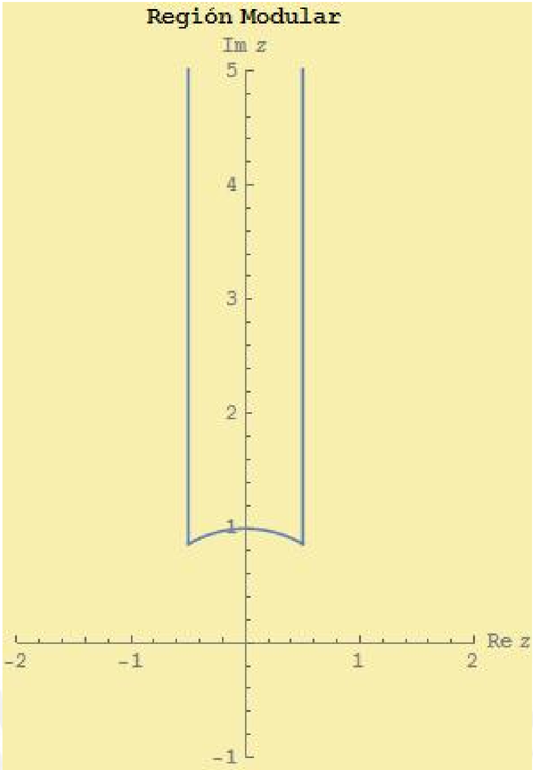

Figura 1.1: Región Modular $F_{\mathrm{SL}_2(\mathbb{Z})}$

cualquier otro γ elemento $\mathrm{SL}_2(\mathbb{Z})$, se cumple la desigualdad $\mathrm{Im}(\gamma z) \leq \mathrm{Im}(\gamma_0 z)$. Más aún, por el ejemplo 1.14, podemos asumir $\gamma_0 z$ está en F_T. Por esta razón, es suficiente confirmar que se satisface la desigualdad $|\gamma_0 z| \geq 1$. En efecto, si se supone lo contrario, se cumpliría $\mathrm{Im}(S\gamma_0 z) > \mathrm{Im}(\gamma_0 z)$, lo cual es una contradicción. Por lo tanto, hemos verificado que $\gamma_0 z$ está en $F_{\mathrm{SL}_2(\mathbb{Z})}$.

Ahora mostremos que si dos elementos de $F_{\mathrm{SL}_2(\mathbb{Z})}$ son $\mathrm{SL}_2(\mathbb{Z})$-equivalentes, uno de ellos está necesariamente en la frontera de $F_{\mathrm{SL}_2(\mathbb{Z})}$. Sean z y w elementos de $F_{\mathrm{SL}_2(\mathbb{Z})}$ tal que para algún $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ se cumple la igualdad $\gamma z = w$. Sin pérdida de generalidad, podemos asumir $\mathrm{Im}(w) \geq \mathrm{Im}(z)$. Esto último es equivalente a $|cz+d| \leq 1$, es decir, tenemos $|c|\mathrm{Im}(z) \leq 1$. Como se cumple $\mathrm{Im}(z) \geq \sqrt{3}/2$ para todo $z \in F_{\mathrm{SL}_2(\mathbb{Z})}$, obtenemos $|c| \leq 2/\sqrt{3}$. De esta forma deducimos que c vale 0 o ± 1.

Por un lado, si c es 0, entonces ad es igual a 1. De ser necesario, tras multiplicar a γ por $-I$ se logra $a = d = 1$. En este caso, γ será alguna potencia de T. De este modo, tanto z como w serían elementos de la frontera de $F_{\mathrm{SL}_2(\mathbb{Z})}$.

Por otro lado, si c es ± 1, entonces al escribir z como $x + iy$ obtenemos

$$1 \geq |cz+d|^2 = (x \pm d)^2 + y^2 \geq (x \pm d)^2 + 3/4,$$

lo cual implica $|x \pm d| \leq 1/2$. Si se verifica $|x \pm d| = 1/2$, entonces necesariamente se cumple $|x| = 1/2$. Es decir, en este caso z sería un elemento de la frontera $F_{\mathrm{SL}_2(\mathbb{Z})}$. Por el contrario, si se verifica la desigualdad estricta deducimos $d = 0$. Esto implicaría que z está en la frontera $F_{\mathrm{SL}_2(\mathbb{Z}))}$ pues su norma sería 1. Por lo tanto, no existen z y w puntos interiores de $F_{\mathrm{SL}_2(\mathbb{Z})}$ que sean $\mathrm{SL}_2(\mathbb{Z})$-equivalentes.

Finalmente, la frontera de $F_{\mathrm{SL}_2(\mathbb{Z})}$ es claramente la unión de curvas suaves. Específicamente, es la unión de dos rectas y una arco de circunferencia. Por lo tanto, $F_{\mathrm{SL}_2(\mathbb{Z})}$ es un dominio fundamental para $\mathrm{SL}_2(\mathbb{Z})$. □

En el transcurso de la demostración del teorema anterior se estableció el siguiente resultado.

Corolario 1.18. *Si z y w son elementos diferentes de $F_{\mathrm{SL}_2(\mathbb{Z})}$ que son $\mathrm{SL}_2(\mathbb{Z})$-equivalentes, entonces se cumple $\mathrm{Im}(z) = \mathrm{Im}(w)$ y $\mathrm{Re}(z) = -\mathrm{Re}(w)$.* □

Denotemos por $F'_{\mathrm{SL}_2(\mathbb{Z})}$ al conjunto que resulta de quitarle a $F_{\mathrm{SL}_2(\mathbb{Z})}$ los puntos con parte real $1/2$ y los de norma 1 con parte real positiva . Por el corolario 1.18, $F'_{\mathrm{SL}_2(\mathbb{Z})}$ es un conjunto de representantes de $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$. Es decir, la región modular es una descripción fiel del espacio de órbitas $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ siempre que se hagan las identificaciones adecuadas en la frontera de $F_{\mathrm{SL}_2(\mathbb{Z})}$.

Es aquí donde nos preguntamos si cualquier subgrupo de congruencia Γ tiene está cualidad. En otras palabras, ¿todo subgrupo de congruencia Γ tiene un dominio fundamental? La respuesta es afirmativa (véase [15]). Más aún, podemos escoger representantes convenientes de $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}\Gamma$ de tal manera que si reunimos todas las imágenes de la región modular vía estos representantes, obtenemos un dominio fundamental para Γ (véase [13]).

Capítulo 2

Formas modulares I

En este capítulo estudiaremos las formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$. Los principales materiales de consulta para este capítulo son [6] y [19].

2.1 Primeras definiciones

Sea k un entero y $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ un elemento de $\mathrm{GL}_2^+(\mathbb{R})$. El **operador k-peso** $[\gamma]_k$ para las funciones $f : \mathbb{H} \to \mathbb{C}$ está definido como

$$f[\gamma]_k(z) = \det(\gamma)^{k/2}(cz+d)^{-k} f(\gamma z),$$

donde z es un elemento de $\mathbb{H}$. Notemos que el operador $[I]_k$ es el operador identidad para las funciones $f : \mathbb{H} \to \mathbb{C}$. La siguiente proposición muestra que los operadores k-peso son compatibles con la multiplicación de matrices.

Proposición 2.1. *Para cualesquiera γ_1 y γ_2 elementos de $\mathrm{GL}_2^+(\mathbb{R})$ y función $f : \mathbb{H} \to \mathbb{C}$ se cumple la identidad*

$$f[\gamma_1\gamma_2]_k = (f[\gamma_1]_k)[\gamma_2]_k.$$

Prueba. Consideremos $\gamma_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ y $\gamma_2 = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$. Al aplicar sucesivamente la definición del operador k-peso a $f[\gamma_1]_k[\gamma_2]_k$ obtenemos

$$\begin{aligned} f[\gamma_1]_k[\gamma_2]_k(z) &= \det(\gamma_2)^{k/2}(c'z+d')^{-k} f[\gamma_1]_k(\gamma_2 z) \\ &= \det(\gamma_2)^{k/2}(c'z+d')^{-k}\det(\gamma_1)^{k/2}(c\gamma_2 z+d)^{-k} f(\gamma_1\gamma_2 z) \\ &= \det(\gamma_1)^{k/2}\det(\gamma_2)^{k/2}(c(a'z+b')+d(c'z+d'))^{-k} f(\gamma_1\gamma_2 z), \end{aligned}$$

donde lo último se cumple debido a

$$(c'z+d')(c\gamma_2 z+d) = (c'z+d')\Big(c\Big(\frac{a'z+b'}{c'z+d'}\Big)+d\Big).$$

Por tanto, al agrupar convenientemente conseguimos

$$f[\gamma_1]_k[\gamma_2]_k(z) = \det(\gamma_1\gamma_2)^{k/2}((ca'+dc')z+(cb'+dd'))^{-k}f(\gamma_1\gamma_2 z),$$

que resulta igual a $f[\gamma_1\gamma_2]_k$, pues se cumple

$$\gamma_1\gamma_2 z = \frac{(aa'+bc')z+(ab'+bd')}{(ca'+dc')z+(cb'+dd')}. \qquad \square$$

Sea k un entero y Γ un subgrupo de $\mathrm{GL}_2^+(\mathbb{R})$. Una función $f:\mathbb{H}\to\mathbb{C}$ satisface la **condición de modularidad** de peso k para Γ si para todo $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ y $z\in\mathbb{H}$ se cumple la igualdad

$$f(\gamma z) = (cz+d)^k f(z).$$

En particular, diremos que f es **invariante bajo** Γ o simplemente Γ**-invariante** si f satisface la condición de modularidad de peso 0 para Γ.

Ejemplo 2.2. Toda función $f:\mathbb{H}\to\mathbb{C}$ que satisfaga la condición de modularidad de peso k para $\mathrm{SL}_2(\mathbb{Z})$ cumple las identidades

$$f(z+n) = f(z) \quad \text{y} \quad f\Big(-\frac{1}{z}\Big) = z^k f(z)$$

para todo $z\in\mathbb{H}$ y n entero. En efecto, ambas propiedades son consecuencia directa de la definición de condición de modularidad restringida a las matrices T^n y S.

Observemos que la noción de condición de modularidad está relacionada con la de los operadores de k-peso. Específicamente, se tiene que una función $f:\mathbb{H}\to\mathbb{C}$ satisface la condición de modularidad de peso k para Γ si y solo si f es un punto fijo de todos los operadores $[\gamma]_k$, para γ elemento de Γ. A continuación mostramos la utilidad de esta observación.

Ejemplo 2.3. Sea Γ un subgrupo de congruencia y α un elemento de $\mathrm{SL}_2(\mathbb{Z})$. Si una función $f:\mathbb{H}\to\mathbb{C}$ satisface la condición de modularidad de peso k para Γ, entonces la función $f[\alpha]_k$ satisface la condición de modularidad de peso k para $\alpha^{-1}\Gamma\alpha$. En efecto, por la proposición 2.1 para todo $\gamma \in \Gamma$ tenemos

$$\begin{aligned} f[\alpha]_k[\alpha^{-1}\gamma\alpha]_k &= f[\alpha\alpha^{-1}\gamma\alpha]_k \\ &= f[\gamma\alpha]_k \\ &= f[\gamma]_k[\alpha]_k \quad (\text{pues } f[\gamma]_k = f) \\ &= f[\alpha]_k, \end{aligned}$$

lo cual por definición significa que $f[\alpha]_k$ satisface la condición de modularidad de peso k para $\alpha^{-1}\Gamma\alpha$.

En la sección 2 del capítulo anterior, mencionamos que todo subgrupo de congruencia es finitamente generado. Esto es sumamente útil al momento de verificar la condición de modularidad para una función, pues basta verificar la identidad asociada a la condición de modularidad en sus generadores. El siguiente resultado precisa la afirmación.

Proposición 2.4. *Sea Γ un subgrupo de $\mathrm{GL}_2^+(\mathbb{R})$ y $\{\gamma_1,\ldots,\gamma_n\}$ un conjunto que lo genera. Una función $f:\mathbb{H}\to\mathbb{C}$ satisface la condición de modularidad de peso k para Γ si y solo si f es un punto fijo para los operadores $[\gamma_i]_k$. En particular, f satisface la condición modularidad de peso k para $\mathrm{SL}_2(\mathbb{Z})$ si y solo si cumple*

$$f(z+n) = f(z) \quad y \quad f\Big(-\frac{1}{z}\Big) = z^k f(z),$$

para todo $z\in\mathbb{H}$. □

A consecuencia del ejemplo 2.2, se deduce que si una función $f:\mathbb{H}\to\mathbb{C}$ satisface la condición de modularidad para un subgrupo de congruencia de nivel N, entonces f tiene período N. Por lo cual, bajo ciertas condiciones la función f se exhibe como una serie de Fourier. El siguiente teorema detalla los atributos necesarios que debe cumplir la función f para obtener tal representación.

Teorema 2.5. *Sea $f:\mathbb{C}\to\mathbb{C}$ una función de periodo real h. Si f es holomorfa en la franja horizontal $D=\{z\in\mathbb{C}: -\infty < a < \mathrm{Im}(z) < b < \infty\}$, entonces f tiene una representación válida en D dada por*

$$f(z) = \sum_{n\in\mathbb{Z}} a_n q_h^n,$$

donde a_n son números complejos y q_h es $e^{\frac{2\pi iz}{h}}$. Más aún, los coeficientes de esta representación están únicamente determinados por la fórmula

$$a_n = \int_0^h f(re^{\frac{2\pi xi}{h}})r^{-n}e^{\frac{-2\pi xni}{h}}dx,$$

donde r es cualquier valor en el intervalo $(e^{\frac{-2\pi b}{h}}, e^{\frac{-2\pi a}{h}})$.

*Esta representación es conocida como la q_h-**expansión** de la función f. En adelante, convengamos que en el caso $h = 1$ escribiremos q en vez de q_1.*

Prueba. Sea A la corona abierta de $\mathbb{C}$ centrada en el origen de radio menor $e^{\frac{-2\pi b}{h}}$ y mayor $e^{\frac{-2\pi a}{h}}$. Definamos la función $\tilde{f}_h : A \to \mathbb{C}$ via $q_h \mapsto f(z)$ para $q_h \in A$. Esta función está bien definida, pues si tenemos $e^{\frac{2\pi iz_1}{h}} = e^{\frac{2\pi iz_2}{h}}$ con z_1 y z_2 en $\mathbb{C}$, entonces existe un entero k para el cual se cumple $2\pi iz_1 = 2\pi iz_2 + 2\pi ikh$. Así, la periodicidad de f asegura la buena definición de $\tilde{f}_h$.

Observemos que para cualquier $q_h \in A$ existe una rama holomorfa del logaritmo, digamos L, la cual está definida en $U \subset \mathbb{C}$, vecindad de q_h. Por este motivo, para cualquier $q_h \in U \cap A$ se cumple

$$\tilde{f}_h(q_h) = f\Big(\frac{hL(q_h)}{2\pi i}\Big).$$

Esto implica que $\tilde{f}_h$ es holomorfa en la corona abierta A. De este modo, $\tilde{f}_h(q_h)$ admite como expansión de Laurent a

$$\tilde{f}_h(q_h) = \sum_{n\in\mathbb{Z}} a_n q_h^n.$$

En otras palabras, para todo $z \in D$ se cumple

$$f(z) = \sum_{n\in\mathbb{Z}} a_n q_h^n.$$

Dado que la corona tiene como centro al origen, la expansión de Laurent $\tilde{f}_h(q_h)$ es única, es decir, los coeficentes a_n están únicamente determinados. Es más, la fórmula para calcularlos es la indicada. □

Sean C un real no negativo y $f : \mathbb{H} \to \mathbb{C}$ una función de periodo real h y holomorfa en la región $\mathrm{Im}(z) > C$ con q_h-expansión $\sum_{n\in\mathbb{Z}} a_n q_h^n$. Diremos que f es **meromorfa en infinito** si 0 es una singularidad no esencial de la función $\tilde{f}_h$, donde ella es aquella que aparece en la prueba del teorema 2.5. En particular, diremos que f es **holomorfa en infinito** si 0 es una singularidad removible de $\tilde{f}_h$.

Observemos que las nociones definidas arriba son independientes del periodo h. En efecto, si f no es constante en la región $\mathrm{Im}(z) > C$, entonces los periodos de f forman un subgrupo discreto de $(\mathbb{R},+)$ (véase [15, capítulo 6, lema 7]). Por lo cual, la unicidad de la expansión de Laurent de $\tilde{f}_h(q_h)$ nos asegura que la regularidad de ella en infinito es un múltiplo positivo de la de $\tilde{f}_{nh}(q_{nh})$, donde n es un entero positivo.

En virtud de la descripción dada para la regularidad en infinito, podemos definir ahí una noción de orden. De manera específica, para una función $f : \mathbb{H} \to \mathbb{C}$ de periodo real h y holomorfa en la región $\mathrm{Im}(z) > C$, con $C \geq 0$, el **orden de f en infinito** con respecto h está dado por

$$\mathrm{ord}_{\infty i}(f;h) = \mathrm{ord}_0(\tilde{f}_h),$$

donde $\tilde{f}_h$ es la función definida en la prueba del teorema 2.5. Nuevamente, convengamos que si h vale 1, entonces escribiremos $\mathrm{ord}_{\infty i}(f)$ en vez de $\mathrm{ord}_{\infty i}(f;1)$.

Como consecuencia directa del teorema de clasificación de singularidades del análisis complejo, podemos enunciar las distintas caracterizaciones de la regularidad.

Proposición 2.6. *Sea C un real no negativo y $f : \mathbb{H} \to \mathbb{C}$ una función periodo real h y holomorfa en la región $\mathrm{Im}(z) > C$ con q_h-expansión dada por $\sum_{n\in\mathbb{Z}} a_n q_h^n$. Las siguientes condiciones son equivalentes:*

- *f es holomorfa en infinito (respectivamente meromorfa en infinito);*
- *el valor de $\lim_{\mathrm{Im}(z)\to\infty} q_h f(z)$ es 0 (respectivamente el valor de $\lim_{\mathrm{Im}(z)\to\infty} q_h^n f(z)$ es 0 para algún entero positivo n);*
- *el orden de f en infinito respecto a h es no negativo (respectivamente es acotado inferiormente).* □

En este punto, ya podemos definir el principal objeto de estudio de este capítulo. Una función holomorfa $f : \mathbb{H} \to \mathbb{C}$ es una **forma modular** de peso k respecto a $\mathrm{SL}_2(\mathbb{Z})$ si satisface la condición de modularidad de peso k para $\mathrm{SL}_2(\mathbb{Z})$ y si además es holomorfa en infinito. Adicionalmente, diremos que f es una **forma cuspidal** si se cumple

$$\lim_{\mathrm{Im}(z)\to\infty} f(z) = 0.$$

Notemos que toda forma modular respecto a $\mathrm{SL}_2(\mathbb{Z})$ tiene una q-expansión con índices no negativos.

La siguiente proposición nos indica cuál es la relación analítica entre distintos puntos de $\mathbb{H}$ asociada a una forma modular respecto a $\mathrm{SL}_2(\mathbb{Z})$.

Proposición 2.7. *Sea f una forma modular de peso k respecto a $\mathrm{SL}_2(\mathbb{Z})$. Si z_1 y z_2 son elementos de $\mathbb{H}$ que pertenecen a misma órbita de $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$, entonces se cumple*

$$\mathrm{ord}_{z_1}(f) = \mathrm{ord}_{z_2}(f).$$

Prueba. Si z_1 y z_2 son $\mathrm{SL}_2(\mathbb{Z})$-equivalentes, entonces existe $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tal que se cumple $z_1 = \gamma z_2$. Por lo tanto, el resultado se sigue de la igualdad

$$f(z_2) = (cz_1 + d)^k f(z_1). \qquad \square$$

Al conjunto de las formas modulares de peso k respecto a $\mathrm{SL}_2(\mathbb{Z})$ lo denotaremos por $M_k(\mathrm{SL}_2(\mathbb{Z}))$ y al de las formas cuspidales de peso k respecto a $\mathrm{SL}_2(\mathbb{Z})$ por $S_k(\mathrm{SL}_2(\mathbb{Z}))$. La siguiente proposición, cuya prueba es trivial, lista las propiedades más ostensibles de las formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$.

Proposición 2.8. *Las siguientes propiedades se cumplen.*

a. Los conjuntos $M_k(\mathrm{SL}_2(\mathbb{Z}))$ y $S_k(\mathrm{SL}_2(\mathbb{Z}))$ son $\mathbb{C}$-espacios vectoriales.

b. El producto de dos formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$ es también una forma modular respecto a $\mathrm{SL}_2(\mathbb{Z})$ de peso igual a la suma de los pesos. Más aún, si una de ellas es una forma cuspidal, entonces el producto es también una forma cuspidal. $\square$

Hasta ahora las cualidades exhibidas de las formas modulares no nos brindan información sobre su presentación. No obstante, la siguiente proposición pondrá en evidencia los casos más resaltantes.

Proposición 2.9. *La función idénticamente nula definida sobre $\mathbb{H}$ es la única forma modular de peso impar respecto a $\mathrm{SL}_2(\mathbb{Z})$. Es decir, el espacio vectorial $M_k(\mathrm{SL}_2(\mathbb{Z}))$ es trivial para k impar.*

Prueba. Sea $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ con k impar. Para $-I$ la condición de modularidad de peso k se transforma en

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

Deducimos que f es idénticamente nula en $\mathbb{H}$. $\square$

Como consecuencia inmediata de la proposición anterior, las formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$ que discutiremos en adelante, tendrán peso par.

2.2 Series de Eisenstein

En la sección anterior apenas mostramos que la función idénticamente nula definida sobre $\mathbb{H}$ es una forma modular de peso impar respecto a $\mathrm{SL}_2(\mathbb{Z})$. Sin embargo, como debe ser evidente, existen otras igualmente elementales. Por ejemplo, las funciones constantes definidas sobre $\mathbb{H}$ son claramente formas modulares de peso 0. Más aún, ninguna de estas es una forma cúspidal a excepción de la función idénticamente nula definida sobre $\mathbb{H}$.

Presentar ejemplos adicionales de formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$ es una tarea nada trivial. Por lo cual, el resto de la sección está dedicada a presentar ejemplos no elementales de formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$; de paso exhibiremos sus q-expansiónes.

Sea $k \geq 2$ un entero. La **serie de Eisenstein** G_k de peso k definida para todo elemento z de $\mathbb{H}$ está dada por

$$G_k(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^k}.$$

Teorema 2.10. *Todas las series de Eisenstein $G_k(z)$ de peso $k > 2$ son formas modulares de peso k respecto a $\mathrm{SL}_2(\mathbb{Z})$.*

Prueba. Primero verifiquemos que las series de Eisenstein $G_k(z)$ de peso $k > 2$ son holomorfas en $\mathbb{H}$.

Sea K un subconjunto compacto de $\mathbb{H}$. El producto $K \times S^1$ es un subconjunto compacto de $\mathbb{H} \times \mathbb{R}^2$. Como z no es real, la aplicación continua $K \times S^1 \to \mathbb{R}$ definida por $(z, x, y) \mapsto |xz + y|$ alcanza un mínino positivo, digamos u. Más aún, se cumple

$$\begin{aligned}|mz+n|^2 &= \left|\frac{m}{\sqrt{m^2+n^2}}z + \frac{n}{\sqrt{m^2+n^2}}\right|^2 (m^2+n^2)\\ &\geq u^2(m^2+n^2),\end{aligned}$$

para todo $z \in K$ y $(m, n) \in \mathbb{Z}^2$ con $(m, n) \neq (0, 0)$. De esta manera, para todo $z \in K$, el valor de $G_k(z)$ queda acotado superiormente por la serie

$$u^{-2k} \sum_{\substack{(m,n)\in\mathbb{Z}^2\\(m,n)\neq(0,0)}} \frac{1}{(m^2+n^2)^k}.$$

Evidentemente, se tiene

$$\sum_{\substack{(m,n)\in\mathbb{Z}^2\\(m,n)\neq(0,0)}} \frac{1}{(m^2+n^2)^k} = \sum_{N=1}^{\infty} \sum_{m,n} \frac{1}{(m^2+n^2)^k},$$

donde la suma interior es sobre aquellos números enteros m y n que satisfacen $|m| = N$ y $|n| \leq N$, o $|n| = N$ y $|m| \leq N$. Observemos que si fijamos N, entonces existarán a lo más $8N + 4$ pares (m, n) de números enteros que satisfarían las condiciones de la suma interior. Además, se cumple $m^2 + n^2 \geq N$. De este modo, tenemos

$$\sum_{N=1}^{\infty} \sum_{m,n} \frac{1}{(m^2+n^2)^k} \leq \sum_{N=1}^{\infty} (8N+4)\frac{1}{N^k} = \sum_{N=1}^{\infty} 8N^{-k+1} + 4N^{-k}.$$

Esto último implica que las series $G_k(z)$ convergen uniformente sobre K bajo la condición $k > 2$. Es decir, las series de Eisenstein de peso $k > 2$ son holomorfas en $\mathbb{H}$. Notemos que la sutileza que asegura esta parte de nuestro resultado es la convergencia de las p-series, la cual no cubre el caso G_2. Es importante señalemos que la serie de Eisentein de peso 2 junto una pequeña corrección términos es también holomorfa en $\mathbb{H}$; sin embargo, la sustentación de esta afirmación la postergaremos.

Ahora, verifiquemos que todas las series Eisenstein $G_k(z)$ con $k > 2$ satisfacen la condición de modularidad de peso $k > 2$ para $\mathrm{SL}_2(\mathbb{Z})$.

Sea $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Al desarrollar la expresión $G_k(\gamma z)$, obtenemos

$$\begin{aligned} G_k(\gamma z) &= G_k\Big(\frac{az+b}{cz+d}\Big) \\ &= \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \Big(m\frac{az+b}{cz+d}+n\Big)^{-k} \\ &= \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \Big(\frac{maz+mb+ncz+nd}{cz+d}\Big)^{-k} \\ &= (cz+d)^k \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{((ma+nc)z+mb+nd)^k}. \end{aligned}$$

Como las series Eisenstein $G_k(z)$ con $k>2$ convergen absolutamente sobre $\mathbb{H}$ y dado que $\gamma^T = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ define un automorfismo del $\mathbb{Z}$-módulo libre $\mathbb{Z}^2$, se cumple

$$G_k(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{((ma+nc)z+mb+nd)^k}$$

para todo $k>2$. Por lo tanto, las series de Eisenstein $G_k(z)$ con $k>2$ satisfacen la condición de modularidad de peso $k>2$ para $\mathrm{SL}_2(\mathbb{Z})$.

Finalmente, verifiquemos que las series de Eisenstein $G_k(z)$ de peso $k>2$ son holomorfas en infinito.

Notemos primero que para todo $k\geq 2$ se cumple

$$G_k(z) = \sum_{n\in\mathbb{Z}^*} \frac{1}{n^k} + \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0) \\ m\neq 0}} \frac{1}{(mz+n)^k}.$$

Por la proposición 2.6, es suficiente calcular el límite de la expresión de arriba cuando la parte imaginaria de z tiende al infinito; lo que da como resultado

$$\lim_{\mathrm{Im}(z)\to\infty} G_k(z) = 2\zeta(k),$$

donde ζ es **la función zeta de Riemann**. Como $\zeta(k)$ converge para $k\geq 2$, las series de Eisentein $G_k(z)$ de peso $k\geq 2$ son holomorfas en infinito.

En conclusión, las series de Eisenstein $G_k(z)$ de peso $k>2$ son formas modulares (no cuspidales) de peso $k>2$ respecto a $\mathrm{SL}_2(\mathbb{Z})$, ya que $\zeta(k)$ no se anula para $k\geq 2$. $\square$

Como sabemos, las formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$ tienen una q-expansión. Por esta razón, en lo queda de esta sección determinaremos q-expansión de la series de Eisenstein.

Lema 2.11. *La serie* $\sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^2}$ *definida sobre* $\mathbb{H}$ *tiene q-expansión dada por*

$$\sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^2} = (2\pi i)^2 \sum_{n=1}^{\infty} n q^n.$$

Prueba. La función $\pi\cot(\pi z)$ tiene una expasión (véase la proposición III.3.17 de [7]) dada por

$$\pi\cot(\pi z) = \sum_{n\in\mathbb{Z}} \frac{1}{z+n},$$

la cual al ser derivada respecto a z deviene en

$$-\frac{\pi^2}{(\sin(\pi z))^2} = -\sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^2}.$$

Por la definición de $\cot(z)$ tenemos

$$\pi\cot(\pi z) = \pi\frac{\cos(\pi z)}{\sin(\pi z)} = \pi i \frac{q+1}{q-1} = \pi i - \frac{2\pi i}{1-q} = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n.$$

Al igual que antes, derivamos con respecto a z y obtenemos

$$-\frac{\pi^2}{(\sin(\pi z))^2} = -(2\pi i)^2 \sum_{n=1}^{\infty} n q^n,$$

y la afirmación queda verificada. □

La igualdad del siguiente teorema es conocida como la **fórmula de Lipschitz**.

Teorema 2.12. *Para todo entero $k \geq 2$, las series* $(-1)^k \sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^k}$ *definidas sobre* $\mathbb{H}$ *tienen q-expansión dada por*

$$(-1)^k \sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^k} = \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^n.$$

Prueba. Esto es una fácil inducción que se obtiene al derivar sucesivamente la fórmula del lema 2.11. □

Corolario 2.13. *La q-expansión de la serie de Eisenstein $G_k(z)$ está dada por*

$$G_k(z) = 2\zeta(k) + 2\frac{(-2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n,$$

donde $\sigma_{k-1}(n)$ es igual a $\sum_{d|n} d^{k-1}$.

Prueba. Claramente, $G_k(z)$ puede expresarse cual

$$G_k(z) = 2\zeta(k) + 2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^k}.$$

Por el teorema anterior, para todo entero $m \geq 1$ tenemos

$$\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^k} = \sum_{n=1}^{\infty} n^{k-1}q^{mn},$$

De este modo, podemos reescribir $G_k(z)$ cual

$$G_k(z) = 2\zeta(k) + 2\frac{(-2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n^{k-1}q^{mn}.$$

Ahora, si juntamos los términos de igual grado con respecto a q, obtenemos que el coeficiente de cado uno de ellos es $\sigma_{k-1}(s)$, donde s es el grado con respecto a q. Por ello, la nueva presentación para $G_k(z)$ está dada por

$$G_k(z) = 2\zeta(k) + 2\frac{(-2\pi i)^k}{(k-1)!}\sum_{s=1}^{\infty}\sigma_{k-1}(s)q^s. \qquad \square$$

Debido a lo engorroso que es determinar el valor de $\zeta(k)$ para enteros $k \geq 2$, es conveniente normalizar las q-expansión de las series de Eisenstein $G_k(z)$ de manera que el término independiente de ellas sea 1. De este modo, definimos las **series de Eisenstein normalizadas** $E_k(z)$ de peso k mediante

$$E_k(z) = \frac{1}{2\zeta(k)}G_k(z).$$

Ejemplo 2.14. Las q-expansión de las seis primeras series de Eisenstein normalizadas están dadas por (para E_2 la expresión es apenas formal)

$$\begin{aligned} E_2(z) &= 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n, & E_8(z) &= 1 + 480\sum_{n=1}^{\infty}\sigma_7(n)q^n, \\ E_4(z) &= 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n, & E_{10}(z) &= 1 - 264\sum_{n=1}^{\infty}\sigma_9(n)q^n, \\ E_6(z) &= 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n, & E_{12}(z) &= 1 + \frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n. \end{aligned}$$

Finalicemos esta sección mostrando que las únicas formas modulares no cuspidales respecto a $\mathrm{SL}_2(\mathbb{Z})$ de peso al menos cuatro son aquellas generadas por alguna serie de Eisenstein normalizada.

Proposición 2.15. *Los espacios $M_k(\mathrm{SL}_2(\mathbb{Z}))$ con $k \geq 4$ satisfacen la descomposición*

$$M_k(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}E_k \oplus S_k(\mathrm{SL}_2(\mathbb{Z})).$$

En particular, se tiene $\dim M_k(\mathrm{SL}_2(\mathbb{Z})) = 1 + \dim S_k(\mathrm{SL}_2(\mathbb{Z}))$.

Prueba. Sea $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$. Como la identidad $f = cE_k + (f - cE_k)$ se verifica para cualquier $c \in \mathbb{C}$, es suficiente mostrar que existe un c adecuado tal que $f - wE_k$ es cuspidal. En efecto, si tomamos $c = \lim_{\mathrm{Im}(z)\to\infty} f(z)$ cumplimos con lo solicitado. □

2.3 La fórmula $k/12$

En la sección precendente mostramos que las series de Eisenstein de peso al menos cuatro son formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$. Más aún, si consideramos sus versiones normalizadas, verificamos que estas son no cuspidales ya que toman 1 como valor de término independiente en sus correspondientes q-expansiones.

Al final de la sección mostramos que el conjunto de formas modulares no cuspidales de peso al menos cuatro es el subespacio vectorial generado por alguna serie de Eisenstein normalizada. Por tal motivo, para determinar cuán grande es el espacio vectorial de las formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$, basta determinar la dimensión de las formas cuspidales. En esta sección, estableceremos una fórmula para determinar la dimension exacta de estos espacios.

Sea $f : \mathbb{H} \to \mathbb{C} \cup \{\infty\}$ una función meromorfa. Diremos que f es **forma modular meromorfa** si existe $C > 0$ para el cual f es holomorfa en la región $\mathrm{Im}(z) > C$, satisface la condición de modularidad de peso k para $\mathrm{SL}_2(\mathbb{Z})$ y si además es meromorfa en infinito. Claramente, toda forma modular de peso k respecto a $\mathrm{SL}_2(\mathbb{Z})$ es una forma modular meromorfa de peso k respecto a $\mathrm{SL}_2(\mathbb{Z})$.

Lema 2.16. *Toda forma modular meromorfa respecto a* $\mathrm{SL}_2(\mathbb{Z})$ *no idénticamente nula en* $\mathbb{H}$ *tiene una cantidad finita de ceros y polos en la región modular.*

Prueba. Sea f una forma modular meromorfa. Por definición, existe un real $C > 0$ tal que el conjunto $K = \{z \in F_{\mathrm{SL}_2(\mathbb{Z})} : |z| \leq C\}$ contiene a los polos de f. Dado que este conjunto es compacto, la cantidad de polos y ceros es finita. Como f no tiene una singularidad esencial en $i\infty$, los ceros no se acumulan en $F_{\mathrm{SL}_2(\mathbb{Z})} \backslash K$. Se sigue que la cantidad de ceros es finita. $\square$

El siguiente teorema es conocido como la **fórmula** $k/12$.

Teorema 2.17. *Para toda forma modular meromorfa f de peso k respecto a* $\mathrm{SL}_2(\mathbb{Z})$ *no idénticamente nula en* $\mathbb{H}$ *se verifica*

$$\mathrm{ord}_{\infty i}(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_{\rho^2}(f) + \sum_{\substack{\overline{z} \in \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \\ \overline{z} \neq \overline{i}, \overline{\rho}^2}} \mathrm{ord}_z(f) = \frac{k}{12}.$$

Prueba. Este resultado es esencialmente una aplicación del ***principio del argumento de Cauchy***. Como el enunciado lo sugiere, debemos considerar una región en la cual estén representados todos los elementos de $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$. Esto nos está insinuando que la región con la que trabajemos tiene relación con un dominio fundamental de $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$.

Si consideramos toda la región modular salvo por los puntos i, ρ y ρ^2, el lema anterior nos asegura que para algún $C > 0$ se cumple

$$\sum_{\substack{\overline{z} \in \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \\ \overline{z} \neq \overline{i}, \overline{p}^2}} \mathrm{ord}_z(f) = \sum_{\substack{z \in F_{\mathrm{SL}_2(\mathbb{Z})} \\ |z| < C \\ z \neq i, \rho, \rho^2}} \mathrm{ord}_z(f).$$

Esta igualdad se satisface siempre que no haya ceros ni polos en los puntos de la frontera de $F_{\mathrm{SL}_2(\mathbb{Z})}$ excepto por lo no tomados, pues de lo contrario habría duplicidades en la suma de la derecha debido a la proposición 2.7.

Por lo disctutido en el párrafo anterior, la región a considerar es aquella limitada por la curva descrita en la imagen 2.1. En este gráfico, las líneas punteadas describen

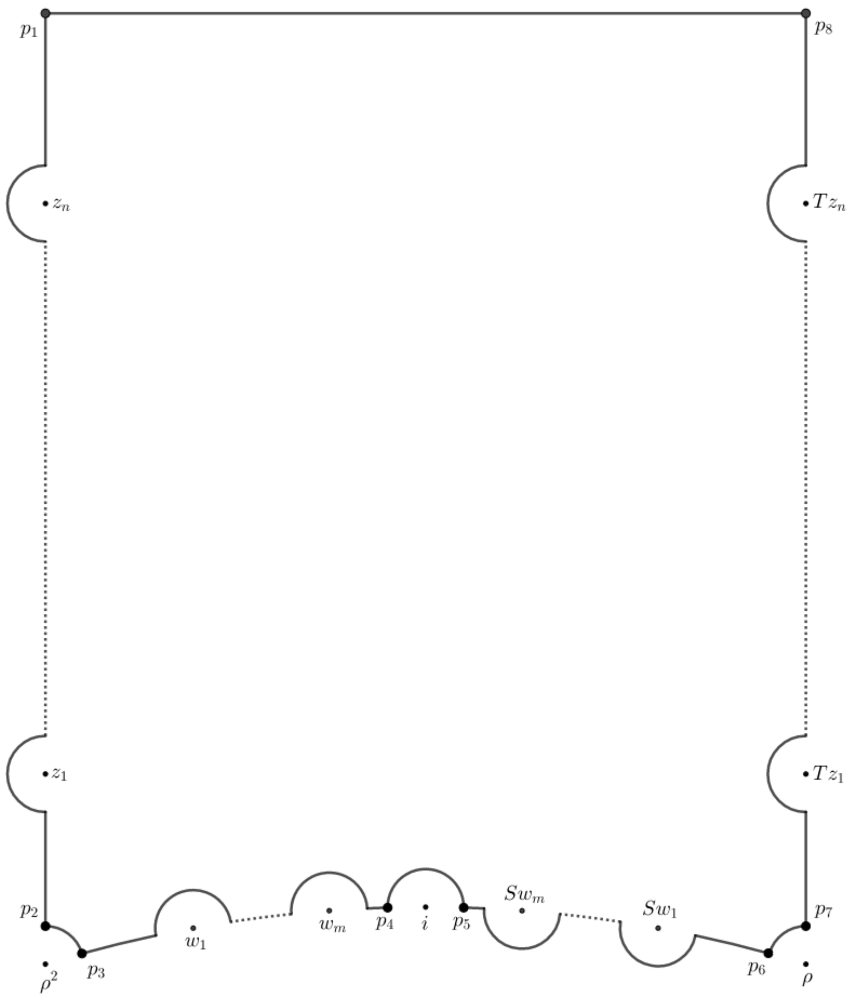

Figura 2.1: Curva $\mathscr{C}_\epsilon$

implícitamente a otros puntos y a otros arcos de circuferencia cuyos centros son los anteriores. El tramo vertical de la izquierda pertenece a la recta $\mathrm{Re}(z) = -\dfrac{1}{2}$ y el de la derecha a la recta $\mathrm{Re}(z) = \dfrac{1}{2}$. En el primero están los puntos $z_1, \ldots, z_n, p_1$ y p_2; y en segundo están los puntos p_7 y p_8. Además, se cumple $Tp_1 = p_8$ y $Tp_2 = p_7$. El tramo superior es parte de la recta $\mathrm{Im}(z) = C$ y los puntos $w_1, \ldots, w_m, p_3, p_4, p_5$ y p_6 son elementos de la semicircunferencia $|z| = 1$ dentro $\mathbb{H}$. Finalmente, los radios de los arcos de la curva descrita valen ϵ, el cual es muy pequeño.

Claramente, se cumple

$$\lim_{\epsilon \to 0} \frac{1}{2\pi i} \oint_{\mathscr{C}_\epsilon} \frac{f'(z)}{f(z)} dz = \sum_{\substack{\overline{z} \in \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \\ \overline{z} \neq \overline{i}, \overline{p}^2}} \mathrm{ord}_z(f).$$

Por ello, nuestros esfuerzos estarán enfocadas al cálculo del límite anterior.

1. **Evalución del tramo p_8-p_1:**

$$\lim_{\epsilon\to 0}\frac{1}{2\pi i}\int_{p_8}^{p_1}\frac{f'(z)}{f(z)}dz = \lim_{\epsilon\to 0}\frac{1}{2\pi i}\oint_{q\in U}\frac{\tilde{f}'(q)}{\tilde{f}(q)}dq \quad (U=\partial B(0,e^{-2\pi C}))$$
$$= -\mathrm{ord}_{\infty i}(f).$$

2. **Evalución de los tramos p_1-p_2 y p_7-p_8:**

$$\begin{aligned}\lim_{\epsilon\to 0}\Big(\frac{1}{2\pi i}\int_{p_1}^{p_2}\frac{f'(z)}{f(z)}dz+\frac{1}{2\pi i}\int_{p_7}^{p_8}\frac{f'(z)}{f(z)}dz\Big) &= \lim_{\epsilon\to 0}\Big(\frac{1}{2\pi i}\int_{p_8}^{p_7}\frac{f'(Tz)}{f(Tz)}dTz+\frac{1}{2\pi i}\int_{p_7}^{p_8}\frac{f'(z)}{f(z)}dz\Big)\\ &= \lim_{\epsilon\to 0}\Big(-\frac{1}{2\pi i}\int_{p_7}^{p_8}\frac{f'(z)}{f(z)}dz+\frac{1}{2\pi i}\int_{p_7}^{p_8}\frac{f'(z)}{f(z)}dz\Big)\\ &= 0.\end{aligned}$$

3. **Evalución de los tramos p_3-p_4 y p_5-p_6:**

$$\begin{aligned}\lim_{\epsilon\to 0}\Big(\frac{1}{2\pi i}\int_{p_3}^{p_4}\frac{f'(z)}{f(z)}dz+\frac{1}{2\pi i}\int_{p_5}^{p_6}\frac{f'(z)}{f(z)}dz\Big) &= \lim_{\epsilon\to 0}\Big(\frac{1}{2\pi i}\int_{p_6}^{p_5}\frac{f'(Sz)}{f(Sz)}dSz+\frac{1}{2\pi i}\int_{p_5}^{p_6}\frac{f'(z)}{f(z)}dz\Big)\\ &\lim_{\epsilon\to 0}\Big(=\frac{1}{2\pi i}\int_{p_6}^{p_5}\left(\frac{k}{z}+\frac{f'(z)}{f(z)}\right)dz+\frac{1}{2\pi i}\int_{p_5}^{p_6}\frac{f'(z)}{f(z)}dz\Big)\\ &= \lim_{\epsilon\to 0}\Big(\frac{k}{2\pi i}(\ln(p_5)-\ln(p_6))\Big)\\ &= \frac{k}{2\pi i}\Big(\frac{\pi i}{6}\Big)\\ &= \frac{k}{12}.\end{aligned}$$

4. **Evalución de los tramos p_2-p_3 y p_6-p_7:**

$$\lim_{\epsilon\to 0}\Big(\frac{1}{2\pi i}\int_{p_2}^{p_3}\frac{f'(z)}{f(z)}dz+\frac{1}{2\pi i}\int_{p_6}^{p_7}\frac{f'(z)}{f(z)}dz\Big)=-\frac{1}{6}\mathrm{ord}_{\rho^2}(f)-\frac{1}{6}\mathrm{ord}_{\rho}(f)$$
$$=-\frac{1}{3}\mathrm{ord}_{\rho^2}(f)\quad (\textbf{por la proposición 2.7}).$$

5. Evalución del tramo p_4-p_5:

$$\lim_{\epsilon\to 0}\left(\frac{1}{2\pi i}\int_{p_4}^{p_5}\frac{f'(z)}{f(z)}dz\right)=-\frac{1}{2}\mathrm{ord}_i(f).$$

En resumen, tenemos

$$\lim_{\epsilon\to 0}\frac{1}{2\pi i}\oint_{\mathscr{C}_\epsilon}\frac{f'(z)}{f(z)}dz=-\mathrm{ord}_{\infty i}(f)-\frac{1}{2}\mathrm{ord}_i(f)-\frac{1}{3}\mathrm{ord}_{\rho^2}(f)+\frac{k}{12}.$$

Hemos asíconseguido lo anunciado. □

Corolario 2.18. *Para las formas modulares respecto a* $\mathrm{SL}_2(\mathbb{Z})$ *tenemos las siguientes propiedades en* $\mathbb{H}$.

a) Todas las formas modulares de peso negativo son idénticamente nulas.

b) Las funciones constantes son las únicas formas modulares de peso 0.

c) Las formas modulares de peso 2 son idénticamente nulas.

d) La forma modular $E_4(z)$ *tiene un cero simple en* $z=\rho^2$.

e) La forma modular $E_6(z)$ *tiene un cero simple en* $z=i$.

f) Los espacios cuspidales de peso menor o igual a 10 están conformados por la función idénticamente nula.

g) Los espacios de formas modulares de peso 4, 6, 8 y 10 son expandidos por las series de Eisenstein normalizadas. En particular, son unidimensionales.

h) Se satisfacen las igualdades $E_4^2=E_8$ *y* $E_4E_6=E_{10}$.

Prueba. Todas estas propiedades son consecuencia inmediata de la fórmula $\frac{k}{12}$.

a) Si hubiese alguna forma modular de peso negativo no idénticamente nula, esta no cumpliría la fórmula $\frac{k}{12}$ pues el valor de la parte izquierda sería no negativo y el de la derecha negativo. Así, la función idénticamente nula es la única forma modular de peso 0.

b) Si $f(z)$ es una forma de peso 0, entonces $f(z) - f(i)$ también lo es con un cero en $z = i$. Si $f(z) - f(i)$ no se anula idénticamente, entonces el valor de la parte de la izquierda de fórmula $\frac{k}{12}$ es positivo y el de la derecha es 0. Por lo cual, $f(z) - f(i)$ debe ser la función idénticamente nula; es decir, f es una función constante.

c) Al igual que antes, si consideramos una forma modular de peso 2 no idénticamente nula, esta no satisfaría la fórmula $\frac{k}{12}$ ya que el valor de la parte de la izquierda de la fórmula, cuando no es 0, es al menos $1/3$, valor diferente a $1/6$, el cual es el valor correspondiente a la parte derecha de la fórmula. De este modo, la única forma modular de peso 2 es la función idénticamente nula.

d) Como E_4 es una forma modular de peso 4 no idénticamente nula, en este caso la fórmula $\frac{k}{12}$ nos dice para ella que el valor del lado izquierdo debe ser $1/3$. Lo cual solo es posible si el orden de $E_4(z)$ en $z = \rho^2$ es 1.

e) Como E_6 es una forma modular de peso 6 no idénticamente nula, en este caso la fórmula $\frac{k}{12}$ nos dice para ella que el valor del lado izquierdo debe ser $1/2$. Lo cual, solo sucede si el orden de $E_6(z)$ en $z = i$ es 1.

f) Si existiese una forma cuspidal de peso a lo más 10 que no se anula idénticamente, la fórmula $\frac{k}{12}$ no se satisfaría ya que el valor del lado izquierdo es al menos 1 y el de lado derecho como mucho $5/6$. Por esta razón, la función idénticamente nula es la única cuspidal de peso a lo más 10.

g) Por la parte f) y la proposición 2.15 deducimos que la dimensión de los espacios de formas modulares de peso 4, 6, 8 y 10 es 1.

h) Por parte g) y el hecho de que los coeficientes independientes de las series de Eisenstein normalizadas valen 1 concluimos $E_4^2 = E_8$ y $E_4 E_6 = E_{10}$. □

Como mencionamos de pasada al inicio de la sección, la tarea es determinar con exactitud cuál es la dimensión de cada espacio de formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$. Sin embargo, antes debemos probar que cada uno de estos espacio vectoriales es de dimensión finita.

Lema 2.19. *Sea f una forma modular de peso k respecto a* $\mathrm{SL}_2(\mathbb{Z})$*. Si se cumple*

$$\mathrm{ord}_{\infty i}(f) > \frac{k}{12},$$

entonces f es indénticamente nula en $\mathbb{H}$*.*

Prueba. Si f no es idénticamente nula en $\mathbb{H}$, entonces satisface la fórmula $\frac{k}{12}$. Sin embargo, esto sería contradicción debido a la premisa. Por lo tanto, f es necesariamente idénticamente nula en $\mathbb{H}$. □

El siguiente teorema expresa que la búsqueda para determinar una fórmula para las dimensiones de los espacios formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$ tiene asidero.

Teorema 2.20. *El espacio vectorial $M_k(\mathrm{SL}_2(\mathbb{Z}))$ es finito dimensional.*

Prueba. Por la parte *a*) del corolario 2.18, sabemos que cada uno de los espacios vectoriales $M_k(\mathrm{SL}_2(\mathbb{Z}))$ con $k < 0$ son finito dimensionales. Por este motivo, es suficiente verificar la afirmación para $k \geq 0$. Si bien, por la proposición 2.9 y por las partes *b*), *c*) y *g*) del corolario 2.18, son menos casos los que debemos verificar, el argumento que usaremos cubre todos los casos $k \geq 0$.

Consideremos la siguiente transformación lineal

$$\begin{aligned} M_k(\mathrm{SL}_2(\mathbb{Z})) &\to \mathbb{C}^{r+1} \\ \sum_{n=0}^{\infty} a_n q^n &\mapsto (a_0, \ldots, a_r), \end{aligned}$$

donde r es igual a $\left\lfloor \frac{k}{12} \right\rfloor$. Por el lema 2.19, esta transformación es inyectiva. Por lo tanto, tenemos $\dim M_k(\mathrm{SL}_2(\mathbb{Z})) \leq \left\lfloor \frac{k}{12} \right\rfloor + 1$. □

Todo lo desarrollado hasta ahora nos sirve como preludio para presentar el más célebre ejemplo de formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$. Este el caso de la **forma de Ramanujan** Δ, la cual está definida por

$$\Delta = \frac{E_4^3 - E_6^2}{1728}.$$

Observemos que las partes e) y f) del corolario 2.18 aseguran que Δ no es idénticamente nula en $\mathbb{H}$. Es más, gracias a la fórmula $\frac{k}{12}$ se deduce que Δ no se anula en ningún punto de $\mathbb{H}$. Sin embargo, si lo hace en infinito donde admite un cero simple.

Esta observación nos permite probar el siguiente teorema.

Teorema 2.21. *Los espacios vectoriales* $M_{k-12}(\mathrm{SL}_2(\mathbb{Z}))$ *y* $S_k(\mathrm{SL}_2(\mathbb{Z}))$ *son isomorfos.*

Prueba. Consideremos a la aplicación

$$\begin{gathered} M_{k-12}(\mathrm{SL}_2(\mathbb{Z})) \to S_k(\mathrm{SL}_2(\mathbb{Z})) \\ f \mapsto \Delta f, \end{gathered}$$

la cual es un homomorfismo por la proposición 2.8. Por lo tanto, para mostrar que los espacios $M_{k-12}(\mathrm{SL}_2(\mathbb{Z}))$ y $S_k(\mathrm{SL}_2(\mathbb{Z}))$ son isomorfos, solo resta verificar la biyectividad de la aplicación escogida.

Sean f_1 y f_2 elementos de $M_{k-12}(\mathrm{SL}_2(\mathbb{Z}))$ tales que se satisface $\Delta f_1 = \Delta f_2$. Como Δ no se anula en $\mathbb{H}$, deducimos $f_1 = f_2$. Es decir, se verifica la inyectividad.

Sea g un elemento de $S_k(\mathrm{SL}_2(\mathbb{Z}))$. Claramente, el cociente $\dfrac{g}{\Delta}$ es una función holomorfa en $\mathbb{H}$ y además satisface la condición de modularidad de peso $k-12$ para $\mathrm{SL}_2(\mathbb{Z})$. Como se cumple $\mathrm{ord}_{\infty i}(g) \geq 1$ y $\mathrm{ord}_{\infty i}(\Delta) = 1$, la función $\dfrac{g}{\Delta}$ es holomorfa en infinito. Esto implica que este cociente es una forma modular de peso $k-12$ respecto a $\mathrm{SL}_2(\mathbb{Z})$. En otras palabras, hemos verificado la sobreyectividad. □

Corolario 2.22. *Si k es número par, entonces se tienen las siguientes fórmulas para las dimensiones.*

a) Si $k \geq 0$ *se tiene*

$$\dim M_k(\mathrm{SL}_2(\mathbb{Z})) = \begin{cases} \left\lfloor \dfrac{k}{12} \right\rfloor & \textit{para } k \equiv 2 \mod 12, \\ \left\lfloor \dfrac{k}{12} \right\rfloor + 1 & \textit{para } k \not\equiv 2 \mod 12. \end{cases}$$

b) Si $k \geq 4$ *se tiene*

$$\dim S_k(\mathrm{SL}_2(\mathbb{Z})) = \begin{cases} \left\lfloor \dfrac{k}{12} \right\rfloor - 1 & \textit{para } k \equiv 2 \mod 12, \\ \left\lfloor \dfrac{k}{12} \right\rfloor & \textit{para } k \not\equiv 2 \mod 12. \end{cases}$$

Prueba. La parte *a*) se verifica para $k \leq 10$ por las partes *b*), *c*) y *g*) del corolario 2.18.

Por otro lado, por la proposición 2.15 y el teorema 2.21 tenemos

$$\begin{aligned}\dim M_k(\mathrm{SL}_2(\mathbb{Z})) &= 1 + \dim S_k(\mathrm{SL}_2(\mathbb{Z}))\\ &= 1 + \dim M_{k-12}(\mathrm{SL}_2(\mathbb{Z}))\end{aligned}$$

para $k \geq 12$. Por ello, podemos usar inducción en esta recurrencia para verificar la primera fórmula para el resto de casos.

La parte b) es consecuencia de la parte a) junto con el teorema 2.15. $\square$

El corolario anterior salda nuestra deuda respecto a lo prometido al inicio de la sección. Por lo cual, de aquí al final del capítulo solo brindaremos algunas conclusiones adicionales que se derivan de los resultados anteriores de esta misma sección.

Teorema 2.23. *El conjunto* $\{E_4^m E_6^n : m, n \in \mathbb{N} \text{ y } 4m + 6n = k\}$ *es una base de* $M_k(\mathrm{SL}_2(\mathbb{Z}))$ *para todo par* $k \geq 4$.

Prueba. Primero probaremos que para todo par $k \geq 4$ se cumple

$$M_k(\mathrm{SL}_2(\mathbb{Z})) = \operatorname*{span}_{\substack{4m+6n=k\\ m,n\geq 0}} \{E_4^m E_6^n\}.$$

Por la parte f), g) y h) del corolario 2.18, la afirmación es clara para $k \leq 10$. Para los otros valores de k, todos pares, consideremos el hecho de que siempre existen enteros positivos m y n sujetos a $4m + 6n = k$.

Sean $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ con $k \geq 12$ y $g = E_4^m E_6^n$. La forma modular g no se anula en infinito; sin embargo, podemos conseguir $c \in \mathbb{C}$ tal que $f - cg$ sí lo haga. Debido a ello, el teorema 2.21 nos dice que podemos escribir $f = cg + \Delta h$ para algún $h \in M_{k-12}(\mathrm{SL}_2(\mathbb{Z}))$.

Por la parte b) y c) del corolario 2.18, podemos deducir del párrafo anterior que el resultado buscado es válido para $k = 12$ y $k = 14$. Por lo tanto, podemos usar inducción para los valores restantes de k.

A continuación, probaremos la independencia lineal de los monomios $E_4^m E_6^n$.

Consideremos la siguiente ecuación lineal

$$\sum_{\substack{4m+6n=k\\ m,n\geq 0}} a_{mn} E_4^m E_6^n = 0,$$

donde las incógnitas a_{mn} son números complejos. Por las partes d) y e) del corolario 2.18 y por la fórmula $\frac{k}{12}$ se verifica $E_4(\rho^2) = 0$ y $E_6(\rho^2) \neq 0$, lo cual implica que el valor incógnita a_{0n} es 0. Análogamente, tenemos que el valor de a_{m0} es 0, pues se cumple $E_6(i) = 0$ y $E_4(i) \neq 0$. De este modo, nuestra ecuación lineal se convierte en

$$\sum_{\substack{4(m-1)+6(n-1)=k-10 \\ m,n\geq 1}} a_{mn} E_4^m E_6^n = 0.$$

Evidentemente, podemos simplificar un factor $E_4 E_6$ de nuestra ecuación. Así, conseguimos una nueva versión de ella dada por

$$\sum_{\substack{4(m-1)+6(n-1)=k-10 \\ m,n\geq 1}} a_{mn} E_4^{m-1} E_6^{n-1} = 0.$$

Si repetimos sucesivamente el procedimiento del párrafo anterior, eventualmente determinaremos que el valor de todas las incógnitas a_{mn} es 0. □

Corolario 2.24. *El anillo graduado* $\bigoplus_{k\in\mathbb{Z}} M_k(\mathrm{SL}_2(\mathbb{Z}))$ *es isomorfo a* $\mathbb{C}[E_4, E_6]$. □

El **invariante** j es la función holomorfa en $\mathbb{H}$ dada por

$$j(z) = \frac{E_4^3(z)}{\Delta(z)},$$

la cual es $\mathrm{SL}_2(\mathbb{Z})$-invariante y meromorfa en infinito con orden -1. Además, por la fórmula $\frac{k}{12}$ su imagen es $\mathbb{C}$ y cumple $\mathrm{ord}_i(j) = 0$ y $\mathrm{ord}_{\rho^2}(j) = 3$.

El invariante j resalta dentro un conjunto de funciones llamadas funciones modulares. Una función meromorfa $f : \mathbb{H} \to \mathbb{C} \cup \{\infty\}$ es una **función modular** si existe $C > 0$ para el cual f es holomorfa en la región $\mathrm{Im}(z) > C$, es $\mathrm{SL}_2(\mathbb{Z})$-invariante y es meromorfa en infinito.

El siguiente teorema clasifica las funciones modulares.

Teorema 2.25. *Sea* $f : \mathbb{H} \to \overline{\mathbb{C}}$ *una función meromorfa. Las siguientes afirmaciones son equivalentes:*

(i) f *es una función modular;*

(ii) f *es el cociente de dos formas modulares del mismo peso;*

(iii) f es una función racional de j.

Prueba. La ruta (iii) implica (ii) implica (i) es inmediata. Por cual, basta entonces probar que (i) implica (iii).

Si f es una función modular con polo de orden r en un punto $w \in \mathbb{H}$, entonces el producto $(j(z) - j(w))^r f(z)$ es una función modular sin polo en w. Ello nos permite asumir que f es holomorfa en $\mathbb{H}$. Más aún, para un entero $k > 0$ conveniente tenemos que $\Delta^k f$ es holomorfa en infinito, y por lo tanto, es una forma modular de peso $12k$. Por el teorema 2.23, el problema se reduce a verificar que $\frac{E_4^m E_6^n}{\Delta^k}$ es un polinomio en j, donde m y n son enteros positivos que obedecen $4m + 6n = 12k$.

Notemos que 3 divide a m y 2 divide a n, lo cual deriva en

$$\begin{aligned} \frac{E_4^m E_6^n}{\Delta^k} &= \frac{(E_4^3)^{m/3}(E_6^2)^{n/2}}{\Delta^k} \\ &= \left(\frac{E_4^3}{\Delta}\right)^{m/3}\left(\frac{E_6^2}{\Delta}\right)^{n/2}. \end{aligned}$$

Por lo tanto, de la definición de j y de Δ conseguimos

$$\frac{E_4^m E_6^n}{\Delta^k} = j^{m/3}(j - 1728)^{n/2}. \qquad \square$$

Corolario 2.26. *El cuerpo de funciones modulares coincide con el cuerpo de funciones racionales respecto al invariente j.* $\square$

Capítulo 3

Operadores de Hecke I

En este capítulo presentaremos al enésimo operador de Hecke para las formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$ y además probaremos parcialmente la conjetura de Ramanujan. Los principales materiales de consulta para este capítulo son [6] y [19].

3.1 El enésimo operador de Hecke

En esta sección recopilaremos gran parte de los resultados de Hecke de *Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung I* [8]. No obstante, la presentación será en un lenguaje moderno.

Sea $M_2(\mathbb{Z}, n)$ el conjunto de matrices enteras 2×2 de determinante $n > 0$. El grupo modular actúa sobre $M_2(\mathbb{Z}, n)$ de manera natural vía multiplicación por la izquierda. Por consiguiente, podemos definir el espacio órbitas $M_2(\mathbb{Z}, n)/\mathrm{SL}_2(\mathbb{Z})$, el cual es finito gracias al siguiente teorema.

Teorema 3.1. *Un conjunto transversal de $M_2(\mathbb{Z}, n)/\mathrm{SL}_2(\mathbb{Z})$ está dado por*

$$\left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in M_2(\mathbb{Z}, n) : a \geq 1,\ ad = n,\ 0 \leq b \leq d-1 \right\}.$$

En otras palabras, en notación símbolica podemos escribir

$$M_2(\mathbb{Z}, n) = \bigsqcup_{\substack{ad=n \\ d>0}} \bigsqcup_{b=0}^{d-1} \mathrm{SL}_2(\mathbb{Z}) \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}.$$

Prueba. Sea $\begin{bmatrix} e & f \\ g & h \end{bmatrix}$ un elemento de $M_2(\mathbb{Z}, n)$. Para probar la afirmación, debemos encontrar matrices $\begin{bmatrix} r & s \\ t & u \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ y $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in M_2(\mathbb{Z}, n)$ relacionadas mediante

$$\begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} ra & rb+sd \\ ta & tb+ud \end{bmatrix}.$$

La relación de arriba sugiere que tomemos $a = \mathrm{mcd}(e, g)$, $r = \dfrac{e}{a}$ y $t = \dfrac{g}{a}$. Esto connota que r y t son coprimos, por lo cual existen enteros s y u sujetos a $ru - ts = 1$. De este modo, conseguimos

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} r & s \\ t & u \end{bmatrix}^{-1} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} u & -s \\ -t & r \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

que impone $b = fu - hs$ y $d = -ft + hr$.

Como el valor de la determinante de $\begin{bmatrix} r & s \\ t & u \end{bmatrix}^{-1} \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ no varía, obtenemos $ad = n$, lo que de manera indirecta prueba la positividad de d. Esto significa que solo resta asegurar el cumplimiento de $0 \leq b \leq d-1$. Para este fin, recurrimos a la identidad

$$\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} a & b+kd \\ 0 & d \end{bmatrix},$$

donde k es un entero, de donde se desprende mecánicamente lo deseado.

Finalmente, comprobaremos que no existen elementos $\mathrm{SL}_2(\mathbb{Z})$-equivalentes entre sí en el conjunto

$$\left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in M_2(\mathbb{Z}, n) : a \geq 1,\, ad = n,\, 0 \leq b \leq d-1 \right\}.$$

En efecto, sean $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ y $\begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix}$ elementos como arriba tales que existe $\begin{bmatrix} r & s \\ t & u \end{bmatrix}$ en $\mathrm{SL}_2(\mathbb{Z})$ con el cual se cumple $\begin{bmatrix} r & s \\ t & u \end{bmatrix} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix}$. Así debe satisfacerse

$$\begin{bmatrix} ar & br+sd \\ at & bt+ud \end{bmatrix} = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix},$$

de lo que desprende que t y ru son 0 y 1 respectivamente. Como a y a' son positivos, el valor de r y u debe ser 1. Esto último implica que a y a' son iguales, lo mismo se concluye para d y d'. Finalmente, de las desigualdades $0 \leq b \leq d-1$ y $0 \leq b' \leq d-1$ obtenemos que s vale 0, pues $b + sd$ es igual b'. Hemos verificado así la afirmación. □

Sea un entero n positivo. El **enésimo operador de Hecke** $T_n^{[k]}$ de peso k para las formas modulares de peso k respecto a $\mathrm{SL}_2(\mathbb{Z})$ está dado por

$$T_n^{[k]}(f) = n^{k/2-1} \sum_{\overline{\alpha} \in M_2(\mathbb{Z},n)/\mathrm{SL}_2(\mathbb{Z})} f[\alpha]_k,$$

donde f es un elemento de $M_k(\mathrm{SL}_2(\mathbb{Z}))$. Convengamos que cuando el peso del enésimo operador de Hecke esté sobreentendido, escribiremos T_n en vez de $T_n^{[k]}$.

La buena definición de enésimo operador de Hecke $T_n^{[k]}$ está garantizada gracias al teorema 3.1, la proposición 2.1 y al hecho de que los objetos en discusión satisfacen la condición de modularidad peso k para $\mathrm{SL}_2(\mathbb{Z})$. Más aún, $T_n^{[k]}$ puede expresarse de manera más amigable como

$$T_n^{[k]}(f) = n^{k/2-1} \sum_{\substack{ad=n \\ d>0}} \sum_{b=0}^{d-1} f \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}_k.$$

Ejemplo 3.2. El operador $T_1^{[k]}$ es el operador identidad para las formas modulares de peso k respecto a $\mathrm{SL}_2(\mathbb{Z})$.

Como lo afirma su nombre, $T_n^{[k]}$ es un operador del espacio $M_k(\mathrm{SL}_2(\mathbb{Z}))$. Sin embargo, verificarlo no es inmediato. Para ello usaremos el siguiente lema trivial, el cual dejaremos como ejercicio para el lector.

Lema 3.3. *Para n entero positivo se tiene*

$$\sum_{b=0}^{a-1} e^{i\frac{2\pi nb}{a}} = \begin{cases} a & \text{si } a \text{ divide } n, \\ 0 & \text{en caso contrario.} \end{cases}$$

□

El siguiente teorema no solo justifica el nombre de $T_n^{[k]}$ sino también su relevancia.

Teorema 3.4. *Para todo entero positivo n, el operador de Hecke $T_n^{[k]}$ es un operador lineal de $M_k(\mathrm{SL}_2(\mathbb{Z}))$. Explícitamente, si f es una forma modular de peso k respecto a $\mathrm{SL}_2(\mathbb{Z})$, la q-expansión de $T_n(f)$ está dada por*

$$T_n(f) = \sum_{m=0}^{\infty} \Bigg(\sum_{\substack{d|m,n \\ d>0}} d^{k-1} \lambda\Big(\frac{mn}{d^2}\Big) \Bigg) q^m$$

donde los $\lambda(m)$ son los coeficientes de la q-expansión de f.

Prueba. Sea f un elemento de $M_k(\mathrm{SL}_2(\mathbb{Z}))$ con q-expansión dada por $\sum_{s=0}^{\infty} \lambda(s) q^s$. Claramente $T_n(f)$ es holomorfa en todo $\mathbb{H}$, por lo cual solo debemos verificar si satisface la condición de modularidad de peso k para $\mathrm{SL}_2(\mathbb{Z})$ y si es regular en infinito.

Primero mostremos que $T_n(f)$ satisface la condición de modularidad de peso k para $\mathrm{SL}_2(\mathbb{Z})$. De la identidad elemental $\mathrm{SL}_2(\mathbb{Z}) M_2(\mathbb{Z}, n) \mathrm{SL}_2(\mathbb{Z}) = M_2(\mathbb{Z}, n)$ concluimos que se cumple $M_2(\mathbb{Z}, n)\mathrm{SL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) M_2(\mathbb{Z}, n)$. Por lo cual, aseguramos que para cualesquiera $\overline{\alpha} \in M_2(\mathbb{Z}, n)/\mathrm{SL}_2(\mathbb{Z})$ y $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, existen $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ y $\overline{\beta} \in M_2(\mathbb{Z}, n)/\mathrm{SL}_2(\mathbb{Z})$ tales que se cumple $\alpha\gamma = \gamma'\beta$. Más aún, si exisitiese $\overline{\alpha'} \in M_n(\mathbb{Z}, 2)/\mathrm{SL}_2(\mathbb{Z})$ tal que para algún $\gamma'' \in \mathrm{SL}_2(\mathbb{Z})$ se tenga $\alpha'\gamma = \gamma''\beta$, entonces claramente se deberá cumplir $\overline{\alpha}' = \overline{\alpha}$.

Al desarrollar la expresión $T_n(f)[\gamma]_k$ obtenemos por definición

$$\begin{aligned} T_n(f)[\gamma] &= \Big(n^{k/2-1} \sum_{\overline{\alpha} \in M_2(\mathbb{Z},n)/\mathrm{SL}_2(\mathbb{Z})} f[\alpha]_k \Big) [\gamma]_k \\ &= n^{k/2-1} \sum_{\overline{\alpha} \in M_2(\mathbb{Z},n)/\mathrm{SL}_2(\mathbb{Z})} f[\alpha\gamma]_k, \end{aligned}$$

donde esto último se cumple por la proposición 2.1. Por la identidad del párrafo anterior, podemos conseguir convenientes $\gamma_\alpha \in \mathrm{SL}_2(\mathbb{Z})$ y $\overline{\beta}_\alpha \in M_2(\mathbb{Z}, n)/\mathrm{SL}_2(\mathbb{Z})$ para los cuales se cumple $\alpha\gamma = \gamma_\alpha \beta_\alpha$. De este modo la expresión $T_n(f)[\gamma]_k$ se reduce a

$$\begin{aligned} T_n(f)[\gamma]_k &= n^{k/2-1} \sum_{\overline{\alpha} \in M_2(\mathbb{Z},n)/\mathrm{SL}_2(\mathbb{Z})} f[\gamma_\alpha \beta_\alpha]_k \\ &= n^{k/2-1} \sum_{\overline{\alpha} \in M_2(\mathbb{Z},n)/\mathrm{SL}_2(\mathbb{Z})} f[\beta_\alpha]_k, \end{aligned}$$

donde lo último es válido por la proposición 2.1 y el hecho de que f es una forma modular de peso k respecto a $\mathrm{SL}_2(\mathbb{Z})$. En vista de que $\overline{\beta}_\alpha$ y $\overline{\beta}_{\alpha'}$ son iguales si y solo si $\overline{\alpha}$ y $\overline{\alpha'}$ lo son, concluimos que para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ se verifica

$$T_n(f)[\gamma]_k = T_n(f),$$

lo que es precisamente la condición de modularidad de peso k para $\mathrm{SL}_2(\mathbb{Z})$.

A continuación, verificaremos que $T_m(f)$ es holomorfa en infinito. Para ello, es suficiente mostrar que la q-expansión de $T_m(f)$ no tiene términos con índice negativo.

Iniciemos esta tarea expandiendo la versión amigable de $T_n(f)$. En este caso, tenemos

$$\begin{aligned}
T_n(f) &= n^{k/2-1} \sum_{\substack{ad=n\\a>0}} \sum_{b=0}^{a-1} f \begin{bmatrix} d & b \\ 0 & a \end{bmatrix}_k \\
&= n^{k/2-1} \sum_{\substack{ad=n\\a>0}} \sum_{b=0}^{a-1} n^{k/2} a^{-k} f\Big(\frac{dz+b}{a}\Big) \\
&= \sum_{\substack{ad=n\\a>0}} \sum_{b=0}^{a-1} n^{k-1} a^{-k} \sum_{s=0}^{\infty} \lambda(s) e^{i\frac{2\pi s(dz+b)}{a}}.
\end{aligned}$$

Al agrupar la última expresión conseguimos

$$\begin{aligned}
T_n(f) &= \sum_{\substack{ad=n\\a>0}} \sum_{b=0}^{a-1} n^{k-1} a^{-k} \Big(\lambda(0) + \sum_{s=1}^{\infty} \lambda(s) e^{i\frac{2\pi s(dz+b)}{a}}\Big) \\
&= \sum_{\substack{ad=n\\a>0}} n^{k-1} a^{-k} a\lambda(0) + \sum_{\substack{ad=n\\a>0}} \sum_{b=0}^{a-1} n^{k-1} a^{-k} \sum_{s=1}^{\infty} \lambda(s) e^{i\frac{2\pi s(dz+b)}{a}}\Big) \\
&= \sum_{\substack{ad=n\\a>0}} \Big(\frac{n}{a}\Big)^{k-1} \lambda(0) + \sum_{\substack{ad=n\\a>0}} \sum_{b=0}^{a-1} \sum_{s=1}^{\infty} n^{k-1} a^{-k} \lambda(s) e^{i\frac{2\pi s(dz+b)}{a}}.
\end{aligned}$$

La nueva presentación de $T_n(f)$ nos indica cuáles son las modificaciones adicionales que debemos realizar para cumplir con el cometido. Por ejemplo, si ordenamos la suma interior y luego usamos el lema 3.3 obtenemos

$$\begin{aligned}
T_n(f) &= \sum_{\substack{ad=n\\a>0}} \Big(\frac{n}{a}\Big)^{k-1} \lambda(0) + \sum_{\substack{ad=n\\a>0}} \sum_{s=1}^{\infty} \sum_{b=0}^{a-1} n^{k-1} a^{-k} \lambda(s) e^{i\frac{2\pi s(dz+b)}{a}} \\
&= \sum_{\substack{ad=n\\a>0}} \Big(\frac{n}{a}\Big)^{k-1} \lambda(0) + \sum_{\substack{ad=n\\a>0}} \sum_{\substack{s=1\\a|s}}^{\infty} n^{k-1} a^{-k} a\lambda(s) e^{i\frac{2\pi s dz}{a}} \\
&= \sum_{\substack{ad=n\\a>0}} \Big(\frac{n}{a}\Big)^{k-1} \lambda(0) + \sum_{\substack{ad=n\\a>0}} \Big(\frac{n}{a}\Big)^{k-1} \sum_{r=1}^{\infty} \lambda(ra) q^{dr},
\end{aligned}$$

donde para la última línea hemos reescrito s como ar.

Finalmente, si identificamos dr con m y además usamos $\dfrac{n}{a} = d$, la nueva descripción de $T_n(f)$ está dada por

$$T_n(f) = \sum_{\substack{d|n\\d>0}} d^{k-1} \lambda(0) + \sum_{d|n} d^{k-1} \sum_{\substack{m=1\\d|m}}^{\infty} \lambda\Big(\frac{mn}{d^2}\Big) q^m$$

la que es igual a

$$T_n(f) = \sum_{m=0}^{\infty} \Bigg(\sum_{\substack{d|m,n \\ d>0}} d^{k-1} \lambda\Big(\frac{mn}{d^2}\Big) \Bigg) q^m$$

bajo un reordenamiento de los índices. Por lo tanto, hemos probado que $T_n(f)$ es holomorfa en infinito. $\square$

Observemos que $T_n^{[k]}$ es también un operador lineal para $S_k(\mathrm{SL}_2(\mathbb{Z}))$, ya que el valor de $\lim\limits_{\mathrm{Im}(z)\to\infty} T_n^{[k]}(f)$ es 0 cuando f es un elemento de $S_k(\mathrm{SL}_2(\mathbb{Z}))$. El siguiente resultado manifiesta que el operador $T_n^{[k]}$ conmuta condicionalmente.

Proposición 3.5. *Para cualesquiera m y n coprimos se verifica*

$$T_n^{[k]} T_m^{[k]} = T_{mn}^{[k]} = T_m^{[k]} T_n^{[k]}.$$

Prueba. Sea $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ con q-expansión igual a $\sum\limits_{s=0}^{\infty} a(s)q^s$. Por el teorema 3.4, tenemos $T_n(f) = \sum\limits_{s=0}^{\infty} b(s)q^s$ donde cada $b(s)$ es igual a $\sum\limits_{d|n,s} d^{k-1} a\Big(\dfrac{ns}{d^2}\Big)$. Nuevamente, por el teorema 3.4, se cumple $T_m T_n(f) = \sum\limits_{s=0}^{\infty} c(s)q^s$ donde en este caso el valor de $c(s)$ está dado por

$$c(s) = \sum_{e|m,s} e^{k-1} b\Big(\frac{ms}{e^2}\Big) = \sum_{e|m,s} e^{k-1} \sum_{d|n,\frac{ms}{e^2}} d^{k-1} a\Big(\frac{mns}{d^2e^2}\Big).$$

Como m y n son coprimos, la suma $\sum\limits_{d|n,\frac{ms}{e^2}} d^{k-1} a\Big(\dfrac{mns}{d^2e^2}\Big)$ es en realidad una suma que recorre los divisores de n y $\dfrac{s}{e}$, pues n y $\dfrac{m}{e}$ también son coprimos. Con ello obtenemos

$$\begin{aligned} c(s) &= \sum_{e|m,s} e^{k-1} \sum_{d|n,\frac{s}{e}} d^{k-1} a\Big(\frac{mns}{d^2e^2}\Big) \\ &= \sum_{e|m,s} \sum_{d|n,s} (ed)^{k-1} a\Big(\frac{mns}{d^2e^2}\Big) \quad (\text{pues } (m,n)=1). \end{aligned}$$

Dado que el producto ed de la suma del párrafo anterior recorre todos los divisores de mn y s, podemos reescribir $c(s)$ cual

$$c(s) = \sum_{h|mn,s} h^{k-1} a\Big(\frac{mns}{h^2}\Big).$$

Por lo tanto, se cumple $T_m T_n = T_{mn}$ siempre y cuando m y n sean coprimos. $\square$

Es realmente sorprendente que el operador $T_n^{[k]}$ conmute condicionalmente. No obstante, el enésimo operador de Hecke conmuta sin condiciones. En lo queda de esta sección confirmaremos dicha propiedad.

Lema 3.6. *Sea p primo y $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$. Para toda potencia $s > 0$ se tiene*

$$T_{p^s}(T_p(f)) = T_{p^{s+1}}(f) + p^{k-1} T_{p^{s-1}}(f).$$

Prueba. Al desarrollar al detalle $T_{p^s}(T_p(f))$ obtenemos

$$\begin{aligned}
T_{p^s}(T_p(f)) &= p^{s(\frac{k}{2}-1)} \sum_{j=0}^{s} \sum_{b=0}^{p^j-1} T_p(f) \begin{bmatrix} p^{s-j} & b \\ 0 & p^j \end{bmatrix}_k \\
&= p^{s(\frac{k}{2}-1)} \sum_{j=0}^{s} \sum_{b=0}^{p^j-1} \left(p^{\frac{k}{2}-1} f \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}_k + p^{\frac{k}{2}-1} \sum_{c=0}^{p-1} f \begin{bmatrix} 1 & c \\ 0 & p \end{bmatrix}_k \right) \begin{bmatrix} p^{s-j} & b \\ 0 & p^j \end{bmatrix}_k \\
&= p^{(s+1)(\frac{k}{2}-1)} \sum_{j=0}^{s} \sum_{b=0}^{p^j-1} \left(f \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}_k + \sum_{c=0}^{p-1} f \begin{bmatrix} 1 & c \\ 0 & p \end{bmatrix}_k \right) \begin{bmatrix} p^{s-j} & b \\ 0 & p^j \end{bmatrix}_k \\
&= p^{(s+1)(\frac{k}{2}-1)} \sum_{j=0}^{s} \sum_{b=0}^{p^j-1} \left(f \begin{bmatrix} p^{s+1-j} & bp \\ 0 & p^j \end{bmatrix}_k + \sum_{c=0}^{p-1} f \begin{bmatrix} p^{s-j} & b + p^j c \\ 0 & p^{j+1} \end{bmatrix}_k \right).
\end{aligned}$$

Tras algunas modificaciones elementales, la primera parte de la última suma puede escribirse cual

$$p^{(s+1)(\frac{k}{2}-1)} \left(f \begin{bmatrix} p^{s+1} & 0 \\ 0 & 1 \end{bmatrix}_k + \sum_{j=1}^{s} \sum_{b=0}^{p^j-1} f \begin{bmatrix} p^{s+1-j} & bp \\ 0 & p^j \end{bmatrix}_k \right)$$

y la segunda como

$$p^{(s+1)(\frac{k}{2}-1)} \left(\sum_{j=0}^{s} \sum_{c=0}^{p-1} \sum_{b=0}^{p^j-1} f \begin{bmatrix} p^{s-j} & b + p^j c \\ 0 & p^{j+1} \end{bmatrix}_k \right).$$

Con respecto a esta segunda parte, las primeras sumas internas se pueden combinar y arrojan

$$p^{(s+1)(\frac{k}{2}-1)} \left(\sum_{j=0}^{s} \sum_{b'=0}^{p^{j+1}-1} f \begin{bmatrix} p^{s-j} & b' \\ 0 & p^{j+1} \end{bmatrix}_k \right).$$

Similarmente, podemos alterar la primera parte. De este modo, la doble suma interna se escribe como

$$p^{(s+1)(\frac{k}{2}-1)}f\begin{bmatrix} p^{s+1} & 0 \\ 0 & 1 \end{bmatrix}_k + p^{k-1}p^{(s-1)(\frac{k}{2}-1)}\sum_{j=1}^{s}\sum_{b'=0}^{p^{s-1}-1} f\begin{bmatrix} p^{s-j} & b' \\ 0 & p^{j-1} \end{bmatrix}_k,$$

o lo que es lo mismo cual

$$p^{(s+1)(\frac{k}{2}-1)}f\begin{bmatrix} p^{s+1} & 0 \\ 0 & 1 \end{bmatrix}_k + p^{k-1}T_{p^{s-1}}(f).$$

Al reunir todos nuestros hallazgos obtenemos, en resumen,

$$T_{p^s}(T_p(f)) = T_{p^{s+1}}(f) + p^{k-1}T_{p^{s-1}}(f). \qquad \square$$

Notemos que en particular se cumple

$$T_{p^2}^{[k]} = (T_p^{[k]})^2 - p^{k-1}T_1^{[k]},$$

lo cual indica como podemos describir de manera recursiva cualquier $T_{p^{s+1}}$ con $s \geq 0$. En particular, T_{p^s} podrá expresarse como un polinomio de T_p.

Teorema 3.7. *Sea p primo. Para cualesquiera enteros positivos m y n se cumple*

$$T_{p^m}^{[k]}T_{p^n}^{[k]} = T_{p^n}^{[k]}T_{p^m}^{[k]}.$$

Prueba. Sin pérdida de generalidad asumamos $m \leq n$ y que el peso de los operadores de Hecke en discusión es k. Usemos inducción sobre n para probar esta afirmación. El caso base $n = 1$ es claro. Por cual, asumamos que para algún entero $h \geq 1$ se satisface la identidad $T_{p^m}T_{p^n} = T_{p^n}T_{p^m}$ siempre y cuando se cumpla $m \leq n \leq h$.

Ahora, consideremos $T_{p^m}T_{p^{h+1}}$ con la condición $m \leq h+1$. Si se cumple $m = h+1$, la afirmación es clara. Si por el contrario se cumple $m \leq h$, de la hipótesis inductiva y el lema 3.6 concluimos

$$T_{p^m}T_{p^{h+1}} = T_{p^m}(T_{p^h}T_p - p^{k-1}T_{p^h}) = (T_{p^h}T_p - p^{k-1}T_{p^h})T_{p^m} = T_{p^{h+1}}T_{p^m}. \qquad \square$$

Corolario 3.8. *Para cualesquiera enteros positivos m y n se cumple*

$$T_n^{[k]} T_m^{[k]} = T_m^{[k]} T_n^{[k]}.$$

Es decir, los operadores de Hecke conmutan. $\square$

La conmutatividad de los operadores Hecke será de suma ayuda para atacar parte de la conjetura de Ramanujan, la cual discutiremos de inmediato.

3.2 La conjetura de Ramanujan

En esta sección probaremos un fragmento de la conjetura de Ramanujan, la cual fue publicada en el año 1916 en el artículo *On certain arithmetical functions* [17].

Sea $\sum_{n=1}^{\infty} a_n q^n$ la q-expansión de la forma cuspidal Δ. La **función τ de Ramanujan** está definida como los coeficientes de la q-expansión de Δ. Explícitamente, τ es la función aritmética dada por

$$\begin{aligned} \tau : \mathbb{N} &\to \mathbb{C} \\ n &\mapsto a_n. \end{aligned}$$

El siguiente teorema muestra la naturaleza aritmética de ciertas formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$.

Teorema 3.9. *Los valores de la función τ son enteros.*

Prueba. Escribamos $A = \sum_{n=1}^{\infty} \sigma_3(n) q^n$ y $B = \sum_{n=1}^{\infty} \sigma_5(n) q^n$. Ello nos permite obtener

$$\begin{aligned} E_4^3 - E_6^2 &= (1 + 240A)^3 - (1 - 504B)^2 \\ &= 3(240A) + 3(240A)^2 + (240A)^3 + 2(504)B - (504B)^2. \end{aligned}$$

Como se cumple $3(240)^2 \equiv (240)^3 \equiv (504)^2 \equiv 0 \mod 1728$, es suficiente verificar que los coeficientes de $5A + 7B$ son múltiplos de 12. En efecto, por definición tenemos que el coeficiente de q^n es

$$5\sigma_3(n) + 7\sigma_5(n) = \sum_{d|n} (5d^3 + 7d^5).$$

Cálculos sencillos nos permiten deducir que para todo $d \in \mathbb{Z}$ se cumplen las congruencias

$$d^3(5+7d^2) \equiv d^3(d^2-1) \equiv 0 \mod 3 \quad \text{y} \quad d^3(5+7d^2) \equiv d^3(1-d^2) \equiv 0 \mod 4.$$

Por lo tanto, todos los valores de τ son enteros. $\square$

La conjetura de Ramanujan sostiene que la función τ satisface las siguiente tres propiedades.

- Para cualesquiera m y n coprimos positivos se cumple $\tau(mn) = \tau(m)\tau(n)$. Es decir, la función τ es multiplicativa.
- Para todo p primo y a entero positivo se cumple $\tau(p^{a+1}) = \tau(p)\tau(p^a) - p^{11}\tau(p^{a-1})$.
- Para todo p se cumple $|\tau(p)| \leq 2p^{11/2}$.

En el 1917, un año después de la publicación de Ramanujan, Mordell resolvió las dos primeras partes de la conjetura en el artículo *On Mr. Ramanujan's empirical expansions of modular functions* [14]. Sin embargo, no fue hasta 1974 cuando Deligne probó las conjecturas de Weil en *La conjecture de Weil: I* [5], prueba que proporcionó de manera indirecta la solución de última parte de la conjetura de Ramanujan.

Verificar que la función τ no es completamente multiplicativa es fácil, ya que la q-expansión de Δ está dada por

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + 84480q^8 + \dots$$

No obstante, el siguiente teorema nos brinda una fórmula para el producto de dos valores de la función τ.

Teorema 3.10. *Para cualesquiera números enteros positivos m y n se cumple*

$$\tau(m)\tau(n) = \sum_{d|m,n} d^{11}\tau\left(\frac{mn}{d^2}\right).$$

Prueba. Por el teorema 3.4, $T_m(\Delta)$ es una forma modular de peso 12 respecto a $\mathrm{SL}_2(\mathbb{Z})$. Más aún, es una forma cuspidal de peso 12 respecto a $\mathrm{SL}_2(\mathbb{Z})$. Por tal motivo, se cumple

$$T_m(\Delta) = c_m\Delta$$

para algún $c_m \in \mathbb{C}$, ya que por el corolario 2.22 la dimensión de $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ es 1. Esto implica que los coeficientes de las q-expansiones de $T_m(\Delta)$ y $c_m\Delta$ son iguales.

En consecuencia, por el teorema 3.4 para todo n tenemos

$$\sum_{d|m,n} d^{11}\tau\left(\frac{mn}{d^2}\right) = c_m\tau(n).$$

Al reemplazar $n = 1$, verificamos que se cumple $c_m = \tau(m)$ para todo m. Con esto queda establecido el teorema. □

Corolario 3.11. *Las dos primeras partes de la conjetura de Ramanujan son ciertas.*

Prueba. Ambas conjecturas son consecuencia directa del teorema anterior. Discutamos la primera, si m y n son coprimos positivos, por el teorema 3.10 inmediatamente tenemos $\tau(m)\tau(n) = \tau(mn)$.

Ahora, probemos la segunda conjectura. Sea p un primo y a un entero positvo. Por el teorema 3.10, el producto de $\tau(p)$ con $\tau(p^a)$ es igual a

$$\tau(p)\tau(p^a) = \tau(p^{a+1}) + p^{11}\tau(p^{a-1}),$$

lo cual prueba la segunda conjectura. □

En este trabajo no probaremos la última parte de la conjetura de Ramanujan pues escapa a nuestras posibilidades. Sin embargo, probaremos un resultado que logrará acercarnos de la veracidad de ella.

Lema 3.12. *Sea* Γ *un subgrupo de congruencia. Si* $f : \mathbb{H} \to \mathbb{C}$ *es una función que satisface la condición de modularidad de peso* k *para* Γ, *entonces la función* $\mathrm{Im}(z)^{k/2}|f(z)|$ *es* Γ*-invariante.*

Prueba. Sea $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ un elemento de Γ. Claramente, se cumple

$$\begin{aligned}\mathrm{Im}(\gamma z)^{k/2}|f(\gamma z)| &= \frac{\mathrm{Im}(z)^{k/2}}{|cz+d|^k}|cz+d|^k|f(z)| \\ &= \mathrm{Im}(z)^{k/2}|f(z)|.\end{aligned}$$

De este modo, hemos verificado que la función $\mathrm{Im}(z)^{k/2}|f(z)|$ es Γ-invariante. □

El siguiente teorema probado por Hecke genera una cota para $|\tau(p)|$ mucho más débil que la conjeturada por Ramanujan.

Teorema 3.13. *Sea f un elemento de $S_k(\mathrm{SL}_2(\mathbb{Z}))$ con q-expansión dada por $\sum_{n=1}^{\infty} a_n q^n$. Entonces, existe un real $M > 0$ con el que se cumple $|a_n| \leq Mn^{k/2}$ para todo n. En particular, la función τ obedece $\tau(n) = O(n^6)$.*

Prueba. Como f es una forma cuspidal respecto a $\mathrm{SL}_2(\mathbb{Z})$, para todo $C > 0$ existe un algún $M'' > 0$ tal que se cumple

$$|f(z)| \leq M'' e^{-2\pi \mathrm{Im}(z)}$$

en la región $D = \{z \in F_{\mathrm{SL}_2(\mathbb{Z})} : \mathrm{Im}(z) > C\}$. Esto significa que $\mathrm{Im}(z)^{k/2}|f(z)|$ es acotado en la región modular. Es decir, existe $M' > 0$ tal que para todo $z \in F_{\mathrm{SL}_2(\mathbb{Z})}$ se cumple

$$\mathrm{Im}(z)^{k/2}|f(z)| \leq M'.$$

Más aún, ello se verifica para todo $z \in \mathbb{H}$, ya que $\mathrm{Im}(z)^{k/2}|f(z)|$ es $\mathrm{SL}_2(\mathbb{Z})$-invariante debido a lema 3.12.

En el teorema 2.5 se presento la fórmula

$$a_n = \int_0^1 f(x+iy)e^{-2\pi i n(x+iy)}dx,$$

donde y es un número real entre 0 y 1. Si empleamos la estimación de $\mathrm{Im}(z)^{k/2}|f(z)|$ en la integral obtenemos

$$|a_n| \leq M' y^{-k/2} e^{2\pi n y}$$

para todo $y > 0$. Por lo tanto, al reemplazar $y = 1/n$ conseguimos

$$|a_n| \leq Mn^{k/2},$$

donde M es real positivo. □

Capítulo 4

Formas modulares II

En este capítulo extenderemos la definición de formas modulares para cualquier subgrupo de congruencia. Esencialmente, replicaremos todo aquello que hemos hecho para las formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$. El principal material de consulta para este capítulo es [6].

4.1 Formas modulares de niveles altos

Generalizar una noción siempre nos obliga justificar el porqué de su utilidad y ser capaces de mostrar que existe armonía con las ideas que la anteceden. En esta sección, describiremos las formas modulares respecto a un subgrupo de congruencia arbitrario (o formas modulares de niveles altos), los cuales extendarán la definición de forma modular respecto a $\mathrm{SL}_2(\mathbb{Z})$.

Sea Γ un subgrupo de congruencia. Una función holomorfa $f : \mathbb{H} \to \mathbb{C}$ es una **forma modular** de peso k con respecto a Γ si cumple la condición de modularidad de peso k para Γ y si además $f[\gamma]_k$ es holomorfa en infinito para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. En particular, diremos que f es una forma cuspidal si cumple

$$\lim_{\mathrm{Im}(z)\to\infty} f[\gamma]_k(z) = 0$$

para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Notemos que la verificación de la holomorfía en infinito de $f[\gamma]_k$ se reduce a simplemente verificarla en aquellos γ elementos de algún subconjunto transversal de $\Gamma\backslash\mathrm{SL}_2(\mathbb{Z})$. Además, es evidente que esta definición es compatible con aquella dada en el capítulo 2.

Ejemplo 4.1. Sean Γ y Γ' subgrupos de congruencia con $\Gamma' \subset \Gamma$. Toda forma modular de peso k respecto a Γ es una forma modular de peso k respecto a Γ'.

Ejemplo 4.2. Sean Γ y Γ' subgrupos de congruencia con $\Gamma' \subset \Gamma$ y $\{\gamma_1, \ldots, \gamma_n\}$ un subconjunto transversal de $\Gamma' \backslash \Gamma$. Si f es un elemento de $M_k(\Gamma')$, entonces $\sum_{i=1}^{n} f[\gamma_i]_k$ es un elemento de $M_k(\Gamma)$ y $\prod_{i=1}^{n} f[\gamma_i]_k$ es un elemento de $M_{kn}(\Gamma)$.

Sea Γ un subgrupo de congruencia. Al conjunto de las formas modulares de peso k respecto a Γ lo denotemos por $M_k(\Gamma)$ y al de las formas cuspidales por $S_k(\Gamma)$.

Proposición 4.3. *Para cualquier subgrupo de congruencia* Γ *se cumple lo siguiente.*

a. Los conjuntos $M_k(\Gamma)$ *y* $S_{k_1}(\Gamma)$ *son* $\mathbb{C}$*-espacios vectoriales.*

b. El producto de dos formas modulares respecto a Γ *es también una forma modular respecto a* Γ *de peso igual a la suma de los pesos. Más aún, si uno de ellos es una forma cuspidal, entonces el producto es también una forma cuspidal.*

Prueba. Las pruebas son idénticas a las de la proposición 2.8, por lo cual, se dejan como ejercicio para el lector. ☐

Para exhibir ejemplos adicionales de formas modulares con respecto a subgrupos de congruencia arbitrarios es necesario retomar nuestra definición de G_k.

Sea $k \geq 3$ un entero y g un par en $\mathbb{Z}^2$. Una **serie de Eisenstein** $G_{k,g}(z)$ (con $z \in \mathbb{H}$) de peso k para $\Gamma(N)$ es la subserie de $G_k(z)$ dada por

$$G_{k,g}(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\equiv g \ (\text{mód}\, N) \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^k}.$$

Teorema 4.4. *Toda serie de Eisenstein de peso* k *para* $\Gamma(N)$ *es una forma modular de peso* k *respecto a* $\Gamma(N)$.

Prueba. Como G_k converge uniformemente en compactos de $\mathbb{H}$, cualquier subserie de ella también lo hace. En particular, toda serie de Eisenstein para $\Gamma(N)$ es holomorfa en $\mathbb{H}$. Por esta razón, debemos ocuparnos apenas de las otras dos propiedades que aparecen en la definición.

Sea g un elemento de $\mathbb{Z}^2$ y $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ un elemento de $\Gamma(N)$. Notemos que el automorfismo de $\mathbb{Z}^2$ dado por $(m,n) \mapsto (m,n)\gamma$ define una permutación sobre el conjunto de índices de $G_{k,g}$. Por lo cual, al desarrollar la expresión $G_{k,g}(\gamma z)$, tenemos

$$\begin{aligned} G_{k,g}(\gamma z) &= \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\equiv g\,(\text{mód}\,N) \\ (m,n)\neq(0,0)}} \frac{(cz+d)^k}{((ma+nc)z+mb+nd)^k} \\ &= (cz+d)^k \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\equiv g\,(\text{mód}\,N) \\ (m,n)\neq(0,0)}} \frac{1}{((ma+nc)z+mb+nd)^k} \\ &= (cz+d)^k G_{k,g}(z). \end{aligned}$$

De este modo, hemos verificado que $G_{k,g}$ satisface la condición de modularidad de peso k para $\Gamma(N)$.

De lo desarrollado el párrafo anterior, concluimos la identidad

$$G_{k,g}[\gamma']_k = G_{k,g\gamma'}$$

para todo $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$. De este modo, tenemos dos opciones para el valor de

$$\lim_{\mathrm{Im}(z)\to\infty} G_{k,g}[\gamma']_k(z).$$

Vale 0 si $g_1 \not\equiv 0\,(\text{mód}\,N)$; de lo contrario vale $\displaystyle\sum_{n\equiv g_2\,(\text{mód}\,N)} \frac{1}{n^k}$. No obstante, en ambos casos se deduce que $G_{k,g}[\gamma']_k$ es holomorfa en infinito para todo $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$. De este modo, las series de Eisenstein de peso k para $\Gamma(N)$ son formas modulares de peso k respecto a $\Gamma(N)$. $\square$

El siguiente teorema nos indica que ciertas funciones holomorfas invariantes bajo un subgrupo de congruencia arbitrario tienen crecimiento asintóticamente moderado. Más aún, una consecuencia directa de este resultado, la cual presentamos como corolario, brinda una manera alternativa para verificar si una función holomorfa invariante bajo un subgrupo de congruencia arbitrario es una forma modular.

Teorema 4.5. *Sea Γ un subgrupo de congruencia de nivel N y $f : \mathbb{H} \to \mathbb{C}$ una función holomorfa que satisface la condición de modularidad de peso k para Γ. Si f es holo-*

morfa en infinito y todos sus coeficientes de índice positivo en su q_N-expansión (dada por $\sum_{n=0}^{\infty} a_n q_N^n$) satisfacen $|a_n| \leq Kn^r$ para constantes positivas K y r, entonces existen otras constantes K_1, K_2 y C, también positivas, con las cuales se cumple

$$|f(z)| \leq K_1 + \frac{K_2}{\mathrm{Im}(z)^r}$$

siempre que z caiga dentro de la región $\mathrm{Im}(z) > C$.

Prueba. Como la convergencia de f asociada su q-expansión es normal, se cumple

$$|f(z)| \leq |a_0| + K \sum_{n=1}^{\infty} n^r e^{\frac{-2\pi n \mathrm{Im}(z)}{N}}.$$

Consideremos $g(t) = t^r e^{-\frac{2\pi t \mathrm{Im}(z)}{N}}$, la versión continua de $n^r e^{\frac{-2\pi n \mathrm{Im}(z)}{N}}$ en $[0, +\infty)$, la cual

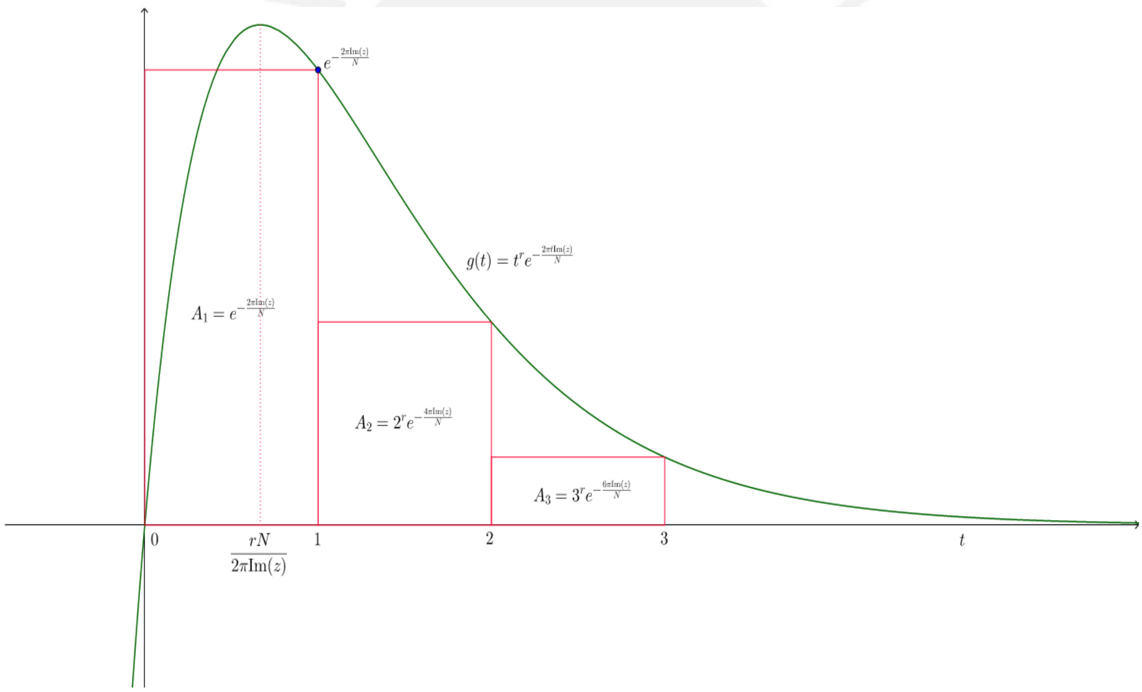

Figura 4.1: gráfica de $g(t)$.

crece monótonamente en $\left[0, \frac{rN}{2\pi \mathrm{Im}(z)}\right)$ y decrece de igual manera en $\left[\frac{rN}{2\pi \mathrm{Im}(z)}, +\infty\right)$. Dado que existe una región $\mathrm{Im}(z) > C$, con $C > 0$, para la cual las restricciones

$$\frac{rN}{2\pi \mathrm{Im}(z)} < 1 \quad \text{y} \quad \mathrm{Im}(z)^r e^{-\frac{2\pi \mathrm{Im}(z)}{N}} \leq 1$$

se verifican, la figura 4.1 muestra que en la región $\mathrm{Im}(z) > C$ se cumple

$$\sum_{n=2}^{\infty} A_n \leq \int_1^{\infty} g(t)dt,$$

acá A_n es el área del rectángulo de altura $g(n)$ y base 1. Por lo tanto, para convenientes constantes positvas K_1 y K_2', en la región $\mathrm{Im}(z) > C$ se cumple

$$|f(z)| \leq K_1 + K_2'\Big(\int_0^{\infty} g(t)dt + \frac{1}{\mathrm{Im}(z)^r}\Big).$$

Al aplicar el cambio de variable $s = \dfrac{2\pi \mathrm{Im}(z)t}{N}$ en la última integral obtenemos

$$|f(z)| \leq K_1 + K_2'\Big(\Big(\frac{N}{2\pi}\Big)^r \frac{1}{\mathrm{Im}(z)^{r+1}} \int_0^{\infty} s^r e^{-s} ds + \frac{1}{\mathrm{Im}(z)^r}\Big).$$

Para el remate usamos el hecho de que la función gamma está bien definida en todos reales positvos. Por lo tanto, una simple estimación acompañada de una constante positiva K_2 deviene en

$$|f(z)| \leq K_1 + \frac{K_2}{\mathrm{Im}(z)^r}$$

para todo z dentro de la región $\mathrm{Im}(z) > C$. □

Corolario 4.6. *Si Γ y f son como en el lema anterior, entonces f es un elemento de $M_k(\Gamma)$.*

Prueba. Por la proposición 2.6, es suficiente verificar que se cumple

$$\lim_{\mathrm{Im}(z)\to\infty} q_N f[\alpha]_k(z) = 0$$

para todo $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, lo cual es evidente por el lema anterior. □

La definición de formas modulares con respecto un subgrupo de congruencia arbitrario para nada insinúa que la dimensión de los espacios vectoriales correspendientes sea finita. Por está razón, en lo queda de esta subsección nos dedicaremos a probar que los espacios de formas modulares son finito dimensionales.

Proposición 4.7. *Sea k un entero impar y Γ un subgrupo de congruencia que contiene a $-I$. Entonces, el espacio vectorial $M_k(\Gamma)$ es trivial.*

Prueba. La prueba es idéntica a la de la proposición 2.9. □

El siguiente resultado nos enseñará, en su prueba, una técnica usual para probar que los espacios vectoriales formados por formas modulares con respecto un subgrupo de congruencia arbitrario son finito dimensionales.

Proposición 4.8. *Los espacios vectoriales $M_k(\Gamma)$ con $k < 0$ son triviales.*

Prueba. Sea f un elemento de $M_k(\Gamma)$. Por el ejemplo 4.2, la función $\prod_{\overline{\gamma_i}\in \mathrm{SL}_2(\mathbb{Z})/\Gamma} f[\gamma_i]_k$ es una forma modular de peso negativo respecto a $\mathrm{SL}_2(\mathbb{Z})$. Es decir, es idénticamente nula en $\mathbb{H}$ debido a la parte *a*) del corolario 2.18. En virtud del lema 2.16, deducimos que algún $f[\gamma_i]_k$ es idénticamente nulo en $\mathbb{H}$, lo cual implica que f también lo es. $\square$

Todas las formas modulares respecto a un subgrupo de congruencia llevan consigo una q-expansión. De hecho, sus imágenes vía un operador k-peso asociado a los elementos de $\mathrm{SL}_2(\mathbb{Z})$ también tienen una q-expansión. Por los requisitos dados en su definición, el orden de las formas modulares en infinito es no negativo. Más aún, este no puede ser arbitrariamente grande. El siguiente teorema nos brinda una cota para determinar cuándo una forma modular respecto a un subgrupo de congruencia arbitrario es idénticamente nula en $\mathbb{H}$.

Lema 4.9. *Sea f un elemento de $M_k(\Gamma)$ donde Γ es de nivel N y r es el índice de subgrupo* $\mathrm{SL}_2(\mathbb{Z})/\Gamma$. *Si f satisface la desigualdad*

$$\sum_{\overline{\gamma_i}\in \mathrm{SL}_2(\mathbb{Z})/\Gamma} \mathrm{ord}_{\infty i}(f[\gamma_i]_k, N) \geq \left\lfloor \frac{kr}{12} \right\rfloor N + N,$$

entonces f es idénticamente nula en $\mathbb{H}$.

Prueba. Por el ejemplo 4.2, la función $F = \prod_{\overline{\gamma_i}\in \mathrm{SL}_2(\mathbb{Z})/\Gamma} f[\gamma_i]_k$ es una forma modular de peso kr respecto a $\mathrm{SL}_2(\mathbb{Z})$. Como cada $f[\gamma_i]_k$ tiene una q_N-expansión dada por

$$f[\gamma_i]_k = a_{n_i}^{(i)} q_N^{n_i} + \dots.$$

la q_N-expansión de F está dada por

$$F(z) = a_{n_1}^{(1)} \dots a_{n_r}^{(r)} q_N^{n_1+\dots+n_r} + \dots$$

De este modo tenemos $\sum_{i=1}^{r} n_i = N\mathrm{ord}_\infty(F)$, lo cual implica $\mathrm{ord}_\infty(F) \geq \left\lfloor \frac{kr}{12} \right\rfloor + 1$. La fórmula $k/12$ nos asegura luego que f es idénticamente nula en $\mathbb{H}$. $\square$

El siguiente teorema establece que los espacios de formas modulares respecto a subgrupo congruencia arbitrario no son mucho más grandes que los espacios de formas modulares respecto a $\mathrm{SL}_2(\mathbb{Z})$.

Teorema 4.10. *El espacio vectorial $M_k(\Gamma)$ es finito dimensional.*

Prueba. Sea N el nivel de Γ. Consideremos la transformación lineal

$$\begin{aligned} M_k(\Gamma) &\to \mathbb{C}^{r+1} \\ \sum_{n=0}^{\infty} a_n q_N^n &\mapsto (a_0, \dots, a_r), \end{aligned}$$

donde r es igual $\left\lfloor \frac{k[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]}{12} \right\rfloor N + N$. Por el lema 4.9, esta transformación lineal es inyectiva. De esto concluimos la cota $\dim M_k(\Gamma) \le r+1$. $\square$

4.2 El teorema de los cuatro cuadrados

En esta sección sustentaremos el beneficio de extender la noción de formas modulares a subgrupos de congruencia arbitrarios. Aparte, el resultado que exhibiremos ilustra nuevamente el carácter aritmético que llevan intrínsecas las formas modulares. Para esto saldaremos cuentas respecto a E_2; específicamente, mostraremos que es casi una forma modular de peso 2 respecto a $\mathrm{SL}_2(\mathbb{Z})$.

Proposición 4.11. *La serie de Eisenstein E_2 tal como es presentada en el ejemplo 2.14 es holomorfa en $\mathbb{H}$ y en infinito.*

Prueba. Sea K un subconjunto compacto de $\mathbb{H}$. A todas luces, existe un real positvo $r < 1$ tal que para todo $z \in K$ se cumple $\mathrm{Im}(z) > r$. Por consiguiente, E_2 converge uniformente en K pues se cumple $\sum_{n=1}^{\infty} \sigma_1(n)|q|^n \le \sum_{n=1}^{\infty} n^2 r^n$ donde esta última converge. De este modo, hemos probado que E_2 es holomorfa tanto en $\mathbb{H}$ como en infinito. $\square$

La siguiente proposición dada por Hurwitz muestra una nueva y enriquecida presentación para E_2.

Proposición 4.12. *La serie E_2 tiene una expansión absolutamente convergente dada por*

$$E_2(z) = 1 + \frac{1}{2\zeta(2)} \sum_{m \in \mathbb{Z}^*} \sum_{n \in \mathbb{Z}} \left(\frac{1}{(mz+n)^2} - \frac{1}{(mz+n-1)(mz+n)} \right),$$

Prueba. La serie E_2 debería estar dada por

$$E_2(z) = 1 + \frac{1}{2\zeta(2)} \sum_{m\in\mathbb{Z}^*} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^2}$$

la cual no converge absolutamente (a diferencia de su presentación modifica). Por dicho motivo, debemos justificar por qué el sumando extra dentro de la suma doble es indispensable.

Heurísticamente, al desarrollar la serie $\sum_{m\in\mathbb{Z}^*} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n-1)(mz+n)}$ conseguimos

$$\sum_{m\in\mathbb{Z}^*} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n-1)(mz+n)} = \sum_{m\in\mathbb{Z}^*} \sum_{n\in\mathbb{Z}} \left(\frac{1}{mz+n-1} - \frac{1}{mz+n} \right).$$

Notemos que la suma interior es una serie telescópica y converge a 0. De este modo, verificamos que la serie doble converge a 0. Por lo tanto, al agregar y quitar el sumando extra a la suma doble de E_2 junto con el reescalamiento de $\frac{1}{2\zeta(2)}$ obtenemos la expansión requerida.

No obstante, ahora si la convergencia absoluta de esta nueva expansión se sostiene por los mismos argumentos presentados al inicio de la prueba del teorema 2.10. $\square$

El siguiente lema técnico es un ejemplo de comó el cambio de orden en una serie doble no se puede dar de manera indiscriminada.

Lema 4.13. *Para todo $z \in \mathbb{H}$ se cumple*

$$\sum_{n\in\mathbb{Z}} \sum_{m\in\mathbb{Z}^*} \left(\frac{1}{mz+n-1} - \frac{1}{mz+n} \right) = -\frac{2\pi i}{z}.$$

Prueba. El cálculo del valor de la serie doble deviene de

$$\begin{aligned}
\sum_{n\in\mathbb{Z}} \sum_{m\in\mathbb{Z}^*} \left(\frac{1}{mz+n-1} - \frac{1}{mz+n} \right) &= \lim_{N\to\infty} \sum_{n=-N}^{N} \sum_{m\in\mathbb{Z}^*} \left(\frac{1}{mz+n-1} - \frac{1}{mz+n} \right) \\
&= \lim_{N\to\infty} \sum_{m\in\mathbb{Z}^*} \sum_{n=-N}^{N-1} \left(\frac{1}{mz+n-1} - \frac{1}{mz+n} \right) \\
&= \lim_{N\to\infty} \sum_{m\in\mathbb{Z}^*} \left(\frac{1}{mz-N} - \frac{1}{mz+N} \right) \\
&= \lim_{N\to\infty} \frac{1}{z} \sum_{m\in\mathbb{Z}^*} \left(\frac{1}{m-N/z} + \frac{1}{-m-N/z} \right).
\end{aligned}$$

Este último límite es equivalente a

$$\lim_{N\to\infty} \frac{1}{z}\frac{2}{N/z} - \frac{1}{z}\frac{2}{N/z} + \frac{1}{z}\sum_{m\in\mathbb{Z}^*}\left(\frac{1}{m-N/z} + \frac{1}{-m-N/z}\right)$$

que a la vez es igual a

$$\lim_{N\to\infty} \frac{1}{N} + \frac{1}{z}\sum_{m\in\mathbb{Z}}\left(\frac{1}{m-N/z} + \frac{1}{-m-N/z}\right).$$

Por la proposición III.3.17 de [7] tenemos

$$\sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}^*}\left(\frac{1}{mz+n-1} - \frac{1}{mz+n}\right) = \lim_{N\to\infty} \frac{1}{N} + \frac{2\pi}{z}\cot\left(-\frac{\pi N}{z}\right).$$

De este modo, al usar la fórmula de Euler conseguimos

$$\sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}^*}\left(\frac{1}{mz+n-1} - \frac{1}{mz+n}\right) = \lim_{N\to\infty} \frac{1}{N} + \frac{2\pi i}{z}\left(\frac{e^{-2\pi i N/z}+1}{e^{-2\pi i N/z}-1}\right).$$

Por lo tanto, al evaluar el límite comprobamos la afirmación. □

El siguiente resultado muestra por que E_2 en su "forma cándida" es una "casi forma modular de peso 2 respecto a $\mathrm{SL}_2(\mathbb{Z})$".

Teorema 4.14. *La serie E_2 satisface las siguientes identidades:*

$$E_2[T]_2(z) = E_2(z),$$
$$E_2[S]_2(z) = E_2(z) - \frac{6i}{\pi z}.$$

Prueba. La primera identidad es clara: para comprobarla basta revisar la q-expansión de E_2. Por ello, apenas verificaremos la segunda. Por la definición $E_2[S]_2(z)$ tenemos

$$\begin{aligned} E_2[S]_2(z) &= z^{-2}E_2\left(\frac{-1}{z}\right) \\ &= z^{-2} + \frac{1}{2\zeta(2)}\sum_{m\in\mathbb{Z}^*}\sum_{n\in\mathbb{Z}}\frac{z^{-2}}{\left(-\frac{m}{z}+n\right)^2} \\ &= z^{-2} + \frac{1}{2\zeta(2)}\sum_{m\in\mathbb{Z}^*}\sum_{n\in\mathbb{Z}}\frac{1}{(nz-m)^2}, \end{aligned}$$

que luego de un reordenamiento y una reindexación lleva a

$$\begin{aligned}
E_2[S]_2(z) &= 1 + \frac{2\zeta(2)}{2\zeta(2)z^2} + \frac{1}{2\zeta(2)} \sum_{m\in\mathbb{Z}^*} \sum_{n\in\mathbb{Z}^*} \frac{1}{(nz-m)^2} \\
&= 1 + \frac{1}{2\zeta(2)} \sum_{m\in\mathbb{Z}} \sum_{n\in\mathbb{Z}^*} \frac{1}{(nz-m)^2} \\
&= 1 + \frac{1}{2\zeta(2)} \sum_{n\in\mathbb{Z}} \sum_{m\in\mathbb{Z}^*} \frac{1}{(mz+n)^2}.
\end{aligned}$$

Más aún, por la proposición 4.11 conseguimos

$$E_2[S]_2(z) = 1 + \left(E_2(z) - 1 + \frac{1}{2\zeta(2)} \sum_{m\in\mathbb{Z}} \sum_{n\in\mathbb{Z}^*} \frac{1}{(mz+n-1)(mz+n)}\right)$$

Finalmente, por el lema 4.13 obtenemos

$$E_2[S]_2(z) = E_2(z) - \frac{6i}{\pi z}. \qquad \square$$

Corolario 4.15. *Para todo* $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *se cumple*

$$E_2[\gamma]_2(z) = E_2(z) - \frac{6ci}{\pi(cz+d)}.$$

Prueba. Sea Γ el subconjunto de $\mathrm{SL}_2(\mathbb{Z})$ para el cual sus elementos cumple la identidad de arriba. Por el teorema anterior, T y S son elementos de Γ. Por lo cual, podemos considerar dos elementos arbitrarios de Γ, digamos $\gamma_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ y $\gamma_2 = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$. para los cuales verificaremos que su producto es también un elemento de Γ. En efecto, al desarrollar detallamente $E_2[\gamma_1\gamma_2]_2$ obtenemos

$$\begin{aligned}
E_2[\gamma_1\gamma_2]_2(z) &= (E_2[\gamma_1]_2)[\gamma_2]_2(z) \\
&= \left(E_2(z) - \frac{6c_1 i}{\pi(c_1 z + d_1)}\right)[\gamma_2]_2 \\
&= E_2(z) - \frac{6c_2 i}{\pi(c_2 z + d_2)} - (c_2 z + d_2)^{-2} \frac{6c_1 i}{\pi\left(c_1\left(\frac{a_2 z + b_2}{c_2 z + d_2}\right) + d_1\right)}.
\end{aligned}$$

Por lo cual, para conseguir lo enunciado solo resta operar. En efecto, tenemos

$$\begin{aligned}
E_2[\gamma_1\gamma_2]_2(z) &= E_2(z) - \frac{6c_2 i}{\pi(c_2z+d_2)} - \frac{6c_1 i}{\pi(c_2z+d_2)(c_1(a_2z+b_2)+d_1(c_2z+d_2))} \\
&= E_2(z) - \frac{6c_2 i(c_1(a_2z+b_2)+d_1(c_2z+d_2))+6c_1 i}{\pi(c_2z+d_2)(c_1(a_2z+b_2)+d_1(c_2z+d_2))} \\
&= E_2(z) - \frac{6(c_2(c_1a_2+d_1c_2)z+c_1b_2c_2+d_1c_2d_2+c_1)i}{\pi(c_2z+d_2)(c_1(a_2z+b_2)+d_1(c_2z+d_2))} \\
&= E_2(z) - \frac{6(c_2(c_1a_2+d_1c_2)z+c_1a_2d_2+d_1c_2d_2)i}{\pi(c_2z+d_2)(c_1(a_2z+b_2)+d_1(c_2z+d_2))} \\
&= E_2(z) - \frac{6(c_2z+d_2)(c_1a_2+d_1c_2)i}{\pi(c_2z+d_2)(c_1(a_2z+b_2)+d_1(c_2z+d_2))} \\
&= E_2(z) - \frac{6(c_1a_2+d_1c_2)i}{\pi((c_1a_2+d_1c_2)z+c_1b_2+d_1d_2)},
\end{aligned}$$

lo cual verifica que $\gamma_1\gamma_2$ es un elemento de Γ. Adicionalmente esto último de pasada verifica que la inversa de cualquier elemento de Γ es también un elemento de él, pues S y T generan a $\mathrm{SL}_2(\mathbb{Z})$ y además las inversas de estas matrices son elementos de Γ. Por lo tanto, Γ es igual a $\mathrm{SL}_2(\mathbb{Z})$. Es decir, el enunciado se cumple. □

Como mencionamos antes, E_2 es prácticamente una forma modular de peso 2 respecto a $\mathrm{SL}_2(\mathbb{Z})$ salvo por los detalles que se muestran en el teorema 4.14. No obstante, el corolario 4.15 nos permite definir, para un entero positivo N, la función $E_{2,N}$ dada por

$$E_{2,N}(z) = E_2(z) - NE_2(Nz),$$

la cual si bien no es una forma modular de peso 2 respecto a $\mathrm{SL}_2(\mathbb{Z})$, si lo es para un subgrupo de congruencia más pequeño.

Teorema 4.16. *La función $E_{2,N}$ es una forma modular de peso 2 con respecto $\Gamma_0(N)$.*

Prueba. La función $E_{2,N}$ es holomorfa en $\mathbb{H}$ debido a la proposición 4.11, por lo cual, solo resta comprobar las otras dos propiedades que mostrarían que $E_{2,N}$ es un elemento de $M_2(\Gamma_0(N))$.

Primero verifiquemos que $E_{2,N}$ satisface la condición de modularidad de peso 2 para $\Gamma_0(N)$. Sea $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$. Por definición del operador 2-peso tenemos

$$\begin{aligned}
E_{2,N}[\gamma]_2(z) &= E_2[\gamma]_2(z) - NE_2[\gamma]_2(Nz) \\
&= E_2[\gamma]_2(z) - N(cz+d)^{-2}E_2(N\gamma z) \\
&= E_2[\gamma]_2(z) - N\left(\frac{c}{N}(Nz)+d\right)^{-2}E_2\left(\frac{aNz+bN}{\frac{c}{N}(Nz)+d}\right) \\
&= E_2(z) - \frac{6ci}{\pi(cz+d)} - N\left(E_2(Nz) - \frac{\frac{6ci}{N}}{\pi(\frac{c}{N}(Nz)+d)}\right) \quad \text{(por el corolario 4.15)} \\
&= E_2(z) - NE_2(Nz) \\
&= E_{2,N}(z).
\end{aligned}$$

De este modo, hemos verificado lo requerido.

Ahora, comprobemos que $E_{2,N}[\gamma]$ es holomorfa en infinito para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Dado que E_2 tiene una q-expansión, $E_{2,N}$ también tiene una y está dada por

$$E_{2,N}(z) = 1 - N - 24\left(\sum_{\substack{n=1 \\ N\nmid n}}^{\infty} \sigma_1(n)q^n + \sum_{\substack{n=1 \\ N\mid n}}^{\infty}\left(\sigma_1(n) - N\sigma_1\left(\frac{n}{N}\right)\right)q^n\right),$$

lo cual implica que es holomorfa en infinito. Más aún, $E_{2,N}[\gamma]$ tiene como q_N-expansión

$$E_{2,N}(z) = 1 - N - 24\left(\sum_{\substack{n=1 \\ N\mid n \\ N^2\nmid n}}^{\infty} \sigma_1\left(\frac{n}{N}\right)q_N^n + \sum_{\substack{n=1 \\ N\mid n \\ N^2\mid n}}^{\infty}\left(\sigma_1\left(\frac{n}{N}\right) - N\sigma_1\left(\frac{n}{N^2}\right)\right)q_N^n\right).$$

Reescribamos la q_N-expansión de $E_{2,N}$ de manera más manejable mediante

$$E_{2,N}(z) = 1 - N + \sum_{n=1}^{\infty} a_n q_N^n,$$

donde a_n está definida como

$$a_n = \begin{cases} -24\sigma_1\left(\frac{n}{N}\right) & \text{si } N \mid n \text{ y } N^2 \nmid n \\ -24\left(\sigma_1\left(\frac{n}{N}\right) - N\sigma_1\left(\frac{n}{N^2}\right)\right) & \text{si } N \mid n \text{ y } N^2 \mid n \\ 0 & \text{en caso contrario.} \end{cases}$$

De esto último concluimos que para todo n se cumple $|a_n| \leq 24n^2$. Por lo tanto, por el corolario 4.6 tenemos que $E_{2,N}$ es una forma modular de peso 2 respecto $\Gamma_0(N)$. $\square$

Ejemplo 4.17. Las funciones $E_{2,2}$ y $E_{2,4}$ son elementos de $M_2(\Gamma_0(2))$ y $M_2(\Gamma_0(4))$ respectivamente. Más aún, la primera es también elemento de $M_2(\Gamma_0(4))$.

Antes de discutir nuestro principal resultado de la sección es necesario que presentamos el siguiente teorema conocido como **la cota de Sturm**, el cual representa una sustancial mejora al lema 4.9.

Teorema 4.18. *Para todo $M_k(\Gamma)$ se verifica*

$$\dim(M_k(\Gamma)) \leq 1 + \left\lfloor \frac{k[\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\Gamma]}{12} \right\rfloor.$$

Prueba. Ver teorema 1 de [20]. $\square$

El siguiente ejemplo muestra que la cota establecida en el teorema 4.18 es óptima.

Ejemplo 4.19. La formas modulares $E_{2,2}$ y $E_{2,4}$ forman una base para $M_2(\Gamma_0(4))$. En efecto, por el corolario 4.18 se cumple $\dim(M_2(\Gamma_0(4))) \leq 2$ y como $E_{2,2}$ y $E_{2,4}$ son linealmente independientes, el resultado se sigue.

En este punto ya podemos describir la finalidad de esta sección, la cual consiste en probar la conjectura de Bachet. Esta es conocida también como el teorema de Lagrange de los cuatro cuadros, la cual fue originalmente probada en 1770 por métodos que no empleamos. Nosotros usaremos la teoría de las formas modulares cuya participación en este problema es misteriosa mas no anecdótica, pues como vimos en capítulo 3, las formas modulares tienen cualidades aritméticas intrínsecas.

La función **theta** de Jacobi sobre $\mathbb{H}$ está dada por

$$\theta(z) = \sum_{n \in \mathbb{Z}} q^{n^2},$$

cuya buena definición está supeditada al hecho de que converge absolutamente en todo $\mathbb{H}$. La siguiente proposición corrobora está afirmación.

Proposición 4.20. *La función $\theta(z)$ converge uniformemente en cualquier región* $\mathrm{Im}(z) > C$ *con $C > 0$. Más aún, es holomorfa en infinito.*

Prueba. La prueba es similar a la de la proposición 4.11. $\square$

De la proposición anterior concluimos que la función theta es holomorfa en el infinito con q-expansión dada por

$$\theta(z) = 1 + \sum_{n=1}^{\infty} 2q^{n^2}.$$

El siguiente lema afirma que la función $\theta(z)$ es una "forma modular de peso $1/2$ respecto al grupo generado por T y $\begin{bmatrix} 0 & -1/2i \\ -2i & 0 \end{bmatrix}$".

Lema 4.21. *La función theta satisface las ecuaciones funcioneles*

$$\theta(z+1) = \theta(z) \quad y \quad \theta\left(\frac{-1}{4z}\right) = \sqrt{-2zi}\,\theta(z)$$

para todo $z \in \mathbb{H}$.

Prueba. La primera igualdad se verifica trivialmente, por lo que solo probaremos la segunda. Sea $f(x) = e^{-\pi y x^2}$ una función real con $y > 0$ fijo. Esta aplicación es un elemento del espacio Schwartz de la recta, por lo cual la fórmula de sumatoria de Poisson tiene asidero. De esta manera, determinar los valores de la transformada de Fourier respecto a los enteros es imperativo. En efecto, para n entero tenemos

$$\begin{aligned}
\hat{f}(n) &= \int_{-\infty}^{\infty} e^{-2\pi i x n} f(x)\, dx \\
&= \int_{-\infty}^{\infty} e^{-\pi y x^2 + 2\pi i x n}\, dx \\
&= \frac{e^{-\pi n^2/y}}{\sqrt{y}} \int_{-\infty}^{\infty} e^{-\pi s^2}\, ds \quad \left(\text{donde } s = \sqrt{y}x - \frac{n}{\sqrt{y}} i\right) \\
&= \frac{e^{-\pi n^2/y}}{\sqrt{y}} \quad \left(\text{pues } \int_{-\infty}^{\infty} e^{-\pi s^2}\, ds = 1\right).
\end{aligned}$$

Por la fórmula de sumatoria de Poisson conseguimos

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 y} = \frac{1}{\sqrt{y}} \sum_{n\in\mathbb{Z}} e^{-\pi n^2/y}$$

siempre que se satisfaga $y > 0$. En resumen, hemos verificado que

$$\theta\left(\frac{-1}{4z}\right) = \sqrt{-2zi}\,\theta(z)$$

es valido para todo $z = \frac{y}{2} i$ con $y > 0$. Finalmente, el resultado se sigue por el teorema de la identidad para funciones analíticas. $\square$

Una razón (si nos es la única) por la cual nos aventuramos a considerar la teoría de formas modulares para resolver el problema de los cuatro cuadrados es que este aparece como parte de la q-representación de una función holomorfa en $\mathbb{H}$. Más precisamente, se cumple

$$\theta^4(z) = \sum_{n=0}^{\infty} r_4(n) q^n$$

donde $r_4(n)$ es igual al cardinal de $\left\{(v_1, v_2, v_3, v_4) \in \mathbb{Z}^4 : v_1^2 + v_2^2 + v_3^2 + v_4^2 = n\right\}$. En otras palabras, $r_4(n)$ es el número de representaciones de un entero n como suma de cuatro cuadrados de enteros. Esta presentación de $\theta^4(z)$, que proviene de simples manipulaciones de productos de $\theta(z)$ consigo mismo, nos permite deducir una estimación elemental para $r_4(n)$. En efecto, como para todo $n \geq 1$ se cumple

$$r_4(n) = \#\left\{(v_1, v_2, v_3, v_4) \in \mathbb{Z}^4 \cap [-n, n]^4 : v_1^2 + v_2^2 + v_3^2 + v_4^2 = n\right\},$$

concluimos que para todo $n \geq 1$ se satisface

$$r_4(n) \leq 81 n^4.$$

El siguiente teorema nos presta el principal ingrediente para probar el teorema de Lagrange de los cuatro cuadrados.

Teorema 4.22. *La función $\theta^4(z)$ es una forma modular de peso 2 respecto a $\Gamma_0(4)$.*

Prueba. La función $\theta^4(z)$ es evidentemente holomorfa por lo que nos enfocamos en probar las otras dos propiedades.

Por la proposición 2.4 y el ejemplo 1.9, la verificación de la condición de modularidad está sujeta a la comprobación de las identidades

$$\theta^4(z+1) = \theta^4(z) \quad \text{y} \quad \theta^4\left(\frac{z}{4z+1}\right) = (4z+1)^2 \theta^4(z)$$

en todo $\mathbb{H}$. La primera de ellas se cumple por lema 4.21 y la segunda se deduce de la ecuación funcional

$$\theta\left(\frac{z}{4z+1}\right) = \sqrt{4z+1}\, \theta(z),$$

la cual es válida para todo $z \in \mathbb{H}$. En efecto, al usar reiteradas veces el lema 4.21 sobre la expresión $\theta\left(\frac{z}{4z+1}\right)$ que reescribimos convenientemente como $\theta\left(-\frac{1}{4\left(-\frac{1}{4z}-1\right)}\right)$ conseguimos

$$\begin{aligned}\theta\left(\frac{z}{4z+1}\right) = \theta\left(-\frac{1}{4\left(-\frac{1}{4z}-1\right)}\right) &= \sqrt{2i\left(\frac{1}{4z}+1\right)}\theta\left(-\frac{1}{4z}-1\right)\\ &= \sqrt{2i\left(\frac{1}{4z}+1\right)}\theta\left(-\frac{1}{4z}\right)\\ &= \sqrt{2i\left(\frac{1}{4z}+1\right)}\sqrt{-2zi}\theta(z)\\ &= \sqrt{4z+1}\theta(z).\end{aligned}$$

Para verificar que $\theta^4[\gamma]_2$ es holomorfa en infinito para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, es suficiente obtener reales positivos C y r tales que se cumple

$$|r_4(n)| \leq Cn^r$$

para todo $n > 0$ debido al corolario 4.6. Pero a estos reales los conocemos, pues luego de la prueba de la lema 4.21 mencionamos que para todo $n > 0$ se verifica

$$|r_4(n)| \leq 81n^4.$$

Por lo tanto, hemos verificado la propiedad restante.

En consecuencia, la función $\theta^4(z)$ es una forma modular de peso 2 respecto a $\Gamma_0(4)$ con q-expansión dada por

$$\theta^4(z) = \sum_{n=0}^{\infty} r_4(n)q^n. \qquad \square$$

El siguiente resultado es conocido como el teorema de los cuatro cuadrados de Jacobi (probado en 1834).

Teorema 4.23. *Para todo $n > 0$ se cumple*

$$r_4(n) = 8\sum_{\substack{d|n\\ 4\nmid d}} d.$$

Prueba. Como vimos en ejemplo 4.19, las formas modulares

$$E_{2,2}(z) = -1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n + 48\sum_{n=1}^{\infty}\sigma_1(n)q^{2n}$$

y

$$E_{2,4}(z) = -3 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n + 96\sum_{n=1}^{\infty}\sigma_1(n)q^{4n}$$

forman una base para $M_2(\Gamma_0(4))$. De este modo, existen a y b números complejos sujetos a

$$aE_{2,2}(z) + bE_{2,4}(z) = \theta^4(z).$$

Cálculos elementales nos permiten obtener $a = 0$ y $b = -\frac{1}{3}$, y así tenemos

$$\theta^4(z) = -\frac{1}{3}E_{2,4}(z).$$

De esto último se infiere que para todo $n \geq 1$ se cumple

$$r_4(n) = \begin{cases} 8\sigma_1(n), & \text{si } 4 \nmid n; \\ 8\sigma_1(n) - 32\sigma_1(n/4), & \text{si } 4 \mid n. \end{cases}$$

Por lo tanto, el resultado se sigue de inmediato. □

En resumen, hemos probado nuestro principal resultado de la sección que enunciamos en el siguiente teorema.

Teorema 4.24. *Todo número natural puede ser representado como la suma de cuatro cuadrados de enteros.* □

Capítulo 5

Operadores de Hecke II

En este capítulo presentaremos distintos ejemplos de operadores lineales para los espacios de formas modulares. Además, exhibiremos la naturaleza hermitiana de los espacios de formas modulares. Los resultados introducidos en este capítulo se encuentran en [6] y [19].

5.1 Operadores de Hecke de niveles altos

Una de las principales utilidades de generar operadores lineales para las formas modulares respecto a un subgrupo de congruencia (o **operadores de Hecke de niveles de altos**) es que conseguimos nuevos ejemplos de formas modulares de apartir otras ya conocidas.

Ejemplo 5.1. Sea $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. Si f es un elemento de $M_k(\Gamma)$, entonces $f[\alpha]_k$ es un elemento de $M_k(\alpha^{-1}\Gamma\alpha)$. Más aún, si f es una forma cuspidal, entonces $f[\alpha]_k$ también lo es. En efecto, por la definición del operador k-peso y por lo discutido en el ejemplo 2.3 la función $f[\alpha]_k$ es holomorfa en $\mathbb{H}$ y satisface la condición de modularidad para $\alpha^{-1}\Gamma\alpha$, el mismo que es un subgrupo de congruencia por el teorema 1.4. En vista de que $f[\beta]_k$ es holomorfa en infinito para todo $\beta \in \mathrm{SL}_2(\mathbb{Z})$, es obvio que $f[\alpha\gamma]_k$ es holomorfa en infinito para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Por lo tanto, por definición $f[\alpha]_k$ es una forma modular de peso k respecto a $\alpha^{-1}\Gamma\alpha$.

Del ejemplo anterior deducimos que para todo $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ el operador $[\alpha]_k$ es un operador lineal entre los espacios $M_k(\Gamma)$ y $M_k(\alpha^{-1}\Gamma\alpha)$ o bien entre $S_k(\Gamma)$ y $S_k(\alpha^{-1}\Gamma\alpha)$.

No obstante, esta construcción no es exclusiva de los elementos de $\mathrm{SL}_2(\mathbb{Z})$. Para extender el resultado anterior es necesario el siguiente lema, una generalización de la parte primera del teorema 1.4.

Lema 5.2. *La intersección de un subgrupo de congruencia con cualquier conjugación de otro subgrupo de congruencia generada por un elemento de* $\mathrm{GL}_2^+(\mathbb{Q})$ *es también un subgrupo de congruencia.*

Prueba. Sean Γ_1 y Γ_2 subgrupos de congruencia y α un elemento de $\mathrm{GL}_2^+(\mathbb{Q})$. Por la parte *b*) de la teorema 1.4, existe un subgrupo de congruencia principal $\Gamma(N) \subset \Gamma_1 \cap \Gamma_2$ de tal manera que las matrices $N\alpha$ y $N\alpha^{-1}$ son enteras. De este modo, de la inclusión

$$\alpha^{-1}\Gamma(N^3)\alpha \subset \alpha^{-1}(I + N^3\mathrm{M}_2(\mathbb{Z}))\alpha \subset M_2(\mathbb{Z})$$

concluimos fácilmente que se cumple

$$\alpha^{-1}\Gamma(N^3)\alpha \subset \Gamma(N) \subset \Gamma_2,$$

lo cual implica $\Gamma(N^3) \subset \alpha\Gamma_2\alpha^{-1}$. En resumidas cuentas $\Gamma_1 \cap \alpha\Gamma_2\alpha^{-1}$ es un subgrupo de congruencia. □

El siguiente ejemplo generaliza lo presentado en el ejemplo 5.1.

Ejemplo 5.3. Sea α un elemento de $\mathrm{GL}_2^+(\mathbb{Q})$ y Γ' un subgrupo congruencia. Si f es un elemento de $M_k(\Gamma)$, entonces $f[\alpha]_k$ es un elemento de $M_k(\alpha^{-1}\Gamma\alpha \cap \Gamma')$. Es más, si f es una forma cuspidal, entonces $f[\alpha]_k$ también lo es. En efecto, $f[\alpha]_k$ es holomorfa en $\mathbb{H}$ y satisface la condición de modularidad de peso k para $\alpha^{-1}\Gamma\alpha \cap \Gamma'$, que es subgrupo de congruencia por el lema 5.2. Como $f[\gamma]_k$ es holomorfa en infinito para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ y dado que $\alpha\gamma$ es un producto de un elemento de $\mathrm{SL}_2(\mathbb{Z})$ con una matriz triangular superior de entradas racionales por la proposición 1.3, obtenemos que $f[\alpha\gamma]_k$ es holomorfa en infinito para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. De este modo queda verificado que $f[\gamma]_k$ es una forma modular de peso k respecto a $\alpha^{-1}\Gamma\alpha \cap \Gamma'$.

Tal como en el ejemplo 5.1, para todo $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ y subgrupos de congruencia arbitrarios Γ y Γ', el operador $[\alpha]_k$ es un operador lineal entre $M_k(\Gamma)$ y $M_k(\alpha^{-1}\Gamma\alpha \cap \Gamma')$ o bien entre $S_k(\Gamma)$ y $S_k(\alpha^{-1}\Gamma\alpha \cap \Gamma')$.

En los ejemplos anteriores hemos presentado operadores lineales entre espacios de formas modulares de subgrupos de congruencia donde el subgrupo de congruencia asociado al rango tiene relación con aquel respecto al dominio. En lo que queda de este capítulo describiremos un operador lineal entre espacios de formas modulares respecto a subgrupos de congruencia arbitrarios. Para ello es necesario un tecnicismo que es apenas una paráfrasis de un resultado clásico sobre los índices de las clase laterales dobles de subgrupos.

Lema 5.4. *Sean* Γ_1 *y* Γ_2 *subgrupos de congruencia y* α *un elemento de* $\mathrm{GL}_2^+(\mathbb{Q})$ *. Si definimos* Γ_3 *como* $\alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$*, la aplicación* $\Gamma_2 \to \Gamma_1\alpha\Gamma_2$ *dada por*

$$\begin{aligned} \Gamma_2 &\to \Gamma_1\alpha\Gamma_2 \\ \gamma_2 &\mapsto \alpha\gamma_2 \end{aligned}$$

induce una biyección natural entre el espacio de clases laterales $\Gamma_3\backslash\Gamma_2$ *y el espacio de órbitas* $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$*.*

Prueba. Claramente, la aplicación de Γ_2 a $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ que envía γ_2 a $\Gamma_1\alpha\gamma_2$ es sobreyectiva. Más aún, dos elementos γ_2 y γ_2' de Γ_2 están en la misma órbita si y solo si $\gamma_2'\gamma_2^{-1}$ es un elemento de $\alpha^{-1}\Gamma_1\alpha$. Por lo tanto, la aplicación natural de $\Gamma_3\backslash\Gamma_2$ a $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ es una biyección. ☐

Sean k un entero, α un elemento de $\mathrm{GL}_2^+(\mathbb{Q})$ y Γ_1 y Γ_2 subgrupos de congruencia. El **operador k-clase lateral doble** $[\Gamma_1\alpha\Gamma_2]_k$ para $M_k(\Gamma_1)$ está definido por

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum_{\overline{\beta}\in\Gamma_1\backslash\Gamma_1\alpha\Gamma_2} f[\beta]_k.$$

Hagamos unas observaciones de rutina asocidas a este operador. Por el lema 5.4, la cantidad de representantes de órbitas de $\Gamma_1\alpha\Gamma_2$ es finita. Por esta razón, la suma de operadores k-peso es finita en la definición del k-operador clase lateral doble; este último está bien definido, pues f es un elemento de $M_k(\Gamma_1)$.

Teorema 5.5. *El operador k-clase lateral doble* $[\Gamma_1\alpha\Gamma_2]_k$ *es un operador lineal entre los espacios* $M_k(\Gamma_1)$ *y* $M_k(\Gamma_2)$*. Es más, define un operador entre* $S_k(\Gamma_1)$ *y* $S_k(\Gamma_2)$*.*

Prueba. Sea f un elemento $M_k(\Gamma_1)$. Como claramente $f[\Gamma_1\alpha\Gamma_2]_k$ es holomorfa en todo $\mathbb{H}$, solo basta verificar las otras dos propiedades para mostrar que es un elemento de $M_k(\Gamma_2)$. Primero probemos que $f[\Gamma_1\alpha\Gamma_2]_k$ satisface la condición de modularidad de peso k para Γ_2.

Para todo $\gamma_2 \in \Gamma_2$, la aplicación $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2 \to \Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ dada por

$$\begin{aligned} \Gamma_1\backslash\Gamma_1\alpha\Gamma_2 &\to \Gamma_1\backslash\Gamma_1\alpha\Gamma_2 \\ \overline{\beta} &\mapsto \overline{\beta\gamma_2} \end{aligned}$$

es una permutación. Así de la proposición 2.1 deducimos la igualdad

$$\begin{aligned} f[\Gamma_1\alpha\Gamma_2]_k[\gamma_2]_k &= \sum_{\overline{\beta}\in\Gamma_1\backslash\Gamma_1\alpha\Gamma_2} f[\beta]_k[\gamma_2]_k \\ &= \sum_{\overline{\beta}\in\Gamma_1\backslash\Gamma_1\alpha\Gamma_2} f[\beta\gamma_2]_k \\ &= \sum_{\overline{\beta\gamma_2}\in\Gamma_1\backslash\Gamma_1\alpha\Gamma_2} f[\beta\gamma_2]_k \\ &= f[\Gamma_1\alpha\Gamma_2]_k. \end{aligned}$$

De este modo, $f[\Gamma_1\alpha\Gamma_2]_k$ satisface la condición de modularidad de peso k para Γ_2.

Ahora, probemos que $f[\Gamma_1\alpha\Gamma_2]_k$ es holomorfa en infinito. Sea $\overline{\beta}$ un elemento arbitrario de $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ y γ un elemento de $\mathrm{SL}_2(\mathbb{Z})$. Por la proposición 1.3, existe r racional positivo, γ' elemento de $\mathrm{SL}_2(\mathbb{Z})$ y $\tau = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ una matriz entera de determinante positiva relacionados vía $\beta\gamma = r\gamma'\tau$. De la proposición 2.1 obtenemos así

$$\begin{aligned} f[\beta]_k[\gamma]_k &= f[\beta\gamma]_k \\ &= f[r\gamma'\tau]_k \\ &= f[\gamma'\tau]_k \\ &= f[\gamma']_k[\tau]_k. \end{aligned}$$

Dado que $f[\gamma']_k$ tiene una q_h-expansión $\sum_{n=0}^{\infty} a_n q_h^n$, podemos conseguir, al igual que en el teorema 3.4, una expansión para $f[\gamma']_k[\tau]_k$:

$$\begin{aligned}
f[\gamma']_k[\tau]_k(z) &= \left(\frac{a}{d}\right)^{k/2} f[\gamma']_k\left(\frac{az+b}{d}\right) \\
&= \left(\frac{a}{d}\right)^{k/2} \sum_{n=0}^{\infty} a_n e^{2\pi i n(az+b)/dh} \\
&= \left(\frac{a}{d}\right)^{k/2} \sum_{n=0}^{\infty} a_n e^{2\pi i b/dh} q_{dh}^{an}.
\end{aligned}$$

Como la suma de funciones holomorfas en infinito es una función holomorfa en infinito resulta que $f[\Gamma_1\alpha\Gamma_2]_k[\gamma]_k$ es holomorfa en infinito para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Más aún, si $f[\gamma']_k$ tiene orden positivo en infinito, entonces $f[\gamma']_k[\tau]_k$ también lo tendrá.

En resumen, hemos probado que $f[\Gamma_1\alpha\Gamma_2]_k$ es elemento de $M_k(\Gamma_2)$. □

5.2 Producto interno de Petersson

En la sección anterior, proporcionamos distintos ejemplos de operadores lineales entre espacios de formas modulares respecto a subgrupos de congruencia. Ahora, nos sentimos obligados a indagar más sobre la estructura de los espacios de formas modulares. Específicamente, en esta sección mostraremos que los espacios de las formas cuspidales son hermitianos. Además, exhibiremos que el operador T_n del capítulo 3 como un operador hermitiano para las formas cuspidales respecto a $\mathrm{SL}_2(\mathbb{Z})$.

Tomemos la medida **hipérbolica** $d\mu$ sobre $\mathbb{H}$ definida por

$$d\mu(z) = \frac{dxdy}{y^2},$$

donde x y y son la parte real e imaginaria de $z \in \mathbb{H}$. Esta la utilizaremos para definir un producto interno en ciertos epacios de funciones.

Ejemplo 5.6. La medida hiperbólica de $F_{\mathrm{SL}_2(\mathbb{Z})}$ es $\frac{\pi}{3}$. En efecto, un cálculo directa lleva a

$$\begin{aligned}
\int_{F_{\mathrm{SL}_2(\mathbb{Z})}} d\mu(z) &= \int_{-1/2}^{1/2}\int_{\sqrt{1-x^2}}^{\infty} \frac{dydx}{y^2} \\
&= \frac{\pi}{3}.
\end{aligned}$$

La medida hiperbólica es interesante debido a que ella se preserva vía las transformaciones de Möbius. La siguiente proposición prueba esta afirmación.

Proposición 5.7. *La medida hiperbólica sobre* $\mathbb{H}$ *es* $\mathrm{GL}_2^+(\mathbb{R})$*-invariante.*

Prueba. Sea $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ un elemento de $\mathrm{GL}_2^+(\mathbb{R})$ y $z = x + yi$ un punto de $\mathbb{H}$. Por un lado, si describimos γz como $u(x, y) + v(x, y)i$ donde u y v son funciones reales diferenciables definidas sobre $\mathbb{R} \times \mathbb{R}^+$ que satisfacen las ecuaciones de Cauchy-Riemann, entonces la fórmula del cambio de variable nos brinda

$$\begin{aligned} d\mu(\gamma z) &= \frac{dudv}{(\mathrm{Im}(\gamma z))^2} \\ &= \det\left(\begin{bmatrix} u_x & u_y \\ v_x & v_y \end{bmatrix}\right)\frac{dxdy}{(\mathrm{Im}(\gamma z))^2} \\ &= \det\left(\begin{bmatrix} u_x & u_y \\ v_x & v_y \end{bmatrix}\right)\frac{|cz+d|^4 dxdy}{(\det(\gamma)y)^2}. \end{aligned}$$

Por otro lado, de las ecuaciones de Cauchy-Riemann tenemos

$$\begin{aligned} \det\left(\begin{bmatrix} u_x & u_y \\ v_x & v_y \end{bmatrix}\right) &= \left|\frac{d\gamma z}{dz}\right|^2 \\ &= \frac{(\det(\gamma))^2}{|cz+d|^4}. \end{aligned}$$

De este modo, tras simplificar obtenemos $d\mu(\gamma z) = d\mu(z)$. □

En pos de simplicar el lenguaje, definamos un número complejo asociado a cada elemento $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ de $\mathrm{GL}_2^+(\mathbb{R})$ y punto z de $\mathbb{H}$ mediante $j(\gamma, z) = cz + d$, el cual es conocido como el **factor de automorfía** de γ en z. Observemos que para todo $z \in \mathbb{H}$ se cumple $j(\gamma_1\gamma_2, z) = j(\gamma_1, \gamma_2 z)j(\gamma_2, z)$ siempre que se tenga $\gamma_1, \gamma_2 \in \mathrm{GL}_2^+(\mathbb{R})$.

Lema 5.8. *Sean* $\phi : \mathbb{H} \to \mathbb{C}$ *una función y* Γ *un subgrupo congruencia. Si* ϕ *es continua, acotada y* Γ*-invariante, entonces la integral de* ϕ *sobre un dominio fundamental* F_Γ *para* Γ*, es decir*

$$\int_{F_\Gamma} \phi(z)d\mu(z),$$

es absolutamente convergente e independiente del dominio fundamental para Γ.

Prueba. Primero probemos que la integral es independiente del dominio fundamental elegido para Γ. Sea F'_Γ un dominio fundamental para Γ distinto de F_Γ. Por la topología de $\mathbb{H}$ y por las propiedades de dominio fundamental, podemos conseguir una partición numerable para F_Γ dada por $F_\Gamma = \bigcup_{n=1}^{\infty} U_n$ para la cual existe una sucesión $\{\alpha_n\}_{n=1}^{\infty}$ de elementos de Γ que satisface $\alpha_n(U_n) \subset F'_\Gamma$ para todo n. Más aún, se cumple que el complemento de $\bigcup_{n=1}^{\infty} \alpha_n(U_n)$ en F'_Γ yace completamente dentro de la frontera de F'_Γ. De este modo, tenemos

$$\int_{\bigcup_{n=1}^{\infty} \alpha_n(U_n)} \phi(z)d\mu(z) = \int_{F'_\Gamma} \phi(z)d\mu(z).$$

Pero como ϕ y $d\mu(z)$ son Γ-invariantes, conseguimos

$$\int_{F_\Gamma} \phi(z)d\mu(z) = \int_{F'_\Gamma} \phi(z)d\mu(z).$$

Por lo tanto, la integral de ϕ es independiente del dominio fundamental.

Ahora probemos que la integral en cuestión es absolutamente convergente. Consideremos $\alpha_1, \ldots, \alpha_n$ un subconjunto tranversal de $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}\Gamma$ tal que $\bigcup_{i=1}^{n} \alpha_i(F_{\mathrm{SL}_2(\mathbb{Z})})$ es un dominio fundamental para Γ. Como ϕ es acotada, existe C tal que para todo $z \in \mathbb{H}$ se cumple $|\phi(z)| \leq C$. Así tenemos

$$\left| \sum_{i=1}^{n} \int_{\alpha_i(F_{\mathrm{SL}_2(\mathbb{Z})})} \phi(z)d\mu(z) \right| \leq C \sum_{i=1}^{n} \int_{\alpha_i(F_{\mathrm{SL}_2(\mathbb{Z})})} d\mu(z).$$

Como $d\mu(z)$ es $\mathrm{SL}_2(\mathbb{Z})$-invariante y dado que la medida hiperbólica de $F_{\mathrm{SL}_2(\mathbb{Z})}$ vale $\pi/3$, obtenemos

$$\left| \sum_{i=1}^{n} \int_{\alpha_i(F_{\mathrm{SL}_2(\mathbb{Z})})} \phi(z)d\mu(z) \right| \leq \frac{C\pi n}{3} \qquad \square$$

El siguiente resultado nos permite definir un producto interno para los espacios de formas cuspidales respecto a subgrupos de congruencia.

Teorema 5.9. *Sean f y g elementos de $S_k(\Gamma)$ y F_Γ un dominio fundamenteal de Γ. La integral*

$$\int_F f(z)\overline{g(z)}\mathrm{Im}(z)^k d\mu(z)$$

es absolutamente convergente e independiente de F_Γ.

Prueba. En virtud del lema anterior, es suficiente probar que $f(z)\overline{g(z)}\mathrm{Im}(z)^k$ es continua, Γ-invariante y acotada. Como la primera propiedad es evidente, nos limitamos a probar las dos propiedades restantes.

Sea γ un elemento de Γ. Por la proposición 2.1 obtenemos

$$\begin{aligned} f(\gamma z)\overline{g}(\gamma z)\mathrm{Im}(\gamma z)^k &= f[\gamma]_k(z)j(\gamma,z)^k\overline{g[\gamma]_k}(z)\overline{j(\gamma,z)}^k\mathrm{Im}(z)^k|j(\gamma,z)|^{-2k} \\ &= f[\gamma]_k(z)\overline{g[\gamma]_k}(z)\mathrm{Im}(z)^k \\ &= f(z)\overline{g}(z)\mathrm{Im}(z)^k, \end{aligned}$$

donde la última igualdad deviene del hecho de que f y g satisfacen la condición de modularidad de peso k para Γ. Por ello, tenemos que $f(z)\overline{g(z)}\mathrm{Im}(z)^k$ es Γ-invariante.

Para mostrar que $f(z)\overline{g(z)}\mathrm{Im}(z)^k$ es acotada en $\mathbb{H}$, basta mostrar que lo es en algún dominio fundamental de Γ. Sea $\bigcup_{i=1}^{n}\alpha_i F_{\mathrm{SL}_2(\mathbb{Z})}$ un dominio fundamental para Γ donde los α_i son elementos convenientemente elegidos de $\mathrm{SL}_2(\mathbb{Z})$. Por lo visto en el párrafo anterior, es suficiente probar que $f[\alpha_i]_k(z)\overline{g[\alpha_i]_k}(z)\mathrm{Im}(z)^k$ es acotada en $F_{\mathrm{SL}_2(\mathbb{Z})}$ para todo α_i.

Sea N el nivel de Γ. El hecho de que f y g sean cuspidales de peso k para Γ nos permite estimar

$$f[\alpha_i]_k(z)\overline{g[\alpha_i]_k}(z)\mathrm{Im}(z)^k = O(q_N^2\mathrm{Im}(z)^k).$$

Esto último implica que $f[\alpha_i]_k(z)\overline{g[\alpha_i]_k}(z)\mathrm{Im}(z)^k$ es acotado en una vecindad de infinito. Y como $f[\alpha_i]_k(z)\overline{g[\alpha_i]_k}(z)\mathrm{Im}(z)^k$ es acotada en cualquier subconjunto compacto de $F_{\mathrm{SL}_2(\mathbb{Z})}$, el resultado finalmente se verifica. □

Corolario 5.10. *La integral del teorema anterior define un producto interno hermitiano sobre $S_k(\Gamma)$, la cual denotaremos por $\langle\ ,\ \rangle_\Gamma$, dado por*

$$\langle f,g\rangle_\Gamma \mapsto \frac{1}{[\mathrm{SL}_2(\mathbb{Z}):\{\pm I\}\Gamma]}\int_{F_\Gamma} f(z)\overline{g(z)}(\mathrm{Im}(z))^k d\mu(z),$$

acá f y g son elementos de $S_k(\Gamma)$ y F_Γ es un dominio fundamental para Γ. □

Este producto interno recién introducido es conocido como **el producto interno de Petersson**. Cuando el subgrupo de congruencia Γ esté claro en el contexto, simplemente escribiremos $\langle,\rangle$.

Teorema 5.11. *Sean Γ_1 y Γ_2 subgrupos de congruencia sujetos a $\Gamma_1 \subset \Gamma_2$. Entones, para* *cualesquiera f y g elementos de $S_k(\Gamma_2)$ se cumple la identidad*

$$\langle f, g\rangle_{\Gamma_1} = \langle f, g\rangle_{\Gamma_2}.$$

Prueba. Sean las descomposiciones $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_i \{\pm I\}\Gamma_2\alpha_i$ y $\{\pm I\}\Gamma_2 = \bigcup_j \{\pm I\}\Gamma_1\beta_j$ de tal manera que $\bigcup_j\bigcup_i \beta_j\alpha_i(F_{\mathrm{SL}_2(\mathbb{Z})})$ y $\bigcup_i \alpha_i(F_{\mathrm{SL}_2(\mathbb{Z})})$ sean dominios fundamentales de Γ_2 y Γ_1, respectivamente. Por definición, se tiene

$$\langle f, g\rangle_{\Gamma_1} = \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\Gamma_1]}\sum_i\sum_j \int\limits_{\beta_j\alpha_i(F_{\mathrm{SL}_2(\mathbb{Z})})} f(z)\overline{g(z)}(\mathrm{Im}(z))^k d\mu(z).$$

Como los β_j pueden ser considerados elementos de Γ_2, obtenemos

$$\begin{aligned}\langle f, g\rangle_{\Gamma_1} &= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\Gamma_1]}\sum_i\sum_j \int\limits_{\alpha_i(F_{\mathrm{SL}_2(\mathbb{Z})})} f(\beta_j z)\overline{g(\beta_j z)}(\mathrm{Im}(\beta_j z))^k d\mu(z)\\ &= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\Gamma_1]}\sum_i\sum_j \int\limits_{\alpha_i(F_{\mathrm{SL}_2(\mathbb{Z})})} f(z)\overline{g(z)}(\mathrm{Im}(z))^k d\mu(z)\end{aligned}$$

Finalmente, de ahí pasamos a

$$\begin{aligned}\langle f, g\rangle_{\Gamma_1} &= \frac{[\{\pm I\}\Gamma_2 : \{\pm I\}\Gamma_1]}{[\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\Gamma_1]}\sum_i \int\limits_{\alpha_i(F_{\mathrm{SL}_2(\mathbb{Z})})} f(z)\overline{g(z)}(\mathrm{Im}(z))^k d\mu(z)\\ &= \langle f, g\rangle_{\Gamma_2},\end{aligned}$$

pues se cumple $[\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\Gamma_1] = [\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\Gamma_2][\{\pm I\}\Gamma_2 : \{\pm I\}\Gamma_1]$. □

Corolario 5.12. *Sea $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. Para f y g elementos de $M_k(\Gamma)$ se verifica la identidad*

$$\langle f, g\rangle_{\Gamma} = \langle f[\alpha]_k, g[\alpha]_k\rangle_{\alpha^{-1}\Gamma\alpha\cap\Gamma}.$$ □

Corolario 5.13. *Sea $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. Para cualesquiera $f, g \in M_k(\Gamma)$ se cumple la identidad*

$$\langle f[\alpha]_k, g\rangle_{\Gamma} = \langle f, g[D\alpha^{-1}]_k\rangle_{\Gamma},$$

acá D es el valor del determinante de α. □

El siguiente teorema corrobora que los operadores de Hecke de nivel bajo son hermitianos.

Teorema 5.14. *Para cualesquiera f y g elementos de $S_k(\mathrm{SL}_2(\mathbb{Z}))$ se cumple*

$$\langle T_n(f), g\rangle = \langle f, T_n(g)\rangle.$$

Prueba. Por la linealidad de producto interno de Petersson y por el hecho de que dado un número primo p y un número entero $s > 0$, el operador T_{p^s} se puede describir como un polinomio del operador T_p, es suficiente verificar la afirmación para $n = p$.

Por definición, tenemos entonces

$$\langle T_p(f), g\rangle = \langle p^{k/2-1}\left(f\begin{bmatrix} p & 0\\ 0 & 1\end{bmatrix}_k + \sum_{b=0}^{p-1} f\begin{bmatrix} 1 & b\\ 0 & p\end{bmatrix}_k\right), g\rangle.$$

Por linealidad, conseguimos

$$\langle T_p(f), g\rangle = p^{k/2-1}\left(\langle f\begin{bmatrix} p & 0\\ 0 & 1\end{bmatrix}_k, g\rangle + \sum_{b=0}^{p-1}\langle f\begin{bmatrix} 1 & b\\ 0 & p\end{bmatrix}_k, g\rangle\right).$$

Por el corolario 5.12 obtenemos

$$\begin{aligned}\langle T_p(f), g\rangle &= p^{k/2-1}\left(\langle f, g\begin{bmatrix} 1 & 0\\ 0 & p\end{bmatrix}_k\rangle + \sum_{b=0}^{p-1}\langle f, g\begin{bmatrix} p & -b\\ 0 & 1\end{bmatrix}_k\rangle\right)\\ &= p^{k/2-1}\left(\langle f, g\begin{bmatrix} p & 0\\ 0 & 1\end{bmatrix}_k\rangle + \langle f, g\begin{bmatrix} 1 & 0\\ 0 & p\end{bmatrix}_k\rangle + \sum_{b=1}^{p-1}\langle f, g\begin{bmatrix} p & -b\\ 0 & 1\end{bmatrix}_k\rangle\right).\end{aligned}$$

Ahora notemos que para todo entero b se cumple la igualdad

$$\begin{bmatrix} 0 & -1\\ 1 & b\end{bmatrix}\begin{bmatrix} p & -b\\ 0 & 1\end{bmatrix}\begin{bmatrix} 0 & 1\\ -1 & -b\end{bmatrix} = \begin{bmatrix} 1 & b\\ 0 & p\end{bmatrix}.$$

Por ello, el corolario 5.13 junto al uso reiterado de la condición de modularidad para $\mathrm{SL}_2(\mathbb{Z})$ de peso k de tanto f como g nos permite conseguir

$$\begin{aligned}\sum_{b=1}^{p-1}\langle f, g\begin{bmatrix} p & -b\\ 0 & 1\end{bmatrix}_k\rangle &= \sum_{b=1}^{p-1}\langle f\begin{bmatrix} 0 & 1\\ -1 & -b\end{bmatrix}_k, g\begin{bmatrix} p & -b\\ 0 & 1\end{bmatrix}_k\begin{bmatrix} 0 & 1\\ -1 & -b\end{bmatrix}_k\rangle\\ &= \sum_{b=1}^{p-1}\langle f\begin{bmatrix} 0 & 1\\ -1 & -b\end{bmatrix}_k, g\begin{bmatrix} 0 & -1\\ 1 & b\end{bmatrix}_k\begin{bmatrix} p & -b\\ 0 & 1\end{bmatrix}_k\begin{bmatrix} 0 & 1\\ -1 & -b\end{bmatrix}_k\rangle\\ &= \sum_{b=1}^{p-1}\langle f, g\begin{bmatrix} 1 & b\\ 0 & p\end{bmatrix}_k\rangle.\end{aligned}$$

En resumen, se verifica $\langle T_n(f), g\rangle = \langle f, T_n(g)\rangle$. $\square$

El siguiente resultado de álgebra lineal es conocido como el teorema espectral.

Teorema 5.15. *Sea un espacio de Hilbert finito dimensional V. Si R es un anillo conmutativo de operadores hermitianos sobre V, entonces este espacio admite una base ortogonal formada por autovectores de R.* $\square$

Corolario 5.16. *El espacio vectorial $S_k(\mathrm{SL}_2(\mathbb{Z}))$ tiene un base ortogonal formada valores propios del operador T_n.*

Prueba. El espacio $S_k(\mathrm{SL}_2(\mathbb{Z}))$ es un espacio de Hilbert, pues es finito dimensional. Por lo cual, es suficiente encontrar un anillo conmutivo de operadores hermitianos sobre los espacios $S_k(\mathrm{SL}_2(\mathbb{Z}))$. Pero, esta tarea ya se hizo, precisamente el teorema 5.14 nos dice que el anillo de operadores formado por los enésimos operadores de Hecke T_n es conmutativo. Por lo tanto, el resultado se verifica como consecuencia del teorema anterior. $\square$

Bibliografía

[1] H. BASS, M. LAZARD, J-P. SERRE, *Sous-groupes d'indice fini dans* $\mathrm{SL}_n(\mathbb{Z})$. Bulletin of the American Mathematical Society, 70 (1964), 385-392.

[2] A. F. BEARDON, *The geometry of discrete groups.* Graduate Texts in Mathematics, Volume 91, Springer-Verlag, Corrected 2nd edition, 1995.

[3] H. COHN, A. KUMAR, S. MILLER, D. RADCHENKO Y M. VIAZOVSKA, *The sphere packing problem in dimension 24.* Annals of Mathematics, 157 (2003), 1017-1033.

[4] H. COHN, N. ELKIES, *New upper bounds on sphere packings I.* Annals of Mathematics, 185 (2017), 689-714.

[5] P. DELIGNE, *La conjecture de Weil: I.* Publications Mathématiques de I'IHÉS, 43 (1974), 273-307.

[6] F. DIAMOND, J. SHURMAN, *A first course in modular forms.* Graduate Texts in Mathematics, Volume 228, Springer-Verlag, New York, 2005.

[7] E. FREITAG, R. BUSAM, *Complex analysis.* Universitext, Springer-Verlag, 2009.

[8] E. HECKE, *Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung. I.* Mathematische Annalen, 114 (1937), 1-28.

[9] E. HECKE, *Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung. II.* Mathematische Annalen, 114 (1937), 316-351.

[10] L. K. HUA, I. REINER, *Automorphisms of the unimodular group.* Transactions of the American Mathematical Society, 71 (1951), 331-348.

[11] N. KOBLITZ, *Introduction to elliptic curves and modular forms.* Graduate Texts in Mathematics, Volume 97, Springer-Verlag, 2nd edition, 1993.

[12] S. LANG, *Undergraduate algebra.* Undergraduate Texts in Mathematics, Springer, 3rd edition, 2005.

[13] T. MIYAKE, *Modular forms.* Springer Monographs in Mathematics, Springer, Corrected edition, 2006.

[14] L.J. MORDELL, *On Mr. Ramanujan's empirical expansions of modular functions.* Proceedings of the Cambridge Philosophical Society, 19 (1917), 117-124.

[15] A. POIRIER, *Aspectos geométricos del análisis complejo.* Fondo Editorial de la Pontificia Universidad Católica del Perú, 2005.

[16] M. S. RAGHUNATHAN, *The congruence subgroup problem.* Proceedings of the Indian Academy of Science, 114 (2003), 299-309.

[17] S. RAMANUJAN, *On certain arithmetical functions.* Transactions of the Cambridge Philosophical Society, 9 (1916), 159-184.

[18] A. SERESS, *Permutation group algorithms.* Cambridge Tracts in Mathematics, Volume 152, Cambridge University Press, New York, 2002.

[19] J-P. SERRE, *A course in Arithmetic.* Graduate Texts in Mathematics, Volume 7, Springer-Verlag, Corrected 3rd edition, 1996.

[20] J. STURM, *On the congruence of modular forms.* Lecture Notes in Mathematics, Volume 1240, Springer-Verlag, Berlin, 1987.

[21] M. VIAZOVSKA, *The sphere packing problem in dimension 8.* Annals of Mathematics, 185 (2017), 991-1015.

[22] N. YOUNG, *An Introduction to Hilbert Space.* Cambridge Mathematical Textbooks, Cambridge University Press, 1 edition, 1988.