2 E. 33

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

LA ECUACION FUNCIONAL DE LA FUNCION ZETA ASOCIADA A UNA FORMA MODULAR

T E S I S

QUE PARA OBTENER EL TITULO DE

M A T E M A T I C O

P R E S E N T A

ARMANDO REYES RODRIGUEZ

MEXICO, D.F. 1984.

ÍNDICE

CAPITULO I

Entre los objetos de estudio más importantes que intervienen en este trabajo se encuentran subespacios de los así llamados grupos lineales clásicos; así como acciones de estos subespacios sobre la mitad superior del plano complejo. Este capítulo comienza con una revisión de los principales resultados concernientes a estos grupos y nos introduce a los espacios con respecto a los cuales quedarán definidas las funciones que aquí estudiaremos; las funciones y formas automorfas. Estos espacios son los llamados grupos Fuchsianos de la primera clase.

1.1 *Grupos lineales clásicos y grupos de transformaciones.*

Esta primera sección no pretende ser una introducción a los grupos topológicos, ni pretende ser una introducción a los grupos lineales clásicos, solamente pretende ser, como ya se ha dicho, una revisión de los principales resultados relativos a estos grupos que son de nuestro particular interés. Esta es la razón por la cual todos los resultados sobre grupos topológicos y grupos lineales clásicos que aquí se mencionan, carecen de demostración. Una demostración de cada uno de estos resultados está fuera del propósito de este trabajo, sin embargo, se pueden recomendar los libros de Chevalley, [3], y Pontrjagin, [13], como excelentes referencias a las cuales se puede remitir aquel lector que desee una demostración de estos resultados. Comenzamos pues introduciendo conceptos a través de definiciones y fijando notación.

Como es costumbre el símbolo $M_n(\mathbb{C})$ denotará al anillo de matrices cuadradas de grado n (de $n \times n$) con coeficientes complejos. Este conjunto, así como sus subconjuntos que se definirán más adelante, nos interesan, sobre todo, desde el punto de vista de sus estructuras continuas, es decir desde el punto de vista topológico. Por esta razón es necesario dotar a $M_n(\mathbb{C})$, y a sus subconjuntos, de una topología. La topología que se define sobre $M_n(\mathbb{C})$ es la que se obtiene asociando a cada matriz $(a_{ij}) \in M_n(\mathbb{C})$ un punto de $\mathbb{C}^{n^2}$ de la siguiente manera:

A cada matriz $(a_{ij}) \in M_n(\mathbb{C})$ se le asocia el punto de coordenadas $(a_{11}, \ldots, a_{1n}, \ldots\ldots, a_{n1}, \ldots, a_{nn})$ en $\mathbb{C}^{n^2}$. Esta asociación establece una biyección entre los elementos de $M_n(\mathbb{C})$ y los puntos de $\mathbb{C}^{n^2}$. Aprovechamos entonces la estructura topológica de $\mathbb{C}^{n^2}$. Un subconjunto O de $M_n(\mathbb{C})$ será un abierto en $M_n(\mathbb{C})$ si y sólo si $\{(z_{11}, \ldots, z_{1n}, \ldots, z_{n1}, \ldots, z_{nn}) \in \mathbb{C}^{n^2} : (z_{ij}) \in O\}$ es abierto en $\mathbb{C}^{n^2}$. Con esta topología la asociación anterior resulta un homeomorfismo de $M_n(\mathbb{C})$ en $\mathbb{C}^{n^2}$, además el producto de matrices en $M_n(\mathbb{C})$ resulta una operación contínua.

De particular interés es el grupo de las matrices inverti bles (matrices regulares o matrices no-singulares) de $M_n(\mathbb{C})$ al que llamaremos el grupo lineal general.

Definición 1. El grupo lineal general es el grupo constituido por las matrices invertibles de $M_n(\mathbb{C})$. Lo denotaremos con el símbolo $GL_n(\mathbb{C})$.

El grupo $GL_n(\mathbb{C})$ se verá como espacio topológico con la topología inducida de $M_n(\mathbb{C})$ (topología de subespacio). Puesto que el determinante de una matriz es una función continua de la matriz, $GL_n(\mathbb{C})$ resulta ser un subconjunto abierto de $M_n(\mathbb{C})$. No es difícil ver también que las operaciones de tomar inversas, conjugadas y transpuestas en los elementos de $GL_n(\mathbb{C})$ son operaciones continuas de estos elementos, aún más, son homeomorfismos de $GL_n(\mathbb{C})$ en sí mismo.

Dada $\sigma \in GL_n(\mathbb{C})$ denotamos por σ^* a la matriz definida por:

$$\sigma^* = {}^t\sigma^{-1}$$

El lado derecho de la igualdad no da lugar a confusiones puesto que los operadores ${}^t(\ )$ y $(\ )^{-1}$ conmutan. Estos operadores junto con el operador $\overline{(\ )}$ tienen las siguientes propiedades:

si $\sigma, \tau \in GL_n(\mathbb{C})$ $\quad {}^t(\sigma\tau) = {}^t\tau\,{}^t\sigma \qquad \overline{\sigma\tau} = \bar{\sigma}\,\bar{\tau} \quad (\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$

de aquí se deduce que los mapeos $\sigma \longrightarrow \bar{\sigma}$ y $\sigma \longrightarrow \sigma^*$ de

$GL_n(\mathbb{C})$ en si mismo, son automorfismos de $GL_n(\mathbb{C})$. Damos aho ra más definiciones.

Definición 2. Una matriz σ es llamada ortogonal si $\sigma = \bar{\sigma} = \sigma^*$. El conjunto de todas las matrices ortogonales de grado n será denotado por $O(n)$.

Si una matriz satisface solamente la condición $\sigma = \sigma^*$, entonces σ es llamada ortogonal compleja y el conjunto de estas matrices es denotado por el símbolo $O_n(\mathbb{C})$. Si por otro lado la matriz σ solamente satisface la condición $\bar{\sigma} = \sigma^*$, entonces σ es llamada unitaria. El conjunto de las matrices unitarias es denotado por $U(n)$.

El mapeo $\sigma \longrightarrow \sigma^*$, de $GL_n(\mathbb{C})$ en sí mismo, es continuo pues es composición de mapeos continuos. Como también el mapeo $\sigma \longrightarrow \bar{\sigma}$ es continuo, resulta que los conjuntos $O(n)$, $O_n(\mathbb{C})$ y $U(n)$ son subconjuntos cerrados de $GL_n(\mathbb{C})$; simplemente el conjunto de las matrices unitarias es la imagen inversa de cero bajo el mapeo continuo $\sigma \longrightarrow \bar{\sigma} - \sigma^*$ y $O_n(\mathbb{C})$ es la imagen inversa de cero bajo el mapeo continuo $\sigma \longrightarrow \sigma - \sigma^*$, además $O(n) = O_n(\mathbb{C}) \cap U(n)$. Por otro lado como los mapeos $\sigma \longrightarrow \sigma^*, \sigma \longrightarrow \bar{\sigma}$ son automorfismos de $GL_n(\mathbb{C})$; $O(n)$, $O_n(\mathbb{C})$ y $U(n)$ resultan subgrupos de $GL_n(\mathbb{C})$.

Cuando una matriz tenga coeficientes reales diremos que la matriz es real. El conjunto de las matrices reales de grado n será denotado por $M_n(\mathbb{R})$, pondremos $GL_n(\mathbb{R})=M_n(\mathbb{R})\cap GL_n(\mathbb{C})$.

A partir de las propiedades de los determinantes se sigue que las matrices de determinante 1 forman un subgrupo de $GL_n(\mathbb{C})$, llamado el grupo lineal especial.

Definición 3. El grupo de las matrices de determinante 1 en $GL_n(\mathbb{C})$ es llamado el grupo lineal especial y es denotado por $SL_n(\mathbb{C})$.

A manera de definición podemos poner:

$$SL_n(\mathbb{R}) = SL_n(\mathbb{C})\cap GL_n(\mathbb{R})\,;\quad SO(n) = SL_n(\mathbb{C})\cap O(n)\,;\quad SU(n) = SL_n(\mathbb{C})\cap U(n)$$

El grupo $SO(n)$ es llamado el grupo ortogonal especial y el grupo $SU(n)$ es llamado el grupo unitario especial. Los conjuntos $SL_n(\mathbb{C})$, $SL_n(\mathbb{R})$, $SO(n)$, $SU(n)$ se considerarán como subespacios de $GL_n(\mathbb{C})$ con la topología inducida. Estos conjuntos son subconjuntos cerrados, y además subgrupos, de $GL_n(\mathbb{C})$. Como uno de los teoremas importantes de esta sección tenemos:

Teorema 1. Los espacios $U(n)$, $O(n)$, $SU(n)$ y $SO(n)$ son compactos.

Se ha visto ya, que existe una relación entre la estructura algebraica de grupo de $GL_n(\mathbb{C})$ y su estructura topológica. Esto no es una mera coincidencia, pues por la manera en que se definió la topología sobre $GL_n(\mathbb{C})$ ambas estructuras resultan compatibles. Conpatibles en el sentido de que tanto el producto como la inversión en $GL_n(\mathbb{C})$ son operaciones continuas. De manera más general, si se tiene un grupo G dotado de una topología, en donde ambas estructuras son compatibles en el sentido señalado anteriormente, entonces se tiene lo que se llama un grupo topológico. Más precisamente:

Definición 4. Se llama grupo topológico a un conjunto G dotado, tanto de una estructura topológica como de una estructura de grupo, y en donde ambas estructuras son compatibles en el sentido siguiente:

i) El producto $p : G \times G \longrightarrow G$

$$(x,y) \longrightarrow p(x,y) = xy$$

es una aplicación continua

ii) La inversión $in : G \longrightarrow G$

$$x \longrightarrow in(x) = x^{-1}$$

es también una aplicación continua.

Las condiciones anteriores son equivalentes a la condición:

i') La aplicación $\rho : G \times G \longrightarrow G$

$$(x,y) \longrightarrow p(x,y) = xy^{-1}$$

es continua.

De esta forma, un conjunto que es a la vez un grupo y un espacio topológico es un grupo topológico si y sólo si sus estructuras topológica y algebraica satisfacen la condición i').

Como ejemplo de grupos topológicos tenemos:

1) El grupo aditivo de los números reales con la topología usual.

2) El círculo unitario visto como subconjunto del plano complejo. La operación de grupo en el círculo es el producto de números complejos unitarios, y la topología es la topología de subespacio.

3) Dado un grupo G, le damos la topología discreta. G es entonces un grupo discreto. Todo grupo discreto es un grupo topológico.

4) El grupo $GL_n(\mathbf{C})$, con el producto como operación de grupo, y la topología definida anteriormente.

Los grupos topológicos tienen una interesante propiedad. La topología de un grupo G puede describirse a partir de un sistema fundamental de vecindades, (o base de vecindades), del elemento neutro. Una justificación de este hecho puede darse con brevedad.

Para cada $x \in G$ definimos dos aplicaciones:

La translación izquierda de G respecto a x, T_x, definida por $T_x(g) = xg$, y la translación derecha de G respecto a x, ${}_xT$, definida por ${}_xT(g) = gx$.

Ambas translaciones son mapeos de G en G invertibles, además son continuas, aún más, son homeomorfismos. Entonces, si $\mathcal{U}$ es un sistema fundamental de vecindades del elemento neutro e, podemos obtener un sistema fundamental de vecindades de cualquier punto $x \in G$ aplicando cualquiera de las dos translaciones T_x o ${}_xT$. Lo anterior nos dice que la Topología del grupo G está determinada por cualquier sistema fundamental de vecindades del elemento e. Entonces, el conocimiento de los sistemas fundamentales de vecindades del neutro multiplicativo de un grupo topológico, nos da una valiosa información acerca de la estructura topológica del grupo.

Todo sistema fundamental de vecindades $\mathcal{U}$, del elemento neutro e, satisface las siguientes propiedades:

I. $\cap\{U : U \in \mathcal{U}\} = \{e\}$

II. Para cada $U, V \in \mathcal{U}$, existe $W \in \mathcal{U}$ tal que $W \in U \cap V$

III. Para cada $U \in \mathcal{U}$, existe $V \in \mathcal{U}$ tal que $V \cdot V \subset U$

IV. Para cada $U \in \mathcal{U}$, existe $V \in \mathcal{U}$ tal que $V^{-1} \subset U$

V. Para cada $U \in \mathcal{U}$ y $x \in U$, existe $V \in \mathcal{U}$ tal que $xV \in U$.

VI. Para cada $U \in \mathcal{U}$ y $x \in G$, existe $V \in \mathcal{U}$ tal que $xV_{x^{-1}} \subset U$

Inversamente, si tenemos un grupo G y una familia $\mathcal{U}$ de subconjuntos de G que satisfacen las propiedades I-VI, entonces las familias $\{xU : U \in \mathcal{U}\}$ y $\{Ux, U \in \mathcal{U}\}$, con $x \in G$, forman sistemas fundamentales de vecindades de x que generan una topología en G que lo convierte en un grupo topológico.

Heremos uso de la siguiente propiedad de un grupo topológico:

Dados $x \in G$, y U vecindad del elemento neutro e de un grupo topológico G, existe una vecindad V de x tal que $V^{-1}V \subset U$.

El aspecto que nos interesa de los grupos topológicos, es la manera en que estos actúan como grupos de transformaciones sobre espacios topológicos. De ahora en adelante, en esta sección, estudiaremos este aspecto y supondremos que los grupos topológicos con los cuales se trabaja son espacios Hausdorff.

De esta manera, sean G un grupo topológico y S un espacio topológico.

Definición 5. Decimos que G actúa continuamente sobre S, o que G es un grupo de transformaciones sobre S, si existe un mapeo continuo de $G \times S$ en S; $(g,x) \longrightarrow gs$, que satisface las siguientes condiciones:

i) $(ab)s = a(bs)$ $\qquad a,b \in G \quad s \in S$

ii) $es = s$ $\qquad s \in S$

Es inmediato a partir de la definición que si G actúa continuamente sobre S y $g \in G$, el mapeo $s \longrightarrow gs$ es un homeomorfismo de S en sí mismo. Este último hecho y la definición anterior, nos permiten introducir una relación de equivalencia en un espacio topológico provisto de la acción de un grupo G, de la siguiente manera:

Dado $s \in S$, el subconjunto de S, $Gs = \{gs : g \in G\}$, es llamado la órbita de s bajo G ó la G-órbita de s. Claramente, si $s_1, s_2 \in G$ la relación, $s_1 \sim s_2$ si y sólo si $s_1 = gs_2$ para alguna $g \in G$, es una relación de equivalencia cuyas clases de equivalencia son las órbitas de los elementos de S bajo la acción dada. Denotamos por $G\backslash S$ al conjunto de todas las G-órbitas de los elementos de S.

Sea $\Pi : S \longrightarrow G\backslash S$ la proyección canónica, a través de Π le damos al conjunto $G\backslash S$ una topología, la topología de identificación, definida por: $X \subset G\backslash S$ es abierto en $G\backslash S$ si y solo si $\Pi^{-1}(X)$ es abierto en S. Con esta topología Π es claramente continua, además es un mapeo abierto pues si Y es un abierto de S se tiene $\Pi^{-1}(\Pi(Y)) = \bigcup_{g \in G} gY$; como el mapeo $s \to gs$ es un homeomorfismo de S en si mismo gY es abierto para cada $g \in G$ y en consecuencia $\bigcup_{g \in G} gY$ es abierto.

Como ejemplo de la acción de un grupo sobre un espacio topológico, podemos considerar la acción que se obtiene de un grupo G sobre el espacio cociente de éste por un subgrupo cerrado. A saber: Sea K un subgrupo cerrado de un grupo topológico G. Consideremos la acción de K sobre G definida por la multiplicación por la derecha. Entonces la K-órbita de un elemento $g \in G$ es justamente la clase lateral izquierda gK en G/K, y de aquí que nuestro espacio $G\backslash K$ sea lo mismo que el conocido espacio cociente G/K con la topología cociente. Como es sabido, cuando el sub-grupo K es cerrado, el cociente resulta un espacio de Hausdorff, entonces podemos considerar ahora la acción del grupo G sobre el grupo G/K determinada por la aplicación $(g,xK) \to gxK$, $g \in G$, $x \in G$, de $G \times G/K$ en G/K, la cual es claramente continua.

Si un grupo topológico G actúa sobre un espacio topológico S, y el espacio $G\backslash S$ de las G-órbitas contiene solamente un elemento, S mismo, entonces diremos que G actúa transitivamente sobre S. Sean S un espacio de Hausdorff, y G un grupo topológico que actúa continua y transitivamente sobre S. Para cualquier punto fijo t de S ponemos

$K = \{g \in G : gt = t\}$. Entonces K es un subgrupo cerrado de G, y es llamado el subgrupo de isotropía de G en t. Existe un mapeo natural inyectivo $\lambda : G/K \longrightarrow S$ definido por $\lambda(gK) = gt$. Para cualquier subconjunto X de S, tenemos $\lambda^{-1}(X) = h(\{g \in G : gt \in X\})$, donde h es la proyección canónica de G en G/K. Esta igualdad muestra que $\lambda^{-1}(X)$ es abierto si X es abierto. Entonces λ es continua. Pero λ no es necesariamente un homeomorfismo. Sin embargo, se puede probar cuando menos el siguiente criterio.

Teorema 2. El mapeo $\lambda : G/K \longrightarrow S$ es un homeomorfismo si G y S son localmente compactos, y G tiene una base contable de conjuntos abiertos.

Dem: Sea X abierto de G/K. Entonces $h^{-1}(X)$ es abierto en G y $\lambda(X) = h^{-1}(X)t$, donde h es la proyección canónica. Lo anterior nos dice que es suficiente considerar un abierto U de G, un punto g de U, y entonces mostrar que gt es un punto interior de Ut. Tomemos una vecindad compacta V del elemento identidad de G tal que $V = V^{-1}$ y $gV^2 \subset U$. Si Vt contiene un punto interior vt con $v \in V$, entonces $gt = gv^{-1}vt$ es un punto interior de Ut. Veremos que Vt contiene efectivamente un punto interior. Por hipótesis. G es una unión $\bigcup_n g_n V$, donde $\{g_n\} \subset G$ es contable. Entonces $S = \bigcup_n g_n Vt$.

El Teorema de Baire, [4] capítulo XI, muestra que Vt debe contener un punto interior.

Proposición 1. Si G es un grupo topológico que actúa continuamente sobre un espacio de Hausdorff localmente compacto S, entonces $G\backslash S$ es compacto si y sólo si existe un subconjunto compacto C de S tal que $GC = S$.

Dem: Supongamos que $G\backslash S$ es compacto. La compacidad local de S nos permite cubrir a S con una familia de abiertos $\{U_i\}_{i\in I}$ cuyas cerraduras son compactas, entonces, tomando la proyección canónica Π tenemos $G\backslash S = \bigcup_{i\in I} \Pi(U_i)$, de donde $G\backslash S = \bigcup_{i=1}^{n} \Pi(U_i)$, lo que implica que $S = \bigcup_{i=1}^{n} G\bar{U}_i$. La continuidad del mapeo Π implica que $G\bar{U}_i$ es compacto para toda $i = 1,\dots,n$ y en consecuencia S es compacto. Inversamente, si $GC = S$ con C compacto de S entonces $\Pi(C) = G\backslash S$, la continuidad de Π implica que $G\backslash S$ es compacto.

Un subgrupo Γ de G es llamado discreto si la topología inducida sobre Γ es discreta.

Proposición 2. Sea Γ un subgrupo de G. Supongamos que la topología inducida sobre Γ es localmente compacta. Entonces Γ es cerrado en G. Especialmente, si Γ es discreto, entonces Γ es cerrado y no tiene puntos límites en G.

Dem. Sea C una vecindad compacta en Γ del elemento identidad e. Tomemos una vecindad abierta U de e en G tal que $U \cap \Gamma \subset C$. Tomemos ahora un elemento x de la cerradura de Γ. La estructura topológica de G nos permite encontrar una vecindad V de x tal que $V^{-1}V \subset U$. Entonces $(V\cap\Gamma)^{-1}(V \cap \Gamma) \subseteq V^{-1}V \cap \Gamma \subset U \cap \Gamma \subset C$. Como x está en la cerradura de Γ, $V \cap \Gamma \neq \emptyset$. Sea y en $V \cap \Gamma$, entonces $V \cap \Gamma \subset yC$. Ahora, para toda vecindad W de x tenemos $(W \cap V) \cap \Gamma = W\cap(V \cap \Gamma) \neq \emptyset$, entonces x pertenece a la cerradura de $V \cap \Gamma$. Como G es Hausdorff y yC es compacto, yC es cerrado, entonces $x \in yC \subset \Gamma$, de donde Γ es cerrado. Si Γ es discreto, entonces Γ es localmente compacto, y por lo tanto es cerrado.

Proposición 3. Sea G un grupo localmente compacto y K un subgrupo compacto de G. Pongamos $S = G/K$, y sea $h : G \to S$ la proyección. Si A es un subconjunto compacto de S, $h^{-1}(A)$ es compacto en G.

Dem: La hipótesis sobre G nos permite tomar una cubierta abierta $\{V_i\}_{i\in I}$ de G cuyos miembros tienen cerraduras compactas. Entonces si A es un subconjunto compacto de S, $A \subset \bigcup_{j=1}^{n} h(V_j)$. Tomando imagenes inversas $h^{-1}(A) \subset \bigcup_{j=1}^{n} \bar{V}_jK$. El teorema de Tychonoff nos dice que $\bar{V}_j x K$ es un subespacio compacto de GxG. La continuidad del producto implica entonces que $\bar{V}_jK$ es compacto en G. Por la proposición anterior

A es cerrado en S, en consecuencia la continuidad de h implica que $h^{-1}(A)$ es cerrado en G. Se ha mostrado que $h^{-1}(A)$ es un subespacio cerrado de un espacio compacto, por lo tanto $h^{-1}(A)$ es compacto.

Proposición 4. Sean G, K, S y h como en la proposición 3, y sea Γ un subgrupo de G. Entonces son equivalentes:

(1) Γ es un subgrupo discreto de G

(2) Si A y B son subconjuntos compactos de S, $\{g \in \Gamma : gA \cap B \neq \emptyset\}$ es finito.

Dem: Sean Γ un subgrupo discreto de G, A y B subconjuntos compactos de S, $C = h^{-1}(A)$, $D = h^{-1}(B)$, $g \in \Gamma$. Si $gA \cap B \neq \emptyset$ entonces $gC \cap D \neq \emptyset$ lo que implica que $g \in \Gamma \cap DC^{-1}$. Por la proposición 3, C y D son compactos, entonces, como se vió en la demostración de esta misma proposición, DC^{-1} es compacto. Si Γ es discreto, $\Gamma \cap DC^{-1}$ es compacto y discreto, entonces es finito. Inversamente, sea V una vecindad compacta de e en G, entonces $\Gamma \cap V \subset \{g \in \Gamma : gh(e) \cap h(V) \neq \emptyset\}$. Como K es compacto $h(K) = h(e)$ es compacto, de donde por la continuidad del producto $gh(e)$ es compacto. De la hipótesis se tiene que $\{g \in \Gamma : gh(e) \cap g(V) \neq \emptyset\}$ es finito, entonces $\Gamma \cap V$ es finito. Por lo tanto Γ es discreto.

Como se vió en la demostración de la proposición anterior, en S todos los puntos son compactos. Si Γ es un subgrupo discreto de G y G, K, S, y h son como en la proposición 3 se tiene el siguiente corolario a la proposición 4:

Corolario $\{g \in \Gamma : gz = z\}$ es un conjunto finito para toda $z \in S$.

Proposición 5. Sean G, K, S, y h como en la proposición 3, y sea Γ un subgrupo discreto de G. Entonces, para toda $z \in S$, existe una vecindad U de z tal que $\{g \in \Gamma : gU \cap U \neq \emptyset\} = \{g \in \Gamma : gz = z\}$.

Dem: Sea V una vecindad compacta de z. Por la proposición 4, $\{g \in \Gamma : gV \cap V \neq \emptyset\}$ es finito. Denotémoslo por $\{g_1, \ldots, g_r\}$. Supongamos que $g_i(z) = z$, para $1 \leq i \leq s$, y $g_i(z) \neq z$, para $s < i \leq r$. Como K es compacto, la proposición 2 muestra que S es un espacio de Hausdorff. Sean entonces, para todo $i > s$, V_i vecindad de z y W_i vecindad de $g_i z$ tales que $V_i \cap W_i = \emptyset$. Defínase $U = V \cap \{\bigcap_{i>s} (V_i \cap g_i^{-1} W_i)\}$. Claramente, $z \in U$ y $\{g \in \Gamma : gU \cap U \neq \emptyset\} \subset \{g_1, \ldots, g_r\}$. También es claro que $\{g_1, \ldots, g_s\} \subset \{g \in \Gamma : gU \cap U \neq \emptyset\}$. Si $i > s$, $g_i U \cap U = \emptyset$ en virtud de la condición $V_i \cap W_i = \emptyset$. Entonces $\{g_1, \ldots, g_s\} = \{g \in \Gamma : gU \cap U \neq \emptyset\}$ y $\{g \in \Gamma : gz = z\} \subset \{g \in \Gamma : gU \cap U \neq \emptyset\} \subset \{g \in \Gamma : gz = z\}$, de donde se tiene la proposición.

Con las mismas hipótesis de la proposición anterior tenemos:

Proposición 6. Si dos puntos z y w de S no son Γ-equivalentes, entonces existen vecindades U de z y V de w tales que $gU \cap V = \emptyset$ para todo $g \in \Gamma$.

Dem: Sean X y Y vecindades compactas de z y w respectivamente. Por la proposición 5, $\{g \in \Gamma : gX \cap Y \neq \emptyset\}$ es finito, digamos $\{g_1, \ldots, g_r\}$. Como z y w no son Γ-equivalentes, tenemos que $g_i z \neq w$, para toda i. Como S es Hausdorff podemos encontrar vecindades U_i de $g_i z$ y V_i de w tales que $U_i \cap V_i = \emptyset$. Pongamos $U = X \cap g_1^{-1} U_1 \cap \ldots\ldots \cap g_r^{-1} U_r$, $V = Y \cap V_1 \cap \ldots\ldots \cap V_r$. Por construcción, $gU \cap V = \emptyset$ para toda $g \in \Gamma$.

Esta última proposición implica que el espacio $\Gamma\backslash S$, es Hausdorff. Especificamente tenemos el siguiente:

Corolario Sea $\Gamma\backslash S$ el conjunto de todas las Γ-órbitas de los puntos de S. Entonces $\Gamma\backslash S$, con la topología de identificación, es un espacio de Hausdorff.

Dem: Si z y w son puntos de S no Γ-equivalentes, la proposición 6 nos asegura la existencia de vecindades U de z

y V de w tales que $gU \cap V = \emptyset$, para todo $g \in \Gamma$. Escrito de otra manera $\Gamma U \cap V = \emptyset$. Como la proyección Π es abierta tenemos que ΓU y ΓV son vecindades de Γz y Γw respectivamente. Finalmente, la condición $\Gamma U \cap V = \emptyset$ implica $\Gamma U \cap \Gamma V = \emptyset$.

1.2 *Transformaciones lineales fraccionales.*

Más adelante estudiaremos funciones definidas en la mitad superior del plano complejo. Estas funciones estarán determinadas por la acción de un subgrupo discreto Γ de $SL_2(\mathbb{R})$ sobre esta parte del plano complejo. En esta sección estudiaremos algunos elementos particulares de $SL_2(\mathbb{R})$, así como algunos elementos particulares de un subgrupo discreto Γ de $SL_2(\mathbb{R})$.

Consideremos primeramente una transformación lineal fraccional sobre $\mathbb{C} \cup \{\infty\}$. Dado un elemento $\sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ del grupo lineal general $GL_2(\mathbb{C})$, definimos la transformación $\sigma(z) = \frac{az+b}{cz+d}$, donde $z \in \mathbb{C} \cup \{\infty\}$. Supondremos que $\sigma(z)$ no es la transformación identidad. Como se sabe, [2] capítulo X, cualquier matriz compleja es similar a una matriz expresada en la forma canónica de Jordan. En consecuencia la matriz σ es similar a una de las dos siguientes formas:

$$\text{i)}\begin{bmatrix}\lambda & 1\\ 0 & \lambda\end{bmatrix} ; \qquad \text{ii)}\begin{bmatrix}\lambda & 0\\ 0 & \mu\end{bmatrix} , \lambda \neq \mu$$

Por lo tanto, la transformación $\sigma(z)$ es esencialmente de los dos tipos siguientes:

$$\text{i)}\ z \longrightarrow z + \lambda^{-1} \qquad \text{ii)}\ z \longrightarrow cz\ ,\ c \neq 1$$

En el primer caso, llamamos a σ parabólica. En el segundo caso, llamamos a σ elíptica si $|c| = 1$, hiperbólica si c es real y positivo, y loxodrónica en otro caso. Esta definición se aplica tanto a matrices como a transformaciones.

Ahora nos restringiremos a transformaciones generadas por matrices reales. Dado $z \in \mathbf{C}$ y $\alpha = \begin{bmatrix}p & q\\ r & s\end{bmatrix} \in GL_2(\mathbb{R})$, definimos:

(1) $j(\alpha, z) = rz + s.$

Si $w = \alpha(z)$, entonces:

(2) $\alpha \cdot \begin{bmatrix}z\\ 1\end{bmatrix} = \begin{bmatrix}pz + q\\ rz + s\end{bmatrix} = \begin{bmatrix}w\\ 1\end{bmatrix} \cdot j(\alpha, z)$

Y si $w' = \alpha(z')$:

$$\alpha \cdot \begin{bmatrix}z & z'\\ 1 & 1\end{bmatrix} = \begin{bmatrix}w & w'\\ 1 & 1\end{bmatrix}\begin{bmatrix}j(\alpha, z) & 0\\ 0 & j(\alpha, z')\end{bmatrix}$$

Sustituyendo $\bar{z}$ y $\bar{w}$ por z' y w', y tomando el determinante, obtenemos:

(3) $\det(\alpha)\ \mathrm{Im}(z) = \mathrm{Im}(\alpha(z))\,|j(\alpha, z)|^2$

Además de las relaciones anteriores, sobre todo de (3), nos interesa obtener la siguiente:

$$(4) \qquad j(\alpha\beta,z) = j(\alpha,\beta(z)) \cdot j(\beta,z) \quad ; \quad \alpha,\beta \in GL_2(\mathbb{R})$$

Justificamos esta relación:

Un cálculo directo nos muestra que $\alpha\beta(z)=\alpha(\beta(z))$. La relación (2) nos dice:

$$(a)\ \alpha\beta\begin{bmatrix} z \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha\beta(z) \\ 1 \end{bmatrix} \cdot j(\alpha\beta,z); \ (b)\ \alpha\begin{bmatrix} \beta(z) \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha(\beta(z)) \\ 1 \end{bmatrix} \cdot j(\alpha,\beta(z));$$

$$(c)\ \beta\begin{bmatrix} z \\ 1 \end{bmatrix} = \begin{bmatrix} \beta(z) \\ 1 \end{bmatrix} j(\beta,z).$$

Multiplicando en (c) por α y utilizando (b):

$$\alpha\beta\begin{bmatrix} z \\ 1 \end{bmatrix} = \alpha\begin{bmatrix} \beta(z) \\ 1 \end{bmatrix} \cdot j(\beta,z) = \begin{bmatrix} \alpha(\beta(z)) \\ 1 \end{bmatrix} \cdot j(\alpha,\beta(z)) \cdot j(\beta,z)$$

(a) implica:

$$\begin{bmatrix} \alpha\beta(z) \\ 1 \end{bmatrix} \cdot j(\alpha\beta,z) = \begin{bmatrix} \alpha(\beta(z)) \\ 1 \end{bmatrix} \cdot j(\alpha,\beta(z)) \cdot j(\beta,z).$$

Y por la observación hecha al principio:

$$j(\alpha\beta,z) = j(\alpha,\beta(z)) \cdot j(\beta,z)$$

Estas relaciones las utilizaremos en la siguiente sección y en el capítulo II. Regresando al grupo $SL_2(\mathbb{R})$, es necesario contar con un criterio que clasifique a los elementos parabólicos, elípticos e hiperbólicos de este grupo, en función de sus puntos fijos. Establecemos entonces la siguiente proposición:

Proposición 7. Sean $\sigma \in SL_2(\mathbb{R})$ $\sigma \neq \pm 1_2$, y $\Omega = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Entonces:

σ es parabólica $\Longleftrightarrow$ σ tiene un solo punto fijo en $\mathbb{R} \cup \{\infty\}$

elíptica $\Longleftrightarrow$ σ tiene un punto fijo z en Ω, y otro punto fijo fuera de Ω : $\bar{z}$.

hiperbólica $\Longleftrightarrow$ σ tiene dos puntos fijos en $\mathbb{R} \cup \{\infty\}$

Dem: El caso σ loxodrómica se omite pues la traza de uno de estos elementos no es real, y en consecuencia $SL_2(\mathbb{R})$ no contiene elementos loxodrómicos. Una justificación de este hecho la posponemos hasta la proposición 9. Ahora, observemos primeramente que si $z \in \Omega$, podemos encontrar un elemento τ de $SL_2(\mathbb{R})$ tal que $\tau(i) = z$. Por ejemplo, si $z = x + iy$ podemos tomar $\tau = y^{-1/2}\begin{bmatrix} y & x \\ 0 & 1 \end{bmatrix}$. Por otro lado, la transformación generada por la matriz τ^{-1}, es la inversa de la transformación generada por τ. La verificación de este hecho está sujeta simplemente a la realización de un cálculo directo. Si $\alpha = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{R})$, se tiene nuevamente por un cálculo directo, (estos cálculos se han omitido por ser rutinarios), que $\alpha(i) = i$ si y sólo si $p = s$, $q = -r$, $p^2 + q^2 = 1$. Si α satisface la condición anterior, entonces es un elemento del grupo ortogonal especial $SO(2)$. Siendo α un elemento de este grupo y $\tau \in SL_2(\mathbb{R})$ con la propiedad $\tau(i) = z$, se obtiene $\tau\alpha\tau^{-1}(z) = z$. Inversamente, si $\alpha \in SL_2(\mathbb{R})$ tiene la propiedad $\alpha(z) = z$, el elemento $\tau^{-1}\alpha\tau$ tiene la propiedad $\tau^{-1}\alpha\tau(i) = i$, y por lo tanto está en $SO(2)$, de aquí que $\alpha = \tau(\tau^{-1}\alpha\tau)\cdot\tau^{-1} \in \tau \cdot SO(2) \cdot \tau^{-1}$. Se ha probado entonces que $\tau \cdot SO(2) \cdot \tau^{-1} = \{\alpha \in SL_2(\mathbb{R}) : \alpha(z) = z\}$. Es claro que si α deja fijo a z, deja fijo a $\bar{z}$. Además, una transformación lineal fraccional, asociada a una matriz $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{R})$ distinta de $\pm 1_2$, no puede tener más de dos puntos fijos, pues un punto fijo de esta transformación satisface la ecuación $cz^2 + (d-a)z - b = 0$. Nos interesa saber de que tipo es una matriz cuya transformación lineal fraccional asociada tiene un punto fijo en Ω. Como se acaba de mostrar, una matriz con estas características es de la forma $\tau\gamma\tau^{-1}$, con $\tau \in SL_2(\mathbb{R})$ y $\gamma \in SO(2)$. Ahora, todo elemento de $SO(2)$ tiene raices características complejas conjugadas unitarias, pues todo elemento de este grupo es de la forma $\begin{bmatrix} \cos\theta & \operatorname{sen}\theta \\ -\operatorname{sen}\theta & \cos\theta \end{bmatrix}$, y las raíces características de estas matrices son de la forma $\cos\theta \pm i \operatorname{sen}\theta$, donde $\operatorname{sen}\theta \neq 0$. De aquí que los vectores característicos correspondientes son linealmente independientes. Todo esto nos dice que los vectores característicos de una matriz de la forma $\tau\gamma\tau^{-1}$, $\tau \in SL_2(\mathbb{R})$, $\gamma \in SO(2)$, son linealmente independientes. Para

ver esto observemos que todo vector característico y de $\tau\gamma\tau^{-1}$, genera un vector característico $\tau^{-1}(y)$ de γ, en consecuencia si y_1 y y_2 son vectores característicos de $\tau\gamma\tau^{-1}$, $\tau^{-1}(y_1)$ y $\tau^{-1}(y_2)$ son vectores característicos de γ, y por lo tanto son linealmente independientes. La linealidad de τ^{-1} implica que y_1 y y_2 también son linealmente independientes. La independencia lineal de los vectores característicos de una matriz de la forma $\tau\gamma\tau^{-1}$.
$\tau \in SL_2(\mathbb{R})$ $\gamma \in SO(2)$, implica que estos vectores generan al espacio vectorial $\mathbb{C}$. De acuerdo con esto, [2] capítulo IX, la matriz $\tau\gamma\tau^{-1}$ se puede diagonalizar y los elementos de la diagonal son las raíces características unitarias de esta matriz. Todo lo anterior arroja como resultado el hecho de que un elemento de $SL_2(\mathbb{R})$, distinto de $\pm 1_2$, con un punto fijo en Ω, es elíptico. Inversamente, si α es un elemento elíptico de $SL_2(\mathbb{R})$, entonces la transformación lineal fraccional asociada a α tiene sólo un punto fijo en Ω. Esto se deduce directamente de la definición. También se deduce de la definición y de lo probado anteriormente, que si α es un elemento parabólico de $SL_2(\mathbb{R})$ entonces la transformación lineal fraccional asociada a este elemento tiene sólo un punto fijo en $R \cup \{\infty\}$. Por otro lado, si $s \in \mathbb{R} \cup \{\infty\}$, definimos

$$F(s) = \{\alpha \in SL_2(\mathbb{R}) : \alpha(s) = s\},$$

$$P(s) = \{\alpha \in F(s) : \alpha \text{ es parabólico ó } = \pm 1_2\}$$

Como $SL_2(\mathbb{R})$ actúa transtitivamente sobre $\mathbb{R} \cup \{\infty\}$, podemos encontrar un elemento σ de $SL_2(\mathbb{R})$ tal que $\sigma(\infty) = s$. Entonces $F(s) = \sigma F(\infty)\sigma^{-1}$, $P(s) = \sigma P(\infty)\sigma^{-1}$. Ahora, la definición de $P(s)$ y la condición sobre el determinante de los elementos de $SL_2(\mathbb{R})$ nos dice que

$$F(\infty) = \{\begin{bmatrix} a & b \\ o & a^{-1} \end{bmatrix} : a \in \mathbb{R} - \{0\},\ b \in \mathbb{R}\},$$

$$P(\infty) = \{\pm\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} : h \in \mathbb{R}\} \cong \mathbb{R} \times \{\pm 1\}.$$

Esto muestra que si un elemento σ de $SL_2(\mathbb{R})$, $\neq \pm 1_2$, tiene al menos un punto fijo en $\mathbb{R} \cup \{\infty\}$, entonces σ es parabólico o hiperbólico. Si es parabólico, entonces tiene un punto fijo. Si tiene dos puntos fijos entonces debe ser hiperbólico, y si es hiperbólico debe tener dos puntos fijos. Esto termina la demostración.

Ahora consideremos un subgrupo discreto Γ de $SL_2(\mathbb{R})$, y denotemos por Ω a la mitad superior del plano complejo, es decir, $\Omega = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Un punto z de Ω es llamado un punto elíptico de Γ si existe un elemento elíptico σ de Γ tal que $\sigma(z) = z$. De manera semejante, un punto s de $\mathbb{R} \cup \{\infty\}$ es llamado un punto cúspide de Γ si existe un elemento parabólico τ de Γ tal que $\tau(s) = s$.

Tenemos los siguientes resultados relativos a puntos cúspides y elípticos de Γ.

Proposición 8. Si z es un punto elíptico de Γ, entonces $\{\sigma \in \Gamma : \sigma(z) = z\}$ es un grupo cíclico finito.

Dem: De la demostración de la proposición anterior se saben dos hechos. Existe $\tau \in SL_2(\mathbb{R})$ con la propiedad $\tau(i) = z$, y además $\tau \cdot SO(2) \cdot \tau^{-1} = \{\sigma \in SL_2(\mathbb{R}) : \sigma(z) = z\}$. Por lo tanto $\{\sigma \in \Gamma : \sigma(z) = z\} = \tau \cdot SO(2) \cdot \tau^{-1} \cap \Gamma$. Como Γ es discreto y $SO(2)$ es compacto, esta intersección debe ser un grupo finito. Ahora, $SO(2)$ es isomorfo a $\mathbb{R}/\mathbb{Z}$, y todos los subgrupos finitos de este grupo son cíclicos, de donde se obtiene la proposición.

Proposición 9. Sea s un punto cúspide de Γ, y $\Gamma_s = \{\sigma \in \Gamma : \sigma(s) = s\}$. Entonces $\Gamma_s/(\Gamma \cap \{\pm 1_2\})$ es isomorfo a $\mathbb{Z}$. Además, un elemento de Γ_s o es $\pm 1_2$, o es parabólico, es decir, $\Gamma_s = \Gamma \cap P(s)$.

Dem: Como se vió en la demostración de la proposición 7, $P(s)$ es isomorfo a $\mathbb{R} \times \{\pm 1\}$. Por lo tanto, $(P(s)\cap\Gamma)/\Gamma\cap\{\pm 1_2\}$ es isomorfo a un subgrupo discreto no trivial de $\mathbb{R}$, entonces es isomorfo a $\mathbb{Z}$. Ahora, $SL_2(\mathbb{R})$ no contiene elementos loxodrómicos, pues la traza de uno de estos elementos no es real. Para ver esto recordemos que una matriz loxodrómica es un elemento de $GL_2(\mathbb{C})$ similar a una matriz de la forma $\begin{bmatrix}\lambda & 0\\ 0 & \mu\end{bmatrix}$, $\lambda \neq \mu$, donde, si λ y μ son distintos de cero, $\frac{\lambda\bar{\mu}}{|\mu|^2}$ es negativo o complejo. Si σ es de esta forma, tiene determinante uno, entonces es de la forma $\begin{bmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{bmatrix}$. Supongamos que su traza $\mathrm{tr}(\sigma) = \lambda + \lambda^{-1}$ es real.

Si λ es real entonces σ es hiperbólica. Si λ es complejo, la condición sobre la traza implica que debe ser unitario. En este caso, λ y $\bar{\lambda}$ son las raíces de la ecuación $x^2 - \mathrm{tr}(\sigma)x + 1 = 0$, es decir $\lambda\bar{\lambda} = 1$, entonces, de acuerdo a la definición σ es elíptica. Lo anterior nos dice que una matriz loxodrónica no puede tener traza real. Entonces Γ no contiene elementos loxodrómicos. La proposición 7 implica que Γ tampoco contiene elementos elípticos. Como $SL_2(\mathbb{R})$ actúa transitivamente sobre $\mathbb{R} \cup \{\infty\}$, no se pierde generalidad si suponemos que $s = \infty$. Tomemos un generador $\sigma = \begin{bmatrix}\pm 1 & h\\ 0 & \pm 1\end{bmatrix}$, módulo $\pm 1_2$, del grupo $P(s)\cap\Gamma/\Gamma\cap\{\pm 1_2\}$. Según la proposición 7 y lo probado anteriormente esto es posible. Veremos que Γ_s no contiene elementos hiperbólicos. Supongamos que contiene un elemento hiperbólico $\tau = \begin{bmatrix}a & 0\\ 0 & a^{-1}\end{bmatrix}$, $|a| \neq 1$. Podemos suponer que $|a| < 1$. Entonces $\tau\sigma\tau^{-1} = \begin{bmatrix}\pm 1 & a^2h\\ 0 & \pm 1\end{bmatrix} \in P(s) \cap \Gamma$, según se ve en la demostración de la proposición 7. Pero $|a^2h| < |h|$, y el cociente de

$P(s) \cap \Gamma$ sobre $\Gamma \cap \{\pm 1_2\}$ es cíclico, entonces el elemento $\tau\sigma\tau^{-1}$ no puede estar en $P(s) \cap \Gamma$, lo que establece una contradicción. Lo anterior establece la contención $\Gamma_s \subset P(s) \cap \Gamma$, y en consecuencia $\Gamma_s = P(s) \cap \Gamma$, lo que completa la demostración de la proposición.

Proposición 10. Los elementos de Γ de orden finito son los elementos elípticos, así como $\pm 1_2$.

Dem: Si un elemento σ de $SL_2(\mathbb{R})$ es de orden finito, σ es conjugada en $SL_2(\mathbb{C})$ a una matriz $\begin{bmatrix} \beta & 0 \\ 0 & \bar{\beta} \end{bmatrix}$, con β una raíz de la unidad. Entonces, de acuerdo a la definición, σ es elíptica si $\beta \neq \pm 1$. Si σ es un elemento elíptico de Γ, entonces pertenece al grupo $\{\sigma \in \Gamma : \sigma(z) = z\}$, con $z \in \Omega$. Como este grupo es cíclico finito, σ es de orden finito.

Proposición 11. El conjunto de todos los puntos elípticos de Γ no tiene puntos límites en Ω.

Dem: Supongamos lo contrario. Sea $w \in \Omega$, y $\{z_n\}$ una sucesión de puntos elípticos distintos de Γ, que convergen a w. Por la proposición 5, podemos encontrar una vecindad U de w tal que, para $\gamma \in \Gamma$, $\gamma U \cap U \neq \emptyset$ si y sólo si $\gamma(w) = w$. La convergencia de la sucesión $\{z_n\}$ implica que existe $n \in \mathbb{N}$ tal que $z_n \in U$ y $z_n \neq w$. Como z_n es elíp tico, existe un elemento elíptico σ de Γ tal que $\sigma(z_n) = z_n$. Entonces $\sigma U \cap U \neq \emptyset$, consecuentemente $\sigma(w) = w$. Esto nos dice que σ, siendo elíptico, tiene dos puntos fijos en Ω, lo cual es imposible.

De entre los subgrupos discretos de $SL_2(\mathbb{R})$ tenemos al grupo $SL_2(\mathbb{Z})$, llamado el grupo modular. Dado un entero positivo N, definimos:

$$\Gamma_N = \Gamma(N) = \{\gamma \in SL_2(\mathbb{Z}) : \gamma \equiv 1_2 \ (\text{mód } N)\}$$
$$= \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : a \equiv d \equiv 1,\ b \equiv c \equiv 0 \ (\text{mód } N)\}.$$

Se verifica directamente que $\Gamma(N)$ es un subgrupo normal de $SL_2(\mathbb{Z})$. Este subgrupo es llamado el subgrupo de congruencia principal de nivel N de $SL_2(\mathbb{Z})$. En general, un subgrupo de $SL_2(\mathbb{Z})$ es llamado un subgrupo de congruencia de $SL_2(\mathbb{Z})$ si contiene a $\Gamma(N)$ para alguna N. Por ejemplo, tenemos una familia de subgrupos de congruencia de $SL_2(\mathbb{Z})$, que no son subgrupos normales de $SL_2(\mathbb{Z})$, definida de la siguiente manera:

Dado un entero positivo N, definimos

$$A_N = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}) : c \equiv 0 \text{ mód } (N)\}$$

$$y \quad \Gamma_o(N) = A_N \cap SL_2(\mathbb{Z}) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \text{ mód } (N)\}$$

A_N es un subanillo de $M_2(\mathbb{Z})$, y $\Gamma_o(N)$ es un subgrupo de $SL_2(\mathbb{Z})$ que contiene a $\Gamma(N)$.

1.3 El espacio topológico $\Gamma\backslash\Omega^*$.

Consideremos nuevamente un subgrupo discreto Γ de $SL_2(\mathbb{R})$. Por Ω^* denotaremos la unión de Ω y los puntos cúspides de Γ, entonces el conjunto Ω^* depende de Γ. Nuestro objetivo en esta sección, es hacer ver que tiene sentido hablar del "espacio $\Gamma\backslash\Omega^*$". En otras palabras, queremos dotar a Ω^* de una topología, de tal manera que Γ actúe continuamente sobre este espacio, y entonces estudiar algunas propiedades topológicas específicas de $\Gamma\backslash\Omega^*$.

Primero definimos la topología de Ω^*. Sea $z \in \Omega$, como sistema fundamental de vecindades abiertas de z, tomamos las usuales. Si $s \neq \infty$ es un punto cúspide de Γ, como sistema fundamental de vecindades abiertas de s tomamos los conjuntos de la forma:

$$\{s\} \cup \{\text{el interior de un círculo en } \Omega \text{ tangente al eje real en } s\}$$

Si ∞ es un punto cúspide de Γ, tomamos los conjuntos:

$$\{\infty\}\cup\{z \in \Omega : \operatorname{Im}(z) > c,\ c \in \mathbb{R},\ c > 0\}$$

como sistema fundamental de vecindades abiertas de ∞. La topología generada en Ω^* por estas familias de subconjuntos de Ω^* es Hausdorff. Ahora, puesto que el determinante de todos los elementos de Γ es positivo, la función $(\sigma,z) \longrightarrow \sigma(z)$, definida en $\Gamma \times \Omega$, mapea este espacio en Ω. Si s es un punto cúspide de Γ, entonces $\sigma(s)$ también es un punto cúspide de Γ, para cualquier $\sigma \in \Gamma$. Para ver esto simplemente considérese el elemento $\sigma\tau\sigma^{-1}$ de Γ, donde τ es un elemento parabólico de Γ con la propiedad $\tau(s) = s$. Es fácil ver que el elemento $\sigma\tau\sigma^{-1}$ es parabólico. Entonces el mapeo anterior manda los puntos cúspides de Γ en si mismos. Esto establece que la función $(\sigma,z) \to \sigma(z)$ manda el espacio $\Gamma \times \Omega^*$ en Ω^*. Este mapeo es continuo y satisface las condiciones i) $\sigma\gamma(z) = \sigma(\gamma(z))$; $\sigma,\gamma \in \Gamma$, $z \in \Omega^*$; ii) $1_2(z) = z$; $1_2 \in \Gamma$, $z \in \Omega^*$. Por lo tanto Γ actúa continuamente sobre Ω^*. Observemos que Ω^* no es localmente compacto, a menos que $\Omega^* = \Omega$.

Como en la sección pasada, si s es un punto cúspide de Γ, definimos los conjuntos:

$$P(s) = \{\alpha \in SL_2(\mathbb{R}) : \alpha(s) = s,\ \alpha \text{ parabólico ó } \pm 1_2\}$$

$$\Gamma_s = \{\gamma \in \Gamma : \gamma(s) = s\} = P(s) \cap \Gamma$$

Para estudiar la estructura topológica de $\Gamma\backslash\Omega^*$, supondremos que ∞ es un punto cúspide de Γ. Recordemos la igualdad (3) probada en la sección 1.2:

$$(3) \qquad \mathrm{Im}(\alpha(z)) = \det(\alpha)\cdot\mathrm{Im}(z)/|cz+d|^2 \qquad \alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})$$

Dado $\sigma \in \Gamma$, denotamos por c_σ la entrada izquierda inferior de la matriz σ. Entonces $\Gamma_\infty = \{\sigma \in \Gamma; c_\sigma = 0\}$. Por la proposición 9, podemos encontrar un generador $\pm\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}$ de Γ_∞ módulo $\pm 1_2$.

La topología que vamos a considerar sobre $\Gamma\backslash\Omega^*$, es la topología de identificación, que fué definida en la sección 1.1. La propiedad topológica más importante que nos interesa del espacio $\Gamma\backslash\Omega^*$, es el axioma de separación T_2. Para verificar que efectivamente el espacio $\Gamma\backslash\Omega^*$ satisface el axioma T_2, estableceremos algunos lemas previos.

Lema 1. Dado $M > 0$, existen solamente un número finito de clases dobles $\Gamma_\infty\,\sigma\,\Gamma_\infty$ tales que $\sigma \in \Gamma$ y $|c_\sigma| < M$

Dem: Las clases dobles $\Gamma_\infty\,\sigma\,\Gamma_\infty$, $\sigma \in \Gamma$, forman una partición de Γ. En vista de que $\Gamma_\infty = \{\sigma \in \Gamma : c_\sigma = 0\}$, es suficiente considerar solamente aquellas σ para las cuales $c_\sigma \neq 0$. Tomemos un generador $\tau = \pm\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}$ de Γ_∞ módulo $\pm 1_2$. La idea de la demostración es asociar a cada clase do ble $\Gamma_\infty \sigma \Gamma_\infty$, $\sigma \in \Gamma$, $o \neq |c_\sigma| \leq M$, un elemento σ'' de la misma clase doble y entonces hacer ver que el conjunto de los elementos asociados es finito.

Sea $\sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$, $o \neq |c| \leq M$. Vamos a encontrar un elemento σ'' en $\Gamma_\infty \sigma \Gamma_\infty$ tal que $\sigma''(i)$ esté contenido en un compacto K que dependa solamente de M y h. Sea n un entero tal que $1 \leq d + nhc \leq 1 + |hc|$. Pongamos $\sigma' = \sigma\tau^n = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$. Entonces $|c'| = |c|$, $|d'| = d+nhc$. Por la igualdad (3) de la sección 1.1, $\mathrm{Im}(\sigma'(i)) = 1/(c'^2+d'^2)$. Tenemos entonces $1 \leq |d'| \leq 1 + |hc|$, y $|c| \leq M$, y de aquí que $1 \leq c'^2 + d'^2 \leq M^2 + (1 + |h|M)^2$. Por lo tanto $\sigma'(i)$ pertenece al dominio:

$$(5) \qquad 1 \geq \mathrm{Im}(z) \geq 1/[M^2 + (1 + |h|M)^2]$$

Ahora, la transformación $z \longrightarrow \tau^m(z) = z + mh$ no cambia la parte imaginaria de z. Podemos tomar m tal que $\tau^m\sigma'(i)$ satisfaga la desigualdad (5) y la condición

$$(6) \qquad o \leq \mathrm{Re}(z) \leq |h|$$

Las desigualdades (5) y (6) definen un subconjunto compacto de Ω, y el elemento $\sigma'' = \tau^m\sigma\tau^n$ tiene la propiedad $\sigma''(i) \in K$. En virtud de la proporción 4, solo existen un número finito de estas σ'' en Γ.

Lema 2. Existe un número positivo r, que depende solamente de Γ, tal que $|c_\sigma| \geq r$ para todo $\sigma \in \Gamma - \Gamma_\infty$. Además, para esta r, se tiene $\mathrm{Im}(z) \cdot \mathrm{Im}(\sigma(z)) \leq 1/r^2$ para todo $z \in \Omega$ y todo $\sigma \in \Gamma - \Gamma_\infty$.

Dem: Por el lema 1, dado $M > 0$, existen solamente un número finito de clases dobles $\Gamma_\infty \sigma \Gamma_\infty$, con $\sigma \in \Gamma$ y $|c_\sigma| \leq M$. Observando que todo elemento τ de una de estas clases satisface también la desigualdad $|c_\tau| \leq M$ (de hecho, si $\tau \in \Gamma_\infty \sigma \Gamma_\infty$, tenemos $c_\tau = c_\sigma$) podemos considerar el número $r = \min \{|c_\sigma| : \sigma$ es representante de una clase doble $\Gamma_\infty \sigma \Gamma_\infty$, con las propiedades $\sigma \in \Gamma - \Gamma_\infty$ y $|c_\sigma| \leq M\}$. Entonces, para todo $\sigma \in \Gamma - \Gamma_\infty$, se obtiene $|c_\sigma| \geq r$. Por otro lado, si $\sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ y $c \neq 0$, tenemos nuevamente por la igualdad (3) de la sección 1.1:

$$\mathrm{Im}(\sigma(z)) = \mathrm{Im}(z) \ |cz+d|^{-2} \leq \mathrm{Im}(z)(c\ \mathrm{Im}(z))^{-2} \leq r^{-2}\mathrm{Im}(z)^{-1}$$

de donde se obtiene la desigualdad deseada.

Lema 3. Para todo punto cúspide s de Γ, existe una vecindad $\mathcal{U}$ de s en Ω^* tal que $\Gamma_s = \{\sigma \in \Gamma : \sigma\mathcal{U} \cap \mathcal{U} \neq \emptyset\}$.

Dem: Sea s un punto cúspide de Γ. Como se vió en la demostración de la proposición 7, el conjunto $P(s)$ se puede expresar en términos de $P(\infty)$ en la forma $P(s) = \sigma P(\infty)\sigma^{-1}$, donde σ tiene la propiedad $\sigma(\infty) = s$ y $\sigma \in SL_2(\mathbb{R})$. Esto nos dice que no se pierde generalidad si suponemos que $s = \infty$. Sea $\mathcal{U} = \{z \in \Omega^* : \mathrm{Im}(z) > 1/r\}$, donde r tiene la propiedad del lema 2. Si $\sigma \in \Gamma - \Gamma_\infty$ y $z \in \mathcal{U}$, tenemos, por el lema 2, $\mathrm{Im}(\sigma(z)) < 1/r$. Por lo tanto si $\sigma \in \Gamma$, $z \in \mathcal{U}$ y $\sigma(z) \in \mathcal{U}$, entonces $\sigma \in \Gamma_\infty$. Lo anterior establece la contención $\{\sigma \in \Gamma : \sigma\mathcal{U} \cap \mathcal{U} \neq \emptyset\} \subset \Gamma_\infty$. La otra contención es clara.

Obsérvese que dos puntos de $\mathcal{U}$ son equivalentes bajo Γ sólo si lo son bajo Γ_s, y entonces $\Gamma_s \backslash \mathcal{U}$ puede identificarse con un subconjunto de $\Gamma \backslash \Omega^*$; además $\mathcal{U}$ no contiene puntos elípticos de Γ.

<u>*Lema 4.*</u> Para todo punto cúspide s de Γ y para todo subconjunto compacto K de Ω, existe una vecindad $\mathcal{U}$ de s tal que $\mathcal{U} \cap \gamma K = \emptyset$ para todo $\gamma \in \Gamma$.

Dem: Nuevamente, no se pierde generalidad si se supone que $s = \infty$. Como la función $z \to \mathrm{Im}(z)$, de Ω en $\mathbb{R}^+$, es continua, existen A y B números positivos tales que $A < \mathrm{Im}(z) < B$ para todo $z \in K$. Sea r un número positivo con la propiedad del lema 2. Entonces definimos:

$$\mathcal{U} = \{z \in \Omega^* : \mathrm{Im}(z) > \mathrm{Max}(B, 1/Ar^2)\}$$

Sea $z \in K$. Por el lema 2, si $\sigma \in \Gamma - \Gamma_\infty$, $\mathrm{Im}(\sigma(z)) < 1/Ar^2$.

Si $\sigma \in \Gamma_\infty$, $\mathrm{Im}(\sigma(z)) = \mathrm{Im}(z) < B$. Entonces U tiene la propiedad deseada.

Ahora veremos que el espacio $\Gamma \backslash \Omega^*$, es Hausdorff.

Teorema 3. El espacio $\Gamma\backslash\Omega^*$, con la topología de identificación, es un espacio Hausdorff.

Dem: Como se vió en la demostración de la proposición 7, un elemento α del grupo $SL_2(\mathbb{R})$ tiene la propiedad $\alpha(i)$ si y sólo si, pertenece al grupo ortogonal especial $SO(2)$. Por lo tanto el grupo $SO(2)$ es el subgrupo de isotropía de $SL_2(\mathbb{R})$ en i. Se puede observar que la acción de $SL_2(\mathbb{R})$ sobre Ω es transitiva, puesto que dado $z \in \Omega$, $z = ai + b$, la transformación lineal fraccional generada por la matriz $a^{-1/2}\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$, manda i a z. Entonces, por el Teorema 2, Ω es homeomorfo a $SL_2(\mathbb{R})/SO(2)$. Aplicando ahora el corolario de la proposición 6, obtenemos que $\Gamma\backslash\Omega$ es un espacio Hausdorff. Como $\Gamma\backslash\Omega$ es la unión de $\Gamma\backslash\Omega$ y las clases de equivalencia de los puntos cúspides de Γ, resta mostrar que la clase de equivalencia de un punto cúspide puede separarse de las clases de equivalencia de puntos de Ω, y también de la clase de equivalencia de otro punto cúspide. El Lema 4 revuelve el primer caso, en virtud de que la proyección $\Pi:\Omega^* \to \Gamma\backslash\Omega^*$ es abierta y continua. Para resolver el segundo caso, tenemos dos puntos cúspides s y t de Γ que no sean Γ-equivalentes. Nuevamente, no se pierde generalidad si suponemos que alguno de los dos puntos, digamos t, es el ∞. Como antes, también, sea $\pm\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}$ un generador de Γ_∞ módulo $\pm 1_2$. Se definen tres conjuntos:

$$L = \{z \in \mathbb{C} : \operatorname{Im}(z) = u\}$$

$$K = \{z \in L : 0 \leqslant \operatorname{Re}(z) \leqslant |h|\}$$

$$V = \{z \in \Omega^* : \operatorname{Im}(z) > u\}$$

donde u es un número positivo. Como K es compacto, existe, por el Lema 4, una vecindad $\mathcal{U}$ de s tal que $K \cap \Gamma\mathcal{U} = \emptyset$. Podemos suponer que la frontera de $\mathcal{U}$ es un círculo tangente al eje real $\mathbb{R}$. Vamos a mostrar que $V \cap \Gamma\mathcal{U} = \emptyset$. Supongamos lo contrario. Es decir, supongamos que $\gamma\mathcal{U} \cap V \neq \emptyset$ para algún $\gamma \in \Gamma$. Como γ es un homeomorfismo de Ω^* en si mismo para todo $\gamma \in \Gamma$, la frontera de $\gamma\mathcal{U}$ es un círculo tangente al eje real. Por lo tanto, si $\gamma\mathcal{U} \cap V \neq \emptyset$, entonces $\gamma\mathcal{U} \cap L \neq \emptyset$, de aquí que $\gamma\mathcal{U}$ intersecta a alguna translación de K por un elemento de Γ_∞, es decir, existe un elemento δ de Γ_∞ tal que $\gamma\mathcal{U} \cap \delta K \neq \emptyset$. Entonces $\delta^{-1}\gamma\mathcal{U} \cap K \neq \emptyset$, lo cual no es posible. Esto completa la prueba.

Proposición 12. El espacio $\Gamma\backslash\Omega^*$ es localmente compacto.

Dem: Como la proyección $\Pi : \Omega \longrightarrow \Gamma\backslash\Omega$ es un mapeo abierto y continuo, y Ω es localmente compacto, el espacio $\Gamma\backslash\Omega$ resulta ser localmente compacto. Entonces solamente resta mostrar que si s es un punto cúspide de Γ y si Π denota ahora la proyección de Ω^* en $\Gamma\backslash\Omega^*$, $\Pi(s)$ tiene una vecindad compacta. Como antes, podemos suponer que $s = \infty$. Por el Lema 3 y la observación hecha al final de éste, existe una vecindad $V = \{z \in \Omega^* : \mathrm{Im}(z) \geq c\}$, donde c es un real positivo, tal que $\Gamma_\infty\backslash V$ se identifica con $\Pi(V)$. Sea $\pm\begin{bmatrix}1 & h\\0 & 1\end{bmatrix}$ un generador de Γ_∞ módulo $\pm 1_2$. Dado un elemento z de V, existe un entero n tal que $(n-1)|h| \leq \mathrm{Re}(z) \leq n|h|$. En consecuencia $0 \leq \mathrm{Re}(z) - (n-1)|h| \leq |h|$, entonces la matriz $\pm\begin{bmatrix}1 & \mp(n-1)h\\0 & 0\end{bmatrix}$ manda a z dentro del conjunto $\{z \in V : z = \infty$ ó $0 \leq \mathrm{Re}(z) \leq |h|\}$. Esto muestra que $\Pi(v)$ coincide con la imagen de $\{z \in V : z = \infty$ ó $0 \leq \mathrm{Re}(z) \leq |h|\}$ bajo Π. Ahora, si se considera una cubierta abierta de este último conjunto formada por abiertos de Ω^*, siempre se puede extraer una subcubierta finita, puesto que todo subconjunto de Ω que es compacto con la topología usual, también es compacto en Ω^* con la topología definida anteriormente. En otras palabras, $\{z \in V : z = \infty$ ó $0 \leq \mathrm{Re}(z) \leq |h|\}$ es compacto, y por lo tanto $\Pi(V)$ también es compacto. Esto termina la demostración.

Se tiene además los siguientes resultados referentes al número de clases de equivalencia de puntos cúspides y elípticos de Γ, así como del número de elementos parabólicos de Γ, cuando se conocen propiedades topológicas de los espacios $\Gamma\backslash\Omega^*$ y $\Gamma\backslash\Omega$.

Proposición 13. Si $\Gamma\backslash\Omega^*$ es compacto, entonces el número de puntos cúspides (resp. puntos elípticos) no equivalentes bajo Γ es finito.

Dem: Sea C (resp. E) el conjunto de los puntos cúspides (resp. puntos elípticos) de Γ. Por la proposición 5, para cada $z \in \Omega$, existe una vecindad U_z de z en Ω tal que $U_z \cap E$ o es el vacío, o posiblemente $\{z\}$. Para cada $s \in C$, podemos encontrar una vecindad U_s de s que no contenga puntos elípticos. Esto es posible en virtud del Lema 3. Si Π denota la proyección de Ω^* en $\Gamma\backslash\Omega^*$, y si $\Gamma\backslash\Omega^*$ es compacto, podemos elegir un número finito de conjuntos de la forma $\Pi(U_z)$ ó $\Pi(U_s)$ que cubra a $\Gamma\backslash\Omega^*$. Entonces el número de puntos en $\Pi(C)$ (resp. $\Pi(E)$) es a lo más el número de $\Pi(U_z)$ (resp. $\Pi(U_s)$), que cubren a $\Gamma\backslash\Omega^*$.

Proposición 14. Si $\Gamma\backslash\Omega$ es compacto, entonces Γ no tiene elementos parabólicos.

Dem: Sea Π la proyección de Ω en $\Gamma\backslash\Omega$. Supongamos que ∞ es un punto cúspide de Γ. Consideremos una sucesión infi nita $\{z_n\}$ de puntos de Ω tal que $\mathrm{Im}(z_n) \longrightarrow \infty$. Por el Lema 3, existe una vecindad

$$U = \{z \in \Omega^* : \mathrm{Im}(z) > c\}$$

de ∞ tal que $\Gamma_\infty = \{\gamma \in \Gamma : \gamma U \cap U \neq \emptyset\}$. Entonces, a partir de cierto índice $z_n \in U$. Como ningún elemento de Γ_∞ cambia $\mathrm{Im}(z)$, si dos puntos de $\{z_n\}$ tienen partes imaginarias distintas y suficientemente grandes, entonces no son equivalentes bajo Γ. Por lo tanto $\{\Pi(z_n)\}$ contiene una sucesión infinita de puntos distintos de $\Gamma\backslash\Omega$. Si $\Gamma\backslash\Omega$ es compacto, existe un punto $w \in \Omega$ tal que $\Pi(w)$ es un punto límite de $\{\Pi(z_n)\}$. Sea K una vecindad compacta de w. Por el Lema 4, existe una vecindad V de ∞ tal que $K \cap \Gamma V = \emptyset$. Esto es una contradicción, pues $\Pi(z_n) \in \Pi(K) \cap \Pi(V)$ para n suficientemente grande.

Hemos visto que $\Gamma\backslash\Omega^*$ es un espacio Hausdorff. Veremos que sobre este espacio se puede definir una estructura de variedad analítica compleja que lo convierte en una superficie de Riemann.

1.4 El espacio $\Gamma\backslash\Omega^*$ como superficie de Riemann.

Como en la sección anterior, Γ denotará un subgrupo discreto de $SL_2(\mathbb{R})$, y Ω^* la unión de Ω y los puntos cúspides de Γ. Como es sabido, cuando un espacio es localmente euclideano es posible introducir el concepto de diferenciabilidad para funciones definidas sobre este espacio. La propiedad de diferenciabilidad de una función resulta importante porque nos permite estudiar el comportamiento local de la función. Esto justifica nuestro interés en introducir una estructura compleja de variedad analítica sobre $\Gamma\backslash\Omega^*$. Recordemos lo que una superficie de Riemann significa.

Por una superficie de Riemann, entendemos una variedad analítica compleja conexa de una dimensión. Siendo más precisos, una superficie de Riemann es un espacio de Hausdorff conexo M sobre el cual está definida una estructura compleja S que satisface las siguientes propiedades:

(1) S es una colección de parejas $\{U_\alpha, P_\alpha\}_{\alpha\in A}$, donde $\{U_\alpha\}_{\alpha\in A}$ es una cubierta abierta de M, y P_α es un homeomorfismo de U_α en un subconjunto abierto del plano complejo $\mathbb{C}$.

(2) Si $U_\alpha \cap U_\beta \neq \emptyset$, entonces el mapeo

$$P_\beta \circ P_\alpha^{-1} : P_\alpha(U_\alpha \cap U_\beta) \longrightarrow P_\beta(U_\alpha \cap U_\beta)$$

es holomorfo.

(3) S es máxima bajo las condiciones (1) y (2).

La condición (3) no es esencial, pues dada cualquier familia S que satisfaga (1) y (2), existe una única estructura compleja S' que contiene a S. A saber, S' esta dada como el conjunto de parejas (V, q) formados por un subconjunto abierto V de M y un homeomorfismo q de V en un subconjunto abierto de plano complejo $\mathbb{C}$ tal que $P_\alpha \circ q^{-1}$ y $q \circ P_\alpha^{-1}$ son holomorfos cuando $V \cap U_\alpha \neq \emptyset$.

Vamos a definir una estructura compleja sobre $\Gamma\backslash\Omega^*$. Sea Π la proyección de Ω^* en $\Gamma\backslash\Omega^*$. Para cada $\nu \in \Omega^*$ consideremos

$$\Gamma_\nu = \{\gamma \in \Gamma : \gamma\nu = \nu\}$$

Por la Proposición 5 y el Lema 3, existe una vecindad abierta U de ν tal que

$$\Gamma_\nu = \{\gamma \in \Gamma : \gamma U \cap U \neq \emptyset\}$$

La observación hecha al final del Lema 3 nos da una inclusión $\Gamma_\nu\backslash U \longrightarrow \Gamma\backslash\Omega^*$. Considerando la acción de Γ_ν sobre U, se obtiene que $\Gamma_\nu\backslash U$ es una vecindad abierta de $\Pi(\nu)$ en $\Gamma\backslash\Omega^*$. La Proposición 7 nos dice que si ν no es ni un punto elíptico, ni un punto cúspide de Γ, entonces Γ_ν contiene solamente al elemento neutro 1_2 y posiblemente, cuando más, al elemento -1_2. Entonces, como el mapeo Π es abierto y contínuo, la restricción $\Pi : U \longrightarrow \Gamma_\nu \backslash U$ es un homeomorfismo. Para esta ν tomamos a $(\Gamma_\nu \backslash U, \Pi^{-1})$ como un miembro de la estructura compleja de $\Gamma \backslash \Omega^*$.

Si ν es un punto elíptico, consideramos el grupo de transformaciones $(\Gamma_\nu \cdot \{\pm 1\}/\{\pm 1\})$. Denotaremos a este grupo por $\overline{\Gamma}_\nu$. Sea λ un isomofismo holomorfo de Ω sobre el disco unitario D tal que $\lambda(\nu) = 0$. Por la proposición 8, Γ_ν es un grupo cíclico finito. Por lo tanto el grupo $\overline{\Gamma}_\nu$ también es cíclico finito. Si n es el orden de $\overline{\Gamma}_\nu$, entonces $\lambda\overline{\Gamma}_\nu\lambda^{-1}$ consiste de las transformaciones

$$w \longrightarrow \xi^k w \qquad k = 0,\ldots\ldots,n-1, \quad \xi = e^{2\Pi i/n}$$

Definimos ahora un mapeo $p : \Gamma_\nu \backslash U \longrightarrow \mathbf{C}$ dado por $p(\Pi(z)) = \lambda(z)^n$. Este mapeo está bien definido. En efecto, si $z, z' \in U$ y $\Pi(z') = \Pi(z)$, entonces existe $\alpha \in \Gamma_\nu$ tal que $\alpha(z) = z'$, de donde $p(\Pi(z')) = \lambda(\alpha(z))^n$. Por otro lado existe $y \in D$ tal que $z = \lambda^{-1}(y)$. De aquí que $p(\Pi(z')) = \lambda(\alpha(\lambda^{-1}(y)))^n = (\xi^k y)^n$ para alguna $0 \leqslant k \leqslant n-1$, y entonces $p\Pi(z')) = y^n = \lambda(z)^n = p(\Pi(z))$. Además p es inyectivo pues si z y z' son elementos de U tales que $p(\Pi(z))=p(\Pi(z'))$, entonces $\lambda(z)^n = \lambda(z')^n$ lo cual significa que $\lambda(z)$ y $\lambda(z')$ son raíces n-ésimas de un mismo número complejo unitario.

Esto implica que existe $0 \leq k \leq n-1$ tal que $\lambda(z') = \xi^k\lambda(z)$ $\xi = e^{2\Pi i/n}$. Entonces existe también $\alpha \in \Gamma_\nu$ tal que $\lambda\, \alpha\, \lambda^{-1}(\lambda(z)) = \lambda(z')$, y por lo tanto $\alpha(z) = z'$, es decir $\Pi(z) = \Pi(z')$. La inyectividad de p nos permite encontrar una aplicación $q: \mathrm{Im}(p) \longrightarrow \Gamma_\nu\backslash\mathcal{U}$, ($\mathrm{Im}(p)$ = Imagen de p), dada por $q(w) = \Pi(\lambda^{-1}(w^{1/n}))$* tal que $p \circ q = 1_{\mathrm{Im}(p)}$ y $q \circ p = 1_{\Gamma_\nu\backslash\mathcal{U}}$. El siguiente diagrama conmutativo nos dice que p es un homeomorfismo de $\Gamma_\nu\backslash\mathcal{U}$ en $\mathrm{Im}(p)$**; que a saber es un subconjunto abierto de $\mathbb{C}$.

$$\begin{array}{ccc} \Gamma_\nu\backslash\mathcal{U} & \underset{q}{\overset{p}{\rightleftarrows}} & \mathbb{C} \\ {\scriptstyle\Pi}\nwarrow & & \nearrow{\scriptstyle\lambda^n} \\ & \mathcal{U} & \end{array}$$

Incluimos a $(\Gamma_\nu\backslash\mathcal{U}, p)$ en nuestra estructura compleja.

Si s es un punto cúspide de Γ, tomemos un elemento ρ de $SL_2(\mathbb{R})$ tal que $\rho(s) = \infty$. Esto es posible porque la acción de $SL_2(\mathbb{R})$ sobre $\mathbb{R} \cup \{\infty\}$ es transitiva. Entonces de la demostración de la proposición 7 y de la proposición 9 tenemos

$$\rho\Gamma_s\rho^{-1} \cdot \{\pm 1\} = \{\pm \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}^m : m \in \mathbb{Z}\}$$

* Al definir la aplicación q estamos considerando la elección de una rama de la función raíz n-ésima, para que ésta sea efectivamente una función. Esto no es indispensable, pues como se vió los n valores de la raíz n-ésima de un complejo en el disco unitario son equivalentes a través de λ, bajo Γ_ν en $\mathcal{U}$.

** Hay que tomar en cuenta el teorema del mapeo abierto. Ver por ejemplo [1], capítulo IV. (Aquí aparece como corolario del Teorema 11).

con h un real positivo. Si definimos un mapeo $p : \Gamma_s \backslash U \to \mathbb{C}$ por $p(\Pi(z)) = \exp[2\Pi i \rho(z)/h]$ vemos que p mapea $\Gamma_s \backslash U$ en un subconjunto abierto de $\mathbb{C}$. Procediendo de manera análoga a como se procedió en el caso de los puntos elípticos, se prueba que p es una aplicación bien definida y que es un homeomorfismo de $\Gamma_s \backslash U$ en su imagen. Incluimos a $(\Gamma_s \backslash U, p)$ en nuestra estructura compleja.

Esta estructura compleja satisface claramente la condición (2). Para que $\Gamma \backslash \Omega^*$ sea una superficie de Riemann sólo falta verificar que este espacio es conexo. Evidentemente, Ω^* con la topología definida en la sección anterior es un espacio conexo. Como la proyección $\Pi : \Omega^* \longrightarrow \Gamma \backslash \Omega^*$ es continua tenemos que $\Gamma \backslash \Omega^*$ es conexo.

Si Γ es un subgrupo discreto de $SL_2(\mathbb{R})$ (o de $SL_2(\mathbb{R})/\{\pm 1_2\}$) tal que el espacio $\Gamma \backslash \Omega^*$ es compacto, entonces Γ será llamado un grupo Fuchsiano de la primera clase. Dotado de la estructura compleja definida anteriormente, $\Gamma \backslash \Omega^*$ se convierte en una superficie de Riemann compacta.

CAPITULO II

Las formas automorfas y las funciones zeta definidas para campos de números algebraicos, han sido usadas para estudiar los enteros en estos campos.

En el siglo XIX la importancia aritmética de las formas automorfas fué claramente reconocida, y ejemplos de estas formas fueron usados con gran efecto en la teoría de los números.

Alrededor de 1830, Jacobi trabajó con la función theta $\theta(z)$ para obtener fórmulas exactas para la representación numérica de n como suma de r cuadrados. Treinta años más tarde, Riemann explotó esta misma función para derivar la continuación analítica y la ecuación funcional de su famosa función zeta $\zeta(s)$.

El propósito de este capítulo es presentar algunos resultados clásicos sobre las formas automorfas.

§2.1 *Formas automorfas, dominio fundamental.*

Sea Γ un grupo Fuchsiano de la primera clase. Es de interés estudiar aquellas funciones meromorfas sobre Ω que son invariantes bajo todas las transformaciones de Γ, esto es, las funciones f tales que $f(\gamma(z)) = f(z)$, para toda $\gamma \in \Gamma$. Esto, por supuesto, es bastante restrictivo. Entonces, en lugar de considerar estas funciones, consideraremos aquellas funciones meromorfas $f(z)$ tales que $f(\gamma(z))$ y $f(z)$ tengan los mismos polos y los mismos ceros, para todo $\gamma \in \Gamma$. En este caso, $f(\gamma(z))/f(z) = \mu_\gamma(z)$ es una función holomorfa sobre Ω que nunca se anula, (el cociente $f(\gamma(z))/f(z)$ se define por continuidad en las singularidades de $f(z)$. Como naturalmente estamos suponiendo que $f(z)$ no es identicamente cero, las singularidades de f son aisladas, entonces $f(z)$ admite una extensión analítica en sus singularidades). Además de esta propiedad, $\mu_\gamma(z)$, $\gamma \in \Gamma$, satisface la siguiente condición de consistencia: $\mu_{\gamma\sigma}(z) = \mu_\gamma(\sigma(z))\,\mu_\sigma(z)$; $\gamma, \sigma \in \Gamma$. La regla de la cadena muestra que estas dos condiciones son satisfechas por la clase de funciones:

$$\mu_\gamma(z) = (cz + d)^{-2k} = \frac{d\gamma}{dz}^{k} \quad ; \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

Peterson mostró(*) que esta clase de funciones son, esencialmente, las únicas que satisfacen estas dos condiciones.

Esto motiva la siguiente:

Definición 6. Sean Γ un grupo Fuchsiano de la primera clase, k un entero. Una forma automorfa de peso k con respecto a Γ es una función meromorfa $f(z)$ sobre Ω que es "casi" invariante bajo las transformaciones $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$, es decir, es una función tal que

(*) Petersson, H., Monatshefte für Mathematk, vol. 53, (1949) pp. 17-41. (Ver [8])

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k\, f(z) \qquad (1)$$

para toda $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ en Γ.

Algunos autores llaman a una función con estas caracterís ticas forma modular, mientras que otros reservan este nombre para las formas automorfas definidas respecto al subgrupo de congruencia principal de $SL_2\ (\mathbb{R})$ de nivel N, en este caso la forma automorfa es llamada forma modular de nivel N.

Una función automorfa sobre Ω con respecto a Γ es una función f definida sobre Ω que es de la forma $f = g_o\varphi$, con g una función meromorfa sobre la superficie de Riemann $\Gamma\backslash\Omega^*$ (Γ grupo Fuchsiano de la primera clase), y donde φ es la proyección de Ω^* en $\Gamma\backslash\Omega^*$. El concepto anterior de forma automorfa es más general que el de función automorfa.

La propiedad (1) que caracteriza a las formas automorfas implica que $f(z)$ esta determinada por sus valores sobre un "dominio fundamental" D respecto a la acción del grupo Γ sobre Ω. Más precisamente, un dominio fundamental para $\Gamma\backslash\Omega$ (o simplemente para Γ) es un subconjunto abierto conexo D, de Ω que no contiene ningun par de puntos distintos equivalentes bajo Γ y cuya cerradura contiene al menos un punto de cada clase de equivalencia de Γ Ω elementos de Ω.

Se sigue a partir de la definición que las transformadas de D cuya intersección contenga un subconjunto abierto deben coincidir.

Aunque se puede construir explicitamente un dominio fundamental para un grupo dado Γ, solamente nos ocuparemos de encontrar un dominio fundamental para el grupo modular $\Gamma = SL_2(\mathbb{Z})$

(Es conveniente aclarar que debe distinguirse entre el grupo $SL_2(\mathbb{Z})$, que algunos autores llaman el grupo modular homogeneo, y el grupo $SL_2(\mathbb{Z})/\pm 1_2$ que es llamado el grupo modular no-homogeneo. La razón de esta distinción es clara; la matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ y su inverso aditivo $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ determinan la misma transformación lineal fraccional. Entonces el grupo de las transformaciones lineales fraccionales distintas es el grupo cociente $SL_2(\mathbb{Z})/\pm 1_2$. Cuando hablemos aquí del grupo modular, entenderemos el grupo modeular no-homogeneo y lo seguiremos denotando por $SL_2(\mathbb{Z})$).

Para encontrar un dominio fundamental para el grupo modular Γ estableceremos los siguientes lemas:

Lema 5. Para un punto fijo z en Ω existen sólo un número finito de pares de enteros (c,d) tales que

$$|cz + d| \leq 1$$

Demostración: Sea (c,d) un par con esta propiedad; entonces $|cz + d|^2 = (cx + d)^2 + c^2 y^2$; $(z = x + iy)$, de aquí que

$c^2 y^2 < (cx + d)^2 + c^2 y^2 \leq 1$.

Como z esta en Ω, $y > 0$ y entonces $|c| < 1/y$ en consecuencia sólo hoy un número finito de valores posibles para c. Para cualquiera de estos valores de c la ecuación $(cx + d)^2 + c^2 y^2 \leq 1$ muestra que existen sólo un número finito de valores posibles para d.

Lema 6. Dadas las transformadas $\{\gamma(z)\}_{\gamma \in \Gamma}$ de un punto z en Ω, existen solamente un número finito de éstas cuyas partes imaginarias son mayores que la parte imaginaria de z.

Demostración. Dados z en Ω y $\gamma \in \Gamma$

$$\gamma(z) = \frac{az + b}{cz + d} = \frac{az + b}{cz + d} \cdot \frac{c\bar{z} + d}{c\bar{z} + d} = \frac{r + i\,(ad - bc)\,\operatorname{Im} z}{|cz + d|^2} ;$$

$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $z = x + iy$ de aquí que $\operatorname{Im} \gamma(z) = \dfrac{\operatorname{Im} z}{|cz + d|^2}$

y el resultado se sigue del Lema 1.

El Lema 2 nos sugiere elegir de cada clase de equivalencia un elemento de parte imaginaria máxima, es decir, un punto z tal que $|cz + d| \geq 1$, para todos los pares de enteros c, d. Como la translación $\gamma : z \longrightarrow z + 1$ esta en Γ podemos suponer que el dominio fundamental se encuentra en la banda $|\operatorname{Re} z| = |x| \leq 1/2$.

Teorema 4. Un dominio fundamental para Γ es el conjunto

$$D = \{z \in \Omega : \ |\operatorname{Re} z| < 1/2 \ \text{ y } \ |z| > 1\}$$

Demostración. Primero mostramos que D es el mismo conjunto que

$$D_1 = \{z \in \Omega : |\mathrm{Re}\ z| < {}^1/_2 \quad y \quad |cz + d| > 1\}$$

para todos los pares de enteros c, d excepto $c = d = o$. Poniendo $c = 1$, $d = o$, vemos que $D_1 \subseteq D$. Inversamente, supongamos que z esta en D; entonces

$|cz + d|^2 = (cx + d)^2 + c^2 y^2 = c^2 (x^2 + y^2) + 2cdx + d^2 > c^2 - cd + d^2 \geqslant 1$

para todos los pares de enteros c, d excepto $c = d = o$. Ahora, de nuestras observaciones anteriores se sigue que la cerradura de D contiene al menos un punto de cada clase de equivalencia bajo el grupo modular Γ. Vamos a mostrar que los únicos pares de puntos de la cerradura de D que son equivalentes bajo Γ son los pares de puntos de la frontera de D que coinciden bajo refexión respecto a la línea $x = o$; estos puntos están identificados por las transformaciones $\gamma : z \longrightarrow z + 1$ y $z : z \longrightarrow {}^{-1}/_z$. Supongamos que z, z^1 están en D y $z \underset{\Gamma}{\sim} z^1$, digamos $\sigma(z) = z^1$; entonces $\mathrm{Im}\ (z) = \mathrm{Im}\ \sigma(z)$, así que

$$1 = |cz + d| = (cx + d)^2 + c^2 y^2 \geqslant c^2 + d^2 - cd \geqslant 1,$$

entonces o $c = o$, $d = \pm 1$ o $d = o$, $c = \pm 1$. Un cálculo simple muestra que el primer caso implica que $\sigma = \gamma$, y el segundo que $\sigma = \tau$; estas son las identificaciones ya mencionadas, esto concluye la prueba.

Los únicos puntos fijos de transformaciones de Γ que están en $\overline{D}$ son los puntos i, ρ, y ρ^2, donde $\rho = e^{\pi i/3}$ e i

es la unidad imaginaria. Estos puntos están fijos bajo las transformaciones elípticas $\tau : z \longrightarrow {}^{-1}/_z$, $\gamma\tau : z \longrightarrow {}^{z-1}/_z$ y $\tau\gamma : z \longrightarrow {}^{-1}/_{z+1}$ respectivamente.

Observación: Las dos transformaciones $\gamma : z \longrightarrow z + 1$ y $\tau : z \longrightarrow -{}^{1}/_z$ generan al grupo modular. Para justificar este hecho, sea G el subgrupo de Γ generado por γ y τ . Notemos primero que las transformadas de D por elementos de G cubren a Ω . Sea z un punto de Ω ; después de aplicar γ ó γ^{-1} un número suficiente de veces, la transformada $T^m(z) = z_1$ satisfacerá $|\mathrm{Re}\ z_1| \leqslant {}^{1}/_2$. Si z_1 está en D hemos terminado; de otra manera $|z_1| < 1$ y la parte imaginaria de $\tau(z_1)$ es estrictamente mayor que $\mathrm{Im}\ z_1 = \mathrm{Im}\ z$. Repitiendo la construcción ahora con el punto $\tau(z_1)$, y continuando este procedimiento, alguna transformada de z por un elemento de G debe eventualmente estar en D , pues por el Lema 2, existen solamente un número finito de partes imaginarias de transformadas de z que son estrictamente mayores que $\mathrm{Im}\ z$. Ahora sea σ una transformación en Γ y z algún punto interior de D . Como antes, existe una transformación g en G tal que $g(z) = \sigma(z)$. Entonces $\sigma^{-1}g$ está en Γ y deja fijo a z ; pero como z es dejado fijo sólo por la identidad se sigue que $g = \sigma$, entonces que $G = \Gamma$, como deseabamos.

Una forma automorfa debe satisfacer además, algunas condiciones de regularidad: Debe ser una función holomorfa en los puntos cúspides de Γ y en el infinito.

Precisamos esta última condición:

En adelante fijaremos nuestra atención en subgrupos Γ del grupo modular $SL_2(\mathbb{Z})$. Sea entonces Γ un subgrupo del grupo modular. Consideremos el menor entero positivo h tal que la transformación $z \longrightarrow z + h$ está en Γ, entonces, siendo f una forma automorfa, $f(z+h) = f(z)$. Considerando la expansión de f en serie de Laurent y teniendo en cuenta la igualdad anterior obtenemos que f se puede expresar en términos de una serie de Fourier $f(z) = \sum_{-\infty}^{\infty} a_n e^{2\Pi inz/h}$. Decimos que $f(z)$ es holomorfa en el infinito si $a_n = 0$ para $n < 0$, y que $f(z)$ se anula en el infinito si $a_n = 0$, para $n \leq 0$. La condición para una forma automorfa $f(z)$ de ser holomorfa en el infinito establece que ésta tiene un desarrollo en serie de Fourier de la forma:

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\Pi inz/h}$$

Si una forma automorfa se anula en el infinito, es decir si $a_0 = 0$, entonces la forma es llamada forma parabólica (cusp form).

En relación a la terminología, el término forma modular será utilizado como sinónimo de forma automorfa. Entonces, una forma modular es una forma automorfa para la cual el grupo de transformaciones es un subgrupo del grupo modular $SL_2(\mathbb{Z})$.

Como ejemplos de formas automorfas (formas modulares) tenemos los siguientes:

i) La función theta

$$\Theta(z) = \sum_{n=-\infty}^{\infty} e^{\Pi i n^2 z} = 1 + \sum_{n=1}^{\infty} 2e^{\Pi i n^2 z} \qquad (\mathrm{re}\ z > 0)$$

esta función es holomorfa en Ω y satisface

$$\Theta(z + 2) = \Theta(z)$$

$$\Theta(-1/z) = (z/i)^{1/2}\Theta(z)$$

estas dos ecuaciones dicen que $\Theta(z)$ es una forma modular de peso $1/2$ para el grupo $\Gamma(2)$ generado por las transformaciones $z \longrightarrow z + 2$, $z \longrightarrow -1/z$. $\Theta(z)$ es la única solución, salvo un multiplo constante, para estas ecuaciones. Para una demostración de estos hechos consultar [12], capítulo I, pp. 38-40.

ii) Considérese la función $\Delta(z)$ definida en Ω por

$$\Delta(z) = \sum_{n=1}^{\infty} a_n e^{2\Pi i n z} = e^{2\Pi i z} \prod_{n=1}^{\infty} (1-e^{2\Pi i n z})^{24}$$

$\Delta(z)$ es una forma modular de peso 12 para el grupo modular $SL_2(\mathbb{Z})$. Sus coeficientes a_n están cercanamente relacionados con la función partición. Consultar [12], pp. 29-31 y 43-45, Capítulo I.

iii) Las series de Einstein normalizadas

$$E_{2k}(z) = \frac{1}{2\zeta(2k)} \sum_{c,d\neq 0} \frac{1}{(cz+d)^{2k}} \quad ; \; k > 1, \; \zeta \text{ función zeta.}$$

son funciones modulares de peso $2k$ con respecto al grupo modular $SL_2(\mathbb{Z})$. Estas series tienen expansión en series de Fourier

$$E_{2k}(z) = 1 + \frac{(-1)^k 4k}{B_k} \sum_{n=1}^{\infty} \alpha_{2k-1}(n) e^{2\Pi inz}$$

donde B_k es el n-ésimo número de Bernoulli y $\alpha_r(n) = \sum_{d/n} d^r$. Consultar [8], capítulo IV, pp. 44-53.

Para tratar de ejemplificar la importancia de las formas automorfas en la teoría de los números consideremos el siguiente ejemplo:

Denotemos por $Q_r(x_1,\ldots,x_r)$ la forma cuadrática $\sum_{i=1}^{r} x_i^2$, y sea

$$\Theta_r(z) = \sum_{(n_1,\ldots,n_r)} e^{\Pi i Q_r(n_1,\ldots,n_r) z}$$

$\Theta_r(z)$ es una forma automorfa de peso $r/2$. Si $r(n, Q_r)$ denota el número de maneras distintas de expresar a n como suma de r cuadrados, entonces

$$\Theta_r(z) = \Theta(z)^r = \sum_{n=0}^{\infty} r(n, Q_r) e^{\Pi i n z}$$

(ver [6]). Relacionando $\Theta_4(z)$ con una serie de Einstein adecuada seobtiene la fórmula de Jacobi

$$r(n, Q_4) = 8 \sum_{\substack{d/n \\ 4/d}} d$$

En general, los coeficientes de Fourier de una forma automorfa envuelven soluciones numéricas de problemas de caracter numérico teórico.

2.2 *Series de Dirichlet y su relación con formas modulares*

Erich Hecke (1887-1947), desarrolló una teoría que sugirió nuevas formas de visualizar a las formas modulares en la teoría de los números. Al mismo tiempo, esta teoría proporcionó las herramientas necesarias para resolver problemas clásicos existentes.

La idea central de Hecke fué caracterizar las propiedades de una forma modular en términos de una serie de Dirichlet correspondiente. El propósito de esta sección es introducirnos a la teoría de Hecke.

Recordemos que una serie de Dirichlet es una serie de la forma

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

donde s, a_1, a_2,..... son números complejos. Cuando la serie converge, representa una función de s. El ejemplo clásico de una serie de Dirichlet es la función zeta de Riemann $\zeta(s)$, definida (y analítica) para $Re(s) > 1$ por

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

En 1859 Riemann probó que $\zeta(s)$ tiene una continuación analítica a todo el plano complejo excepto por un polo simple de residuo 1 en $s = 1$, y satisface la ecuación funcional:

$$\zeta(s) = 2^s \Pi^{s-1} \operatorname{sen}(s\Pi/2)\Gamma(1-s)\zeta(1-s)$$

El análisis original que Riemann hizo de $\zeta(s)$, fué generalizado por Hecke para obtener relaciones entre funciones definidas a través de series de Fourier y sus series de Dirichlet asociadas. Esbozaremos los pasos centrales del análisis de Riemann.

Necesitaremos la identidad de la función gamma

$$\Gamma(s) = \int_0^{\infty} t^{s-1}e^{-t}\, dt \qquad (Re(s) > 0)$$

que puede obtenerse por medio de la fórmula de Stirling ([1], p.p. 205). (En lenguaje moderno, se dice que $\Gamma(s)$ es la transformada de Mellin de e^{-t} en s). Con esta identidad se deriva la relación

$$\Pi^{-s}\Gamma(s)\zeta(2s) = \sum_{n=1}^{\infty} \int_0^{\infty} (\Pi n^2)^{-s} t^{s-1} e^{-t} dt \quad (\mathrm{re}(s) > 1/2)$$

$$= \sum_{n=1}^{\infty} \int_0^{\infty} t^{s-1} e^{-\Pi n^2 t} dt \quad \text{(usando el cambio de variable } t \to \Pi n^2 t\text{)}$$

$$= \int_0^{\infty} t^{s-1} \left(\frac{\Theta(it)-1}{2}\right) dt \quad \left(\Theta(z) = 1 + \sum_{n=1}^{\infty} 2e^{\Pi i n^2 z}\right)$$

por la convergencia absoluta de $\Theta(z)$. Esta última igualdad establece una estrecha relación entre el comportamiento analítico de $\zeta(s)$ y las propiedades automorfas de $\Theta(z)$, e inversamente. Continuando:

$$\Pi^{-s}\Gamma(s)\zeta(2s) = \int_1^{\infty} t^{s-1} \left(\frac{\Theta(it)-1}{2}\right) dt$$

$$- 1/2\, t^s/s \Big|_0^1 + 1/2 \int_0^1 t^{s-1}\, \Theta(it) dt$$

$$= \int_1^{\infty} t^{s-1} \frac{(\Theta(it)-1)}{2} dt - 1/2s \quad \text{(usando el cambio de variable } t \to 1/t \text{ en la segunda integral)}$$

$$+ 1/2 \int_1^{\infty} t^{-s-1}\, \Theta\left(\frac{i}{t}\right) dt$$

$$= \int_1^{\infty} \left(t^{s-1} + t^{1/2-(s+1)}\right) \frac{(\Theta(it)-1)}{2} dt \quad \left(\text{usando la propiedad automorfa } \Theta\left(\frac{i}{t}\right) = t^{1/2}\Theta(it)\right)$$

$$- \frac{1}{2s} - \frac{1}{1-2s}$$

Obsérvese la invarianza con respecto a la sustitución $s \to 1/2 - s$. Se pueda invertir el proceso y derivar la propiedad automorfa de $\Theta(z)$ (ecuación funcional) a partir de la ecuación funcional de $\zeta(s)$, para esto se requiere de la inversión de Mellin:

$$\frac{\Theta(it) - 1}{2} = \frac{1}{2\Pi i} \int_{Re(s)>0} t^{-s}\Pi^{-s}\Gamma(s)\zeta(2s)\,ds.$$

No nos ocuparemos de "invertir el proceso", pues esto se llevará a cabo en la situación más general estudiada por Hecke. Para ocuparnos de la generalización de Hecke necesitamos hacer las siguientes consideraciones:

i) Dados $a_0, a_1, a_2, \ldots,$ números complejos con $a_n = o(n^c)$ (esto significa que existe $A > 0$ tal que para toda n, $|a_n| \leq A \cdot n^c$) para alguna $c \in \mathbb{R}$, la serie de Dirichlet $\Psi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converge absoluta y uniformemente en $Re(s) \geq c + 1 + \varepsilon$, pues está dominada término a término uniformemente por $\sum_{n=1}^{\infty} n^{-1-\varepsilon} < \infty$, y entonces $\Psi(s)$ define una función analítica en (al menos) la parte del plano $Re(s) > c + 1$.

ii) Sea ahora $f(z) = \sum_{n=0}^{\infty} a_n e^{2\Pi inz/h}$, $h > 0$, $f(z)$ analítica en Ω; entonces $f(z)$ tiene la propiedad $f(z)-a_0=0(e^{-2\Pi y/h})$, $z = x + iy$. En efecto, $f(z) - a_0 = e^{-2\Pi y/h}\, e^{-2\Pi ix/h}$ $(\sum_{n=1}^{\infty} a_n e^{-2\Pi(n-1)z/h}$, el factor derecho del lado derecho de la igualdad es finito, pues la serie converge, de aquí que la igualdad misma muestra nuestra afirmación.

iii) Heremos uso de la fórmula de inversión de Mellin:

$$e^{-x} = \frac{1}{2\Pi i} \int_{Re(s)=\sigma>0} x^{-s}\Gamma(s)ds \quad ,$$

la integral tomada en sentido ascendente sobre una línea vertical. La fórmula anterior se puede justificar a partir del Teorema del Residuo. El lado derecho de la igualdad es $\sum_{n=0}^{\infty} \mathrm{Res}_{s=-n} x^{-s}\Gamma(s)$, y tomando en cuenta que $\Gamma(s)$ es una función entera excepto por polos simples en $s = -n$ de residuos $\frac{(-1)^n}{n!}$, $n = 0, 1, 2, \ldots.$, se obtiene

$$\sum_{n=0}^{\infty} \mathrm{Res}_{s=-n} x^{-s}\ \Gamma(s) = \sum_{n=0}^{\infty} \frac{(-x)^n}{n!} = e^{-x}$$

El uso del Teorema del Residuo para establecer la fórmula de inversión de Mellin, está justificado por el hecho de que podemos pensar al plano complejo (unión el punto al infinito) como la esfera de Riemann, y aquí una línea vertical es una curva cerrada con la propiedad de que todo entero tiene índice igual a uno con respecto a esta curva.

Podemos ahora enunciar y demostrar el siguiente teorema de Hecke:

Dadas dos sucesiones de números complejos $a_0, a_1, a_2, \ldots,$ y $b_0, b_1, b_2, \ldots;$ $a_n, b_n = O(n^c)$ para algún $c > 0$ y $h > 0$, $k > 0$, $C \in \mathbb{C}$, $C \neq 0$, consideremos las series

$$\phi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

$$\psi(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$$

$$\Phi(s) = (2\Pi/h)^{-s}\Gamma(s)\psi(s)$$

$$\Psi(s) = (2\Pi/h)^{-s}\Gamma(s)\psi(s)$$

y las funciones definidas en Ω por

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\Pi inz/h}$$

$$g(z) = \sum_{n=0}^{\infty} b_n e^{2\Pi inz/h}$$

(ϕ, ψ analíticas en alguna región derecha del plano; f, g analíticas en Ω).

Teorema 5. Las siguientes dos condiciones son equivalentes:

(A) $\Phi(s) + \frac{a_0}{s} + \frac{Cb_0}{k-s}$ es entera, acotada en toda franja vertical (abreviado EAV), y satisface la ecuación funcional
$\Phi(s) = C\Psi(k-s)$

(B) $f(z) = C(\frac{z}{i})^{-k} g(-\frac{1}{z})$

Dem: $$\Phi(s) = \sum_{n=1}^{\infty} \int_0^{\infty} a_n (2\Pi n/h)^{-s} t^{s-1} e^{-t} dt$$

$$= \sum_{n=1}^{\infty} \int_0^{\infty} a_n t^{s-1} e^{-2\Pi n t/h} dt$$ (usando el cambio de variable $t \to 2\Pi nt/h$)

$$= \int_0^{\infty} t^{s-1} (f(it) - a_0) dt$$

por convergencia absoluta para $\mathrm{Re}(s)$ suficientemente grande. Esta integral es impropia en ambos extremos pero como $f(it) - a_0 = O(e^{-\lambda t})$ para algún $\lambda > 0$, vemos que $\int_1^{\infty} t^{s-1} (f(it) - a_0) dt$ converge uniformemente sobre franjas verticales, y por lo tanto es EAV.

Supongamos que (B) se satisface. Entonces

$$\int_0^1 t^{s-1} (f(it)-a_0) dt = -a_0 \frac{t^s}{s} \Big|_0^1 + \int_1^{\infty} t^{-s-1} f(1/t) dt \quad (t \to 1/t)$$

$$= \frac{-a_0}{s} + C \int_1^{\infty} t^{k-s-1} (g(it)-b_0) dt$$

$$\frac{-cb_0}{k-s}.$$

Por lo tanto

$$\Phi(s) + \frac{a_0}{s} + \frac{cb_0}{k-s} = \int_1^{\infty} [t^{s-1}(f(it)-a_0) + t^{k-s-1}c(g(it)-b_0)]\,dt$$

es EAV. Calculando la expresión $C\,\Psi\,(k-s)$ de manera similar, se obtiene $\Phi(s) = C\,\Psi\,(k-s)$ y por lo tanto (A).

Inversamente, de la expresión $e^{-x} = \frac{1}{2\Pi i}\int_{Re(s)=\sigma>0} x^{-s}\,\Gamma(s)ds,$

o bien de la transformada de Mellin tenemos:

$$f(ix) - a_0 = \frac{1}{2\Pi i}\int_{Re(s)=\sigma} x^{-s}\,\Phi(s)ds,$$

la integral tomada sobre líneas verticales, y donde $Re(s) = \sigma$ se elige suficientemente grande para que s esté en el dominio de convergencia absoluta de $\Psi(s)$.

2.3 *Operadores de Hecke.*

La importancia de la función zeta de Riemann en la teoría analítica de los números radica en la relación que ésta tiene con los números primos. Esta relación fué establecida por Euler, quien observó que tenía lugar la identidad.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{(1-p^{-s})} \qquad (\mathrm{Re}(s) > 1)$$

donde p corre sobre los números primos. Euler consideró esta igualdad sólo para valores particulares de s, y fué Riemann quien consideró primero a $\zeta(s)$ como una función analítica de una variable compleja. Riemann se ocupó del problema de la distribución de los primos y en su investigación tomó como punto de partida la identidad anterior conocida como la fórmula del producto de Euler. A este respecto quizás resulte interesante para el lector leer el apéndice de [5], titulado "Sobre el número de primos menores que una magnitud dada" que es una traducción de un papel de 8 páginas de Riemann publicado en 1859*. Este artículo ha tenido una gran repercusión en el desarróllo del Análisis Complejo y en la Teoría de los Números, no tanto por el contenido de éste sino por los métodos y las ideas desarrolladas en él.

Así como la serie de Dirichlet $\zeta(s)$ tiene un desarrollo en producto infinito (producto Euleriano), las series de Dirichlet asociados a ciertas formas modulares (eigenfunciones de los operadores de Hecke) poseen también un desarrollo en producto infinito. Este último resultado es muy importante porque los coeficientes de las formas modulares tienen, a su vez, importante significado teórico numérico.

* Título original en alemán: "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse", Monatsber der Berliner Akad., 1859.

Estudiaremos aquí los operadores de Hecke:

Empezaremos por establecer lo que entenderemos por una retícula en $\mathbb{C}$, este espacio considerado como $\mathbb{R}$-espacio vectorial.

De manera general diremos que una retícula en un espacio vectorial V real de dimensión finita es un subgrupo discreto Λ de V que genera al $\mathbb{R}$-espacio vectorial V; de manera equivalente, es un subgrupo Λ de V para el cual existe una $\mathbb{R}$-base $(e_1,\ldots,e_n)$ de V que es una $\mathbb{Z}$-base de Λ (i.e. $\Lambda = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_n$).

Sea X el conjunto de las retículas de $\mathbb{C}$, y sea M el conjunto de las parejas (w_1, w_2) de elementos de $\mathbb{C}^{*}$ † tales que $\mathrm{Im}(w_1/w_2) > 0$. A cada pareja se le asocia la retícula

$$\Lambda(w_1, w_2) = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$$

de base $\{w_1, w_2\}$. De esta manera se obtiene una aplicación suprayectiva $M \longrightarrow X$.

Sea $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$; $(\Gamma = SL_2(\mathbb{Z}))$ y sea $(w_1, w_2) \in M$.

Pongamos:

$$w_1' = aw_1 + bw_2 \qquad \text{y} \qquad w_2' = cw_1 + dw_2$$

† En general si A es un anillo conmutativo con elemento identidad, denotamos por A^* al grupo de los elementos invertibles de A.

entonces $\{w_1', w_2'\}$ es una base de $\Lambda(w_1, w_2)$. Si $z = w_1/w_2$ y $z' = w_1'/w_2'$, se tiene:

$$z' = \frac{az + b}{cz + d} = gz,$$

de aquí que $\mathrm{Im}(z') > 0$, y entonces (w_1', w_2') aparece en M.

Proposición 15. Para que dos elementos de M definan la misma retícula, es necesario y suficiente que sean congruentes módulo $SL_2(\mathbb{Z})$.

Dem: Se acaba de ver que la condición es suficiente. Inversamente, si (w_1, w_2) y (w_1', w_2') son dos elementos de M que definen la misma retícula, existe una matriz con coeficientes enteros $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de determinante ± 1 que transforma la primera base en la segunda. Como $\mathrm{Im}(w_1'/w_2')$ tiene el mismo signo que $\mathrm{Im}(w_1/w_2)$, se tiene necesariamente $\det/g) = 1$ (estos cálculos ya se han hecho cuando se estudió el dominio fundamental de Γ), lo que demuestra la proposición.

Podemos entonces identificar al conjunto X de las retículas de $\mathbb{C}$ con el cociente de M por la acción de $SL_2(\mathbb{Z})$.

Pasemos ahora a las funciones modulares. Sea F una función sobre X, de valores complejos, y sea $k \in \mathbb{Z}$. Diremos que F es de peso k si

$$(1) \qquad F(\lambda\Lambda) = \lambda^{-k}F(\Lambda)$$

para toda retícula Λ y todo $\lambda \in \mathbf{C}^*$.

Sea F una de estas funciones. Si $(w_1, w_2) \in M$, denotamos por $F(w_1, w_2)$ el valor de F sôbre la retícula $\Lambda(w_1, w_2)$. La condición (1) se reescribe en la forma

$$(2) \qquad F(\lambda w_1, \lambda w_2) = \lambda^{-k}F(w_1, w_2);$$

la proposición 15 muestra que $F(w_1, w_2)$ es invariante bajo la acción de $SL_2(\mathbb{Z})$ sobre M.

A su vez la condición (2) muestra que el producto $w_2^kF(w_1, w_2)$ no depende más que de $z = w_1/w_2$. Entonces **F** define una función sobre Ω dada por

$$(3) \qquad F(w_1, w_2) = w_2^{-k}f(w_1/w_2)$$

Escribiendo la condición de invarianza de **F** por $SL_2(\mathbb{Z})$, se ve que f satisface la identidad

$$(4) \qquad f(z) = (cz + d)^{-k}f\left(\frac{az+b}{cz+d}\right)$$

para toda $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$; $\Gamma = SL_2(\mathbb{Z})$.

Inversamente, si f verifica (4), la expresión (3) le asocia una función F sobre X que es de peso k. De esta forma se puede identificar a las formas modulares de peso k con funciones de retículas de peso k.

Definiremos ahora unos operadores sobre X. Sea D el grupo abeliano libre generado por X, es decir el conjunto de sumas finitas formales $\sum\limits_{\Lambda\in X} n_\Lambda \Lambda$, con $n_\Lambda \in \mathbb{Z}$. Sea n un entero $\geqslant 1$. Denotaremos por $T(n)$ a la correspondencia sobre X que transforma una retícula Λ en la suma (en D) de sus subretículos Λ' de índice n. Se tiene entonces:

$$T(n)\Lambda = \sum_{(\Lambda:\Lambda')=n} \Lambda' , \qquad \Lambda \in X$$

La suma del segundo miembro es finita: en efecto, todas las retículas Λ' contienen a $n\Lambda$, y su número es el número de subgrupos de orden n de $\Lambda/n\Lambda$.

Utilizaremos también los operadores de homotecia $R\mu$ $(\mu \in \mathbf{C}^*)$ definidos por

$$R_\mu \Lambda = \mu\Lambda \qquad \Lambda \in X$$

Los operadores $T(n)$ son multiplicativos; de manera más general tenemos el siguiente:

Teorema 6. $T(n)\ T(m) = \sum_{d/n,m} d T(\frac{nm}{d^2}) R_d$; en particular $T(n)$ es multiplicativo, i.e. $T(n)\ T(m) = T(nm)$ si $(m,n) = 1$. Entonces los operadores $T(n)$ y R_μ generan un álgebra conmutativa de correspondencias sobre X.

Dem: Comenzaremos probando el caso especial $n = p^s$, $m = p$, p primo, así que probaremos primero

$$T(p^s)T(p) = T(p^{s+1}) + pT(p^{s-1})R_p \qquad (P \text{ primo, } s \geq 1)$$

Sea Λ una retícula, entonces $T(p^s)T(p)\Lambda$, $T(p^{s+1})\Lambda$ y $T(p^{s-1})R_p\Lambda$ son combinaciones lineales de retículas contenidas en Λ y de índice p^{s+1} en Λ (notar que $R_p\Lambda$ es de índice p^2 en Λ). Sea Λ'' una de estas retículas; entonces aparece en la combinación lineal acompañada de coeficientes a, b, c. Todo se reduce a mostrar que $a = b + pc$, i.e. que

$$a = 1 + pc$$

pues b es evidentemente igual a 1.

Distinguimos dos casos:

i) Λ'' no está contenida en $p\Lambda$. Entonces $c = 0$ y a es el número de retículas Λ', intermedias entre Λ y Λ'', y del índice p en Λ; una de estas retículas Λ' contiene a $p\Lambda$. En $\Lambda/p\Lambda$, la imagen de Λ' es de índice p y contie ne a la imagen de Λ'', que es de orden p (entonces también de índice p puesto que $\Lambda/p\Lambda$ es de orden p^2); entonces hay solamente un Λ' que responde a la pregunta, de donde $a = 1$ y la fórmula $a = 1 + pc$ se verifica.

ii) $\Lambda'' \subset p\Lambda$. Se tiene $c = 1$; no importa qué retícula Λ' de índice p en Λ contenga a $p\Lambda$, y entonces a Λ''. De aquí que $a = p + 1$ y la fórmula $a = 1 + pc$ se verifica nuevamente.

La igualdad (1) se generaliza por inducción para obtener

$$T(p^s)T(p^r) = \sum_{v \leq r,s} p^v T(p^{s+r-2v}) R_p^v.$$

Para obtener el resultado deseado necesitamos probar primero la multiplicatividad de $T(n)$, i.e. necesitamos probar que si $(m, n) = 1$, entonces $T(m)T(n) = T(mn)$. Esta igualdad equivale a la afirmación siguiente: Sean m,n dos enteros $\geqslant 1$ primos entre sí, y sea Λ'' una subretícula de una retícula Λ de índice mn; entonces existe una única subretícula Λ' de Λ, que contiene a Λ'', tal que $(\Lambda:\Lambda') = n$ y $(\Lambda':\Lambda'') = m$. Esta afirmación resulta del hecho de que el grupo Λ/Λ'', que es de orden mn, se descompone de manera única como suma directa de un grupo de orden m y de un grupo de orden n (teorema de Bezout).

De aquí ya es fácil obtener el teorema deseado. Sea $g = (m, n)$, entonces $g = \prod_{p/m,n} p^{\min(\alpha_p, \beta_p)}$ donde p^{α_p}/n, $p^{\alpha_{p+1}} \nmid n$ y p^{β_p}/m, $p^{\beta_{p+1}} \nmid m$. Sean $d_1 = \prod_{p/m,n} p^{\alpha_p}$, $d_2 = \prod_{p/m,n} p^{\beta_p}$

entonces

$$T(n)T(m) = T(n/d_1)T(d_1)T(d_2)T(m/d_2) = \sum_{d/g} dT(\frac{nm}{d^2})R_d$$

pues evidentemente los operadores R_μ y $\mathbf{T(n)}$ satisfacen las relaciones:

(a) $R_\mu R_\tau = R_{\mu\tau}$ $(\mu, \tau \in \mathbf{C}^*)$

(b) $R_\mu T(n) = T(n)R_\mu$ $(n \geqslant 1,\ \mu \in \mathbf{C}^*)$

Sea ahora $F(w_1, w_2)$, $\mathrm{Im}(w_1/w_2) > 0$, una función de peso $\mathbf{k}$ (o función homogénea de grado $\mathbf{k}$). Definimos un operador $\mathbf{T(n)}$ sobre $\mathbf{F}$ por

$$T(n)F(\Lambda) = n^{k-1} \sum_{\Lambda'} (\Lambda')$$

donde Λ' corre sobre las subretículas de índice n en Λ. De manera similar definimos

$$R_d F(\Lambda) = (d^2)^{k-1} F(d\Lambda) = d^{k-2} F(\Lambda)$$

así, la identidad del Teorema 6 se transforma en

$$T(n)T(m) = \sum_{d/n,m} d^{k-1} T(\frac{nm}{d^2})$$

operando sobre F.

Nos proponemos definir un operador $T(n)$ sobre las formas modulares. Para poder hacer esto utilizando lo que ya se ha hecho necesitamos el siguiente lema.

Lema 7. Sea $M(n)$ el conjunto de las matrices con coeficientes enteros $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, con $ad = n$, $a \geq 1$, $0 \leq b < d$. Si $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ pertenece a $M(n)$, sea Λ_σ la subretícula de Λ que tiene por base a:

$$w_1' = aw_1 + bw_2 \quad , \quad w_2' = dw_2.$$

Entonces la aplicación $\sigma \longrightarrow \Lambda_\sigma$ es una biyección de $M(n)$ sobre el conjunto $\Lambda(n)$ de las subretículas de índice n de Λ.

Dem: Es claro que Λ_σ está en $\Lambda(n)$. Inversamente, sea $\Lambda' \in \Lambda(n)$. Pongamos:

$$Y_1 = \Lambda/\Lambda' + \mathbb{Z}w_2 \quad y \quad Y_2 = \mathbb{Z}w_2/(\Lambda' \cap \mathbb{Z}w_2).$$

Estos son grupos cíclicos, generados respectivamente por las clases de w_1 y de w_2. Sean a y d sus órdenes. La sucesión exacta

$$0 \to Y_2 \to \Lambda/\Lambda' \to Y_1 \to 0$$

muestra que $ad = n$. Si $w_2' = dw_2$, se tiene $w_2' \in \Lambda'$. Por otra parte, existe $w_1' \in \Lambda'$ tal que

$$w_1' \equiv a\, w_1 \qquad (\text{mod } \mathbb{Z}w_2)$$

w_1' y w_2' forman una base de Λ'. Además, se puede escribir w_1' en la forma

$$w_1' = aw_1 + bw_2 \quad , \qquad \text{con } b \in \mathbb{Z},$$

donde b está determinado de manera única módulo d; si se impone a b la desigualdad $0 \leqslant b < d$, esto determina a b, entonces también a w_1'. Se ha asociado entonces a toda $\Lambda' \in \Lambda(n)$ una matriz $\sigma(\Lambda') \in M(n)$. Las aplicaciones $\sigma \longrightarrow \Lambda\sigma$ y $\Lambda' \longrightarrow \sigma(\Lambda')$ son inversas una de otra; de donde se obtiene el lema.

Sea k un entero, y sea f una forma modular de peso k. Como se vió anteriormente,a esta f le corresponde una función F de peso k (homogénea de grado k) tal que

$$F(\Lambda(w_1, w_2)) = w_2^{-k} f(w_1/w_2).$$

Definiremos $T(n)f$ como la función sobre Ω asociada a la función $n^{k-1}T(n)F$ sobre X. Entonces, por definición:

$$T(n)f(z) = n^{k-1}T(n)F(\Lambda(z,1))$$

y gracias al lema 7:

$$T(n)f(z) = n^{k-1} \sum_{\substack{a\geq 1, ad=n \\ 0\leq b<d}} d^{-k} f\left(\frac{az+b}{d}\right) \tag{5}$$

$T(n)f$ es llamado el n-ésimo operador de Hecke.

La expresión (5) muestra que $T(n)f$ es meromorfa sobre Ω. Además si $\alpha = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z})$, (5) implica que $T(n)f(\alpha(z)) = (c'z + d')^k T(n)f(z)$. Probaremos en seguida una proposición que nos dirá que $T(n)f$ es holomorfa en el infinito, entonces se habrá verificado que $T(n)f$ es una forma modular de peso k con respecto a $\Gamma = SL_2(\mathbb{Z})$.

El símbolo $M(\Gamma,k)$ denotará al conjunto de las formas modulares de peso k con respecto a Γ.

Proposición 16. Sea $f \in M(\Gamma,k)$, $f(z) = \sum_{v=0}^{\infty} a_v e^{2\Pi ivz}$, entonces

$$T(n)f(z) = \sum_{v=0}^{\infty} a_v(n) e^{2\Pi ivz}$$

donde

$a_v(n) = \sum_{d/v,n} d^{k-1} a_{\frac{nv}{d^2}}$. Entonces $T(n)f \in M(\Gamma,k)$, y es una forma parabólica (cusp form) si f lo es.

Dem: Por definición:

$$T(n)f(z) = n^{k-1} \sum_{\substack{ad=n,\, a\geq 1\\ 0\leq b<d}} d^{-k} \sum_{v=0}^{\infty} a_v e^{2\Pi i \frac{az+b}{d} v}.$$

Ahora bien, $\sum_{0\leq b<d} e^{2\Pi i \frac{bv}{d}}$ es d si d divide a v, y es cero si no lo divide. Poniendo $v' = v/d$, podemos escribir:

$$T(n)f(z) = n^{k-1} \sum_{\substack{ad=n\\ a\geq 1,\, v'\in \mathbb{N}}} d^{-k+1} a_{v'd} e^{2\Pi i a v' z}$$

Y ordenando según las potencias de $e^{2\Pi i}$:

$$T(n)f(z) = \sum_{\mu=0}^{\infty} e^{2\Pi i \mu z} \Big(\sum_{d/n,\mu} d^{k-1}\, a_{\frac{\mu n}{d^2}} \Big) .$$

Consideremos ahora la serie de Dirichlet formal $D(s) = \sum_{n=1}^{\infty} T(n) n^{-s}$, cuyos coeficientes $T(n)$ son operadores sobre $M(\Gamma,k)$. Las identidades de los operadores de Hecke se reflejan en la serie $D(s)$ de la manera siguiente:

Teorema 7. $D(s) = \sum_{n=1}^{\infty} T(n) n^{-s}$

$$= \prod_{p} (1 - T(p) p^{-s} + p^{k-1-2s})^{-1}$$

Dem: Sea s un conjunto finito de números primos, y sea $N(s)$ el conjunto de enteros ≥ 1 cuyos factores primos pertenecen a s. Entonces se tiene la siguiente igualdad:

$$\sum_{n \in N(s)} T(n)\, n^{-s} = \prod_{p \in s} \left(\sum_{m=0}^{\infty} T(p^m)\, p^{-ms} \right)$$

y haciendo crecer a s se obtiene:

$$\sum_{n=1}^{\infty} T(n)\, n^{-s} = \prod_{p} \left(\sum_{m=0}^{\infty} T(p^m)\, p^{-ms} \right)$$

Si probamos:

$$\sum_{m=0}^{\infty} T(p^m)\, p^{-ms} = (1 - T(p)\, p^{-s} + p^{k-1-2s})^{-1}$$

habremos terminado.

Formemos la serie:

$$\Psi(p) = \left(\sum_{m=0}^{\infty} T(p^m)p^{-ms}\right)(1 - T(p)p^{-s} + p^{k-1-2s})$$

El coeficiente de p en Ψ es $T(p) - T(p) = 0$; el de p^{n+1}, $n \geq 1$, es

(A) $\quad T(p^{n+1}) - T(p)T(p^n) + p^{k-1}T(p^{n-1})$.

Ahora, se cuenta con la identidad $T(n)T(m) = \sum_{d/n,m} d^{k-1}T(\frac{nm}{d^2})$ cuando $T(n)$ opera sobre F, pero esta identidad se conserva cuando $T(n)$ opera sobre $M(\Gamma,k)$. Entonces utilizando esta identidad para p primo se obtiene

$$T(p)T(p^n) = T(p^{n+1}) + p^{k-1}T(p^{n-1}).$$

De donde (A) es cero, y la serie Ψ se reduce al término constante 1. Esto demuestra el Teorema.

Corolario. Sea $f \in M(\Gamma,k)$, $f(z) = \sum_{v=0}^{\infty} a_v e^{2\pi i v z}$, y supongamos que f es una eigenfunción del algebra de Hecke, es decir $T(n)f = c_n f$ para toda $n \geq 1$. Entonces $c_n a_1 = a_1(n) = a_n$; normalizando la eigenfunción para tener $a_1 = 1$, el eigenvalor c_n de $T(n)$ es el mismo que el coeficiente de Fourier a_n, y la serie de Dirichlet asociada tiene el producto de Euler

$$\psi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p (1-a_p p^{-s} + p^{k-1-2s})^{-1}$$

Dem: Prácticamente todo se ha hecho. Por la proposición 16, $c_n a_1 = a_1(n) = a_n$; y el producto se obtiene del Teorema 7.

Ahora probamos el inverso del corolario en una "forma fuerte"; $\psi(s)$ tiene un producto de Euler sólo si $f(z)$ es una eigenfunción de los operadores de Hecke $T(n)$. Primero probamos un resultado preliminar útil:

Proposición 17. Sea $f \in M(\Gamma,k)$, $f(z) = \sum_{n=0}^{\infty} a_n e^{2\Pi inz}$

1) Si $f|\alpha \in M(\Gamma,k)$ para alguna $\alpha \in M^*(n)$, $n > 1$, donde $f|\alpha = \det(\alpha)^{k/2} \cdot f(\alpha(z)) \cdot j(\alpha,z)^{-k}$ con la notación del capítulo I $(j(\alpha,z)^{-k} = (cz+d)^{-k}$ si $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix})$, y donde $M^*(n)$ es el conjunto de las matrices primitivas (es decir, el conjunto de matrices $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tales que a,b,c y d son primos relativos), entonces $f = 0$

2) Sea p un primo fijo

a) Si $a_m = 0$ para todo m con $p \nmid m$, entonces $f = 0$.

b) Si $a_{p^n} = 0$ para toda n, entonces $f = 0$.

Dem: 1) Se puede demostrar (ver por ejemplo [16], p.p. 108) que $M^*(n) = \Gamma\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\Gamma$ donde $\Gamma = SL_2(\mathbb{Z})$. Podemos tomar enton ces $\alpha = \begin{pmatrix}1 & 0\\ 0 & n\end{pmatrix}$. En consecuencia $f\Big|\begin{pmatrix}1 & 0\\ 0 & n\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = f\Big|\begin{pmatrix}1 & 0\\ 0 & n\end{pmatrix}$, y de esta forma $f = f\Big|\begin{pmatrix}1 & 0\\ 0 & n\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}n & 0\\ 0 & 1\end{pmatrix} = f\Big|\begin{pmatrix}n & 1\\ 0 & n\end{pmatrix}$. Ahora $\begin{pmatrix}n & 1\\ 0 & n\end{pmatrix} = L\begin{pmatrix}1 & 0\\ 0 & n^2\end{pmatrix}M$, donde $L, M \in \Gamma$, entonces $f\begin{pmatrix}1 & 0\\ 0 & n^2\end{pmatrix} = f$, i.e. $f(z) = f(\frac{z}{n^2}) \cdot n^{-k}$. La serie de Fourier de f nos dice que $f = 0$.

2) Si $a_m = 0$ para $p \nmid m$, entonces $f(z+1/p)=f(z)$, i.e. $f = f\Big|\begin{pmatrix}p & 1\\ 0 & p\end{pmatrix}$, entonces $f = 0$. Si $a_{pn} = 0$ para toda n, entonces $T(p)f = p^{k/2-1}f\Big|\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix} \in M(\Gamma,k)$, y así $f = 0$.

Ahora sea $\psi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \neq 0$ la serie de Dirichlet asociada a $f \in M(\Gamma,k)$. Decimos que $\psi(s)$ tiene un producto de Euler relativo al primo p si

$$\psi(s) = \Big(\sum_{p\nmid m} a_m m^{-s}\Big)\Big(\sum_{v=0}^{\infty} c(p^v)p^{-vs}\Big)$$

i.e. $a_{mp^v} = a_m c(p^v)$ para $p \nmid m$, $v \geq 0$.

Teorema 8. $\psi(s)$ tiene un producto de Euler relativo a p si y sólo si f es una eigenfunción de los operadores de Hceke $T(p)$, i.e. $T(p)f = c\cdot f$. Si esto sucede, entonces el p-factor es necesariamente

$$\sum_{v=0}^{\infty} c(p^v)p^{-vs} = (1 - cp^{-s} + p^{k-1-2s})^{-1}$$

Dem: Supongamos primero que $\psi(s)$ tiene un producto relativo a p, entonces $a_{mp^v} = a_m c(p^v)$ para $p \nmid m$, $v \geq 0$. Ahora

$$T(p)f(z) = p^{k-1}f(pz) + 1/p \sum_{0 \leq l < p} f\left(\frac{z+\ell}{p}\right)$$

$$= p^{k-1}f(pz) + \Sigma a_{pn} z^n,$$

entonces

$$T(p)f(z) - c(p)f(z) = p^{k-1}f(pz) + \Sigma(a_{pn} - c(p)a_n)z^n$$

$$= \text{serie de potencias en } z^p,$$

que por la proposición 17 es cero.

Inversamente, supongamos que $T(p)f = c\cdot f$. Entonces:

$$c\cdot a_n = a_n(p) = \begin{cases} a_{np} & \text{si } p \nmid n \\ \\ a_{np} + p^{k-1}a_{\frac{n}{p}} & \text{si } p|n \end{cases},$$

por la proposición 16. Por lo tanto

$$\psi(s)(1 - cp^{-s} + p^{k-1-2s}) = \sum_n a_n n^{-s} + p^{k-1} \sum_n a_n (np^2)^{-s}$$

$$- \sum_n a_{pn}(pn)^{-s} - p^{k-1} \sum_n a_n (np^2)^{-s}$$

$$= \sum_{p \nmid m} a_m m^{-s} .$$

Entonces $\psi(s)$ tiene un producto de Euler si y sólo si la $f(z)$ asociada es una eigenfunción de los operadores de Hecke.

BIBLIOGRAFIA

[1]. L.V. Ahlfors. Complex Analysis, Mc Graw-Hill, 1979.

[2]. G. Birkhoff - S. Mac Lane. A survey of Modern Algebra, Macmillan, New York, 1953.

[3]. C. Chevalley. Theory of Lie groups, Princeton University Press, Princeton, 1946.

[4]. J. Dugundji. Topology, Allyn and Bacon, Inc. 1966.

[5]. H. M. Edwards. Riemann's Zeta function, Academic Press, 1974.

[6]. S. Gelbart. An elementary introduction to the Langlands program, Bulletin of the American Mathematical Society, Volume 10, Number 2, April 1984, pp. 177-217.

[7]. R. Godement. Les travaux de Hecke I, Séminaire Bourbaki, Decembre, 1951.

R. Godement. Les travaux de Hecke II, Séminaire Bourbaki, Février, 1952.

R. Godement. Les travaux de Hecke III, Séminaire Bourbaki, Février, 1953.

[8]. R. E. Gunning. Lectures on modular forms, Princeton University Press., Princeton, 1962.

[9]. E. Hecke. Mathematische Werke, Vandenhoeck und Ruprecht, Götingen, 1959.

[10]. E. Hecke. Lectures on the theory of Algebraic Numbers, Springer-Verlag New York, Inc, 1981.

[11]. F. A. Ongay Larios. La fórmula de Poisson en la función zeta de Hecke-Iwasawa-Tate, tesis profesional, 1982.

[12]. A. Ogg. Modular forms and Dirichlet Series, W.A.Benjamin Inc, 1969.

[13]. L. S. Pontrjagin. Topological Groups, Princeton University Press, Princeton, 1939.

[14]. J. P. Serre. Cours d'arithmétique, Presses Universitaires de France, 1970.

[15]. I. Piatetski-Shapiro. Classical and adelic automorphic forms. An introduction, Proceeding of Symposia in Pure Mathematics. Vol. 33, 1979, part 1, pp. 185-188.

[16]. G. Shimura. Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten, Publishers and Princeton University Press, 1971.

[17]. J. Tate. Fourier analysis in number fields and Hecke's Zeta functions, Ph. D. Thesis, Princeton, 1950.