0.1 Formas modulares

0.1.1 La acción $\mathrm{SL}_2(\mathbb{R}) \curvearrowright \mathbb{H}$

Para definir formas modulares, primero necesitamos estudiar los automorfismos del semiplano de Poincaré

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

Sabemos que las matrices de 2×2 con coeficientes complejos actúan sobre la esfera de Riemann $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ mediante transformaciones de Möbius:

$$\gamma z = \frac{az+b}{cz+d} \qquad \text{donde} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Nosotros estamos interesados en la restricción de la acción a $\mathrm{GL}_2^+(\mathbb{R}) \curvearrowright \mathbb{H}$ donde $\mathrm{GL}_2^+(\mathbb{R}) = \{\gamma \in \mathrm{GL}_2(\mathbb{R}) \mid \det A > 0\}$ y después nos enfocaremos en subgrupos discretos $\Gamma \subset \mathrm{GL}_2^+(\mathbb{R})$ y sus acciones $\Gamma \curvearrowright \mathbb{H}$ asociadas. A $\mathrm{GL}_2^+(\mathbb{R})$ le ponemos la topología de subespacio del epacio euclideano $\mathbb{R}^4$. De esta manera, la acción $\mathrm{GL}_2^+(\mathbb{R}) \curvearrowright \mathbb{H}$ es continua.

Esta acción no es fiel[†], en efecto $(\lambda\gamma)z = \gamma z$ para toda $\lambda > 0$. Por lo tanto la acción desciende al cociente con las matrices escalares y así obtenemos el isomorfismo:

$$\mathrm{Aut}(\mathbb{H}) = \{f : \mathbb{H} \to \mathbb{H} \mid f \text{ es holomorfa}\} \cong \frac{\mathrm{GL}_2^+(\mathbb{R})}{\{\lambda \mathrm{Id}\}_{\lambda>0}} \cong \frac{SL_2(\mathbb{R})}{\{\pm \mathrm{Id}\}} \overset{\text{def}}{=} \mathrm{PSL}_2(\mathbb{R}).$$

La acción es transitiva. En particular, toda $z = x + iy \in \mathbb{H}$ está en $\mathrm{GL}_2^+(\mathbb{R})i$, la órbita de i. En efecto:

$$\begin{pmatrix} y^{1/2} & xy^{-1/2} \\ 0 & y^{-1/2} \end{pmatrix} i = \frac{iy^{1/2} + xy^{-1/2}}{y^{-1/2}} = x + iy = z.$$

Además, el subgrupo de isotropía de i es:

$$\mathrm{GL}_2^+(\mathbb{R})_i = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R}) \,\middle|\, \frac{ai+b}{ci+d} = i \right\} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \right\}_{a,b\in\mathbb{R}} = \mathrm{SO}_2(\mathbb{R}).$$

Por lo tanto tenemos una función continua y biyectiva $\mathrm{GL}_2^+(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}) \to \mathbb{H}$, más aún, esta biyección es un homeomorfismo[*]. cita de pontryagin

Ahora nos enfocamos en clasificar algunas matrices. Toda matriz $M \in \mathrm{GL}_2(\mathbb{C})$ es conjugada a su forma canónica de Jordan que solamente puede tomar dos formas:

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \quad \text{ó} \quad \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \qquad (\lambda \neq \mu \in \mathbb{C} \text{ y } |\lambda/\mu| \geq 1),$$

correspondientes a las transformaciones $z \mapsto z + \lambda^{-1}$ y $z \mapsto (\lambda/\mu)z$ respectivamente.

[†]Una acción $G \curvearrowright X$ es *fiel* si el subgrupo de isotropía $G_x := \{\gamma \in G \mid \gamma x = x\}$ es el subgrupo trivial $\{1\}$ para toda $x \in X$.

[*]En general, si hay una acción $G \curvearrowright X$ entonces la función natural $G/G_x = \mathrm{Orb}(x)$ es continua y biyectiva. Si además pedimos que G y X sean localmente compactos, y G sea segundo numerable, entonces esa función es un homeomorfismo. La prueba es estándar y usa el teorema de Baire (c.f. la proposición 1.2 y el lema 1.3 de §1.1 de [**?**]).

Definición 1. Sea $A \in \mathrm{GL}_2(\mathbb{C}) - \{\pm\mathrm{Id}\}$ con valores propios $\lambda, \mu \in \mathbb{C}$., decimos que la matriz A es

1. *Parabólica* si $\lambda = \mu$. Además, si $A \in \mathrm{SL}_2(\mathbb{C})$, entonces equivalentemente $\mathrm{tr}A = \pm 2$.
2. *Elíptica* si $\lambda \neq \mu$ y $|\lambda/\mu| = 1$. Además, si $A \in \mathrm{SL}_2(\mathbb{C})$, entonces equivalentemente $\mathrm{tr}A \in \mathbb{R}$ y $|\mathrm{tr}A| < 2$.
3. *Hiperbólica* si $\lambda/\mu \in \mathbb{R}$ y $\lambda/\mu > 1$. Además, si $A \in \mathrm{SL}_2(\mathbb{C})$, entonces equivalentemente $\mathrm{tr}A \in \mathbb{R}$ y $|\mathrm{tr}A| > 2$.
4. *Loxodrómica* en cualquier otro caso. No hay $A \in \mathrm{SL}_2(\mathbb{R})$ loxodrómico.

Ahora nos enfocamos en la restricción de la acción $\mathrm{GL}_2^+(\mathbb{R}) \curvearrowright \mathbb{H}$ a una acción $\Gamma \curvearrowright \mathbb{H}$, donde $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ es un subgrupo discreto. Sea $\overline{\Gamma} \subset \mathrm{PSL}_2(\mathbb{R})$ su imagen bajo la proyección $\mathrm{SL}_2(\mathbb{R}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$.

Nota. En general denotaremos por $\overline{X}$ a la imagen del subconjunto $X \subseteq \mathrm{SL}_2(\mathbb{R})$ bajo la proyección $\mathrm{SL}_2(\mathbb{R}) \twoheadrightarrow \mathrm{PSL}_2(\mathbb{R})$, en particular, si $X = \Gamma$ un subgrupo discreto, $\overline{\Gamma} = \Gamma/(\Gamma \cap \{\pm 1\})$.

Definición 2. Decimos que $z \in \mathbb{H}$ es: un *punto elíptico* de la acción $\Gamma \curvearrowright \mathbb{H}$ si el grupo de isotropía Γ_z contiene una matriz elíptica; el *orden* del punto elíptico $z \in \mathbb{H}$ se define como la cardinalidad de $\overline{\Gamma_z}$. Decimos que $z \in \mathbb{R} \cup \{\infty\}$ es una *cúspide* de la acción $\Gamma \curvearrowright \mathbb{H}$ si Γ_z contiene un elemento parabólico.

Notas. En la definición de cúspide, estamos extendiendo de manera natural la acción $\Gamma \curvearrowright \mathbb{H}$ a la acción $\Gamma \curvearrowright \widehat{\mathbb{C}}$ para poder definir el grupo de isotropía de $z \in \mathbb{R} \cup \{\infty\}$, es decir $\Gamma_z := \{\gamma \in \Gamma \mid \gamma z = z \; \forall z \in \widehat{\mathbb{C}}\}$.

A $\mathbb{H}$ le podemos agregar las cúspides de una acción $\Gamma \curvearrowright \mathbb{H}$ para obtener una curva compacta muy importante al tomar cociente módulo Γ. Pero antes de seguir volvemos a enfocarnos en un caso más particular: suponemos que $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$; a $\mathrm{SL}_2(\mathbb{Z})$ se le llama el *grupo modular*.

En este caso, es bien conocido que las cúspides de Γ solamente pueden ser racionales o ∞. Entonces para agregarle a $\mathbb{H}$ las cúspides, definimos

$$\mathbb{H}^*(\Gamma) = \mathbb{H} \cup \big\{ z \in \mathbb{Q} \cup \{\infty\} \mid z \text{ es una cúspide de } \Gamma \curvearrowright \mathbb{H} \big\}.$$

En general solamente escribimos $\mathbb{H}^*$, en lugar de $\mathbb{H}^*(\Gamma)$, cuando el grupo Γ es implícito del contexto. Γ sigue actuando sobre $\mathbb{H}^*$ como la restricción de la acción $\Gamma \curvearrowright \hat{\mathbb{C}}$. En efecto, si $z \in \mathbb{H}^* - \mathbb{H}$ es una cúspide y $A \in \Gamma_z$ parabólico, entonces BAB^{-1} estabiliza a Bz y $\mathrm{tr}(BAB^{-1}) = \mathrm{tr}(A) = \pm 2$.

Ahora definimos una topología para $\mathbb{H}^*$, especificando una base local para los tres tipos distintos de puntos de $\mathbb{H}^*$:

- Si $z \in \mathbb{H}$, toma al conjunto $\{|z - w| < \varepsilon\}_{w \in \mathbb{H}}$ como base local de z.
- Si $z = \infty$, toma $\{\{\mathrm{Im}\,(w) > N\} \cup \{\infty\}\}_{N \geq 1}$ como base local de ∞.
- Si $z \in \mathbb{Q}$ es una cúspide, para su base local, toma a z y toma los interiores de todos los discos en $\mathbb{H}$ tangentes al eje real sobre z, más precisamente, toma $\{\{|w - z - \varepsilon i| < \varepsilon\}_{w \in \mathbb{H}} \cup \{z\}\}_{\varepsilon > 0}$.

Las vecindades de $z \in \mathbb{Q} \cup \infty$ se llaman vecindades horocíclicas. En la figura 1 viene un ejemplo de un elemento de cada tipo de base local. De esta misma figura es claro que $\mathbb{H}^*$ es un espacio Hausdorff.

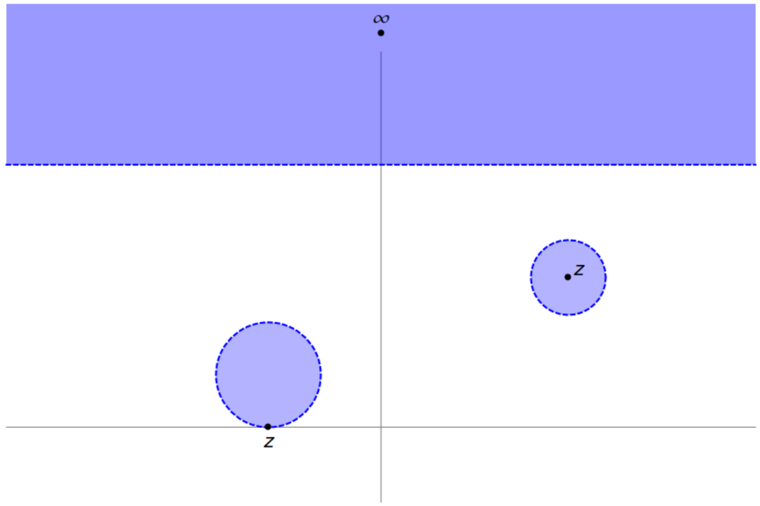

Figure 1: Un ejemplo de cada tipo de abierto básico de la topología de $\mathbb{H}^*$.

Nota. $\mathbb{H}^*$ es conexo. En efecto: si $\mathbb{H}^* = U \cup U'$ es una disconexión, $(U \cap \mathbb{H}) \cup (U' \cap \mathbb{H}) = \mathbb{H}$ es una disconexión de $\mathbb{H}$; como $\mathbb{H}$ que es conexo (sin pérdida de generalidad) tenemos que $U \cap \mathbb{H} = \emptyset$, es decir $U \subseteq \mathbb{Q} \cup \{\infty\}$; el único abierto $U \subseteq \mathbb{H}^*$ que puede cumplir esto es $U = \emptyset$ y terminamos.

El espacio de órbitas de la acción $\Gamma \curvearrowright \mathbb{H}^*$ es un espacio muy importante que definimos en seguida:

Definición 3. Sea $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ un subgrupo discreto que actúa sobre $\mathbb{H}^*$. El espacio cociente se llama la *curva modular* asociada a Γ y se denota:

$$X(\Gamma) := \mathbb{H}^*/\Gamma.$$

De manera elemental (pero no trivial), podemos deducir las siguientes propiedades:

Proposición 4. *Si $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ es un subgrupo, entonces $X(\Gamma)$ es un espacio conexo, Hausdorff y localmente compacto.*

Proof. Aquí solamente esbozamos la prueba, para más detalles nos referimos a [**?**, §1.3, teorema 1.28 y proposición 1.29 respectivamente]. La conexidad se sigue de que $\mathbb{H}^*$ es conexo. Ser Hausdorff se sigue de que la acción $\Gamma \curvearrowright \mathbb{H}^*$ es totalmente disconexa[†]. Lo localmente compacto se sigue de que existe una vecindad $V_C = \{z \in \mathbb{H}^* \mid \Im(z) \geq C\}$ de la cúspide ∞, tal que V_C/Γ_∞ queda identificado con V_C/Γ y así se calcula que

$$V_C/\Gamma = \{z \in V_C \mid z = \infty \text{ ó } 0 \leq \Re(z) \leq |h|\}/\Gamma$$

para alguna $h \in \mathbb{Z}$; como el lado derecho es la imagen continua del compacto $\{z \in V_C \mid 0 \leq \Re(z) \leq |h|\} \cup \{\infty\}$ bajo la proyección $\mathbb{H}^* \twoheadrightarrow \mathbb{H}^*/\Gamma$, concluimos que V_C/Γ es la vecindad compacta buscada. $\square$

[†]Una acción de grupos $G \curvearrowright X$ es *totalmente disconexa* si para cualesquiera dos subconjuntos compactos K y K' de X, el conjunto $\{\gamma \in G \mid K \cap \gamma(K') \neq \emptyset\}$ es finito.

De hecho, a $X(\Gamma)$ le podemos dar una estructura de superficie de Riemann compacta (nos referimos a [**?**, §2.2, §2.3, §2.4] para detalles).

Teorema 5. *Sea* $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ *un subgrupo discreto. El espacio cociente* $\mathbb{H}^*/\Gamma$ *es una superficie de Riemann (i.e. una variedad holomorfa sobre* $\mathbb{C}$ *de dimensión 1). Además si* Γ *es de índice finito,* $X(\Gamma)$ *es compacto.*

Proof. Es bien conocido que el conjunto

$$\mathcal{F} = \left\{ z \in \mathbb{H} \mid -\tfrac{1}{2} \leq \Re(z) \leq \tfrac{1}{2},\ |z| \geq 1 \right\}$$

es un *dominio fundamental*[‡] para la acción $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{H}$ (Véase la figura 2). Además $\mathcal{F}' := \mathcal{F} \cup \{\infty\} \subset \mathbb{H}^*$ es compacto. En efecto, dada cualquier cubierta abierta de $\mathcal{F}' \subseteq \bigcup U_i$, un abierto U_j contiene a ∞ y así contiene a un abierto de la forma $V = \{z \in \mathbb{H} \mid \Im(z) > C\} \cup \{\infty\}$. Por lo tanto

$$\mathcal{F}' - V \subseteq \bigcup_{i \neq j} U_i,$$

pero $\mathcal{F}' - V$ es claramente compacto (por ser intersección de cerrados y además acotado), entonces hay una subcubierta $U_{i_1} \cup \cdots \cup U_{i_n}$ finita de $\mathcal{F}' - V$. Por lo tanto $\mathcal{F}' \subseteq U_j \cup U_{i_1} \cup \cdots \cup U_{i_n}$ y hemos obtenido una subcubierta finita para $\mathcal{F}'$.

Por otro lado, como $\mathcal{F}$ es un dominio fundamental

$$\mathbb{H}^* = \mathrm{SL}_2(\mathbb{Z})\mathcal{F}' = \bigcup_{\gamma_i} (\gamma_i \Gamma)\mathcal{F}'$$

donde la unión corre sobre un sistema completo de representantes de $\mathrm{SL}_2(\mathbb{Z})/\Gamma$. Si aplicamos la proyección natural $\pi : \mathbb{H}^* \twoheadrightarrow \mathbb{H}^*/\Gamma = X(\Gamma)$ obtenemos:

$$X(\Gamma) = \bigcup_{\gamma_i} \pi(\gamma_i(\mathcal{F}')).$$

Por último, la unión anterior es finita pues tiene $(\mathrm{SL}_2(\mathbb{Z}) : \Gamma)$ uniendos y Γ es de índice finita; la composición $\pi \circ \gamma_i : \mathbb{H}^* \to X(\Gamma)$ es claramente continua, entonces $\pi(\gamma_i(\mathcal{F}'))$ es compacto para toda i. De estas dos consideraciones concluimos que $X(\Gamma)$ es compacto. $\square$

En general decimos que un subgrupo discreto $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ es un grupo *Fuchsiano del primer tipo* si $X(\Gamma)$ es compacto. El teorema anterior se puede reescribir como: todo subgrupo $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ de índice finito es Fuchsiano de primer tipo. Ahora, para nuestras consideraciones, no requerimos la generalidad de los grupos Fuchsianos, entonces solamente nos vamos a restringir a la siguiente clase de subgrupos especiales que van a aparecer seguido en este trabajo.

[‡] Un dominio fundamental de una acción $G \curvearrowright X$ es un subconjunto abierto $\mathcal{F} \subseteq X$ tal que si $x, x' \in \mathcal{F}$ entonces $Gx \cap Gx' \supsetneq \{1\} \implies x = x'$ y tal que para todo $x \in X$ existe un $x' \in \overline{\mathcal{F}}$ (la cerradura topológica de $\mathcal{F}$) tal que $Gx = Gx'$.

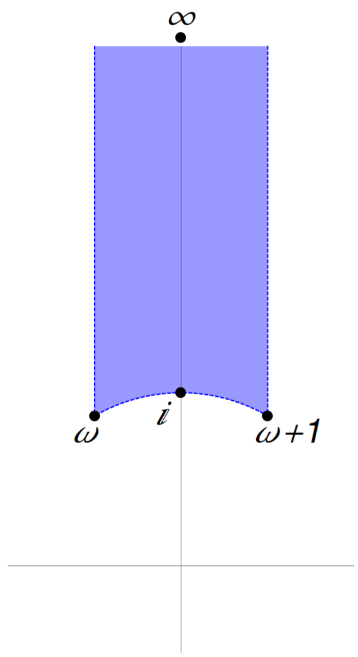

Figure 2: El dominio fundamental $\mathcal{F}$ de la acción $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{H}^*$ (aquí, $\omega = e^{2\pi i/3}$).

0.1.2 Subgrupos de congruencia

Los subgrupos de congruencia son ciertos subgrupos del grupo modular $\mathrm{SL}_2(\mathbb{Z})$. Como éste es discreto en $\mathrm{SL}_2(\mathbb{R})$, los resultados de la sección anterior aplican a cualquier subgrupo de $\mathrm{SL}_2(\mathbb{Z})$. En particular vamos a estar interesados en subgrupos que contengan matrices que, módulo alguna $N \in \mathbb{Z}^+$, sean la identidad. Estos son:

Definición 6. Sea $N \in \mathbb{Z}^+$. El *subgrupo de congruencia principal de nivel* N se define como

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

A la curva modular asociada a $\Gamma(N)$ la denotamos por $X(N)$ en lugar de $X(\Gamma(N))$. Además decimos que un subgrupo discreto $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ es un *subgrupo de congruencia* si existe una $N \in \mathbb{Z}^+$ tal que $\Gamma(N) \subseteq \Gamma$.

Primero notamos que $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ entonces, cuando la notación lo requiera, vamos a usar ambas notaciones intercambiablemente.

Tenemos que $\Gamma(N)$ es un subgrupo normal de $\mathrm{SL}_2(\mathbb{Z})$. En efecto si extendemos la proyección natural $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/N\mathbb{Z}$ a $\mathrm{SL}_2(\mathbb{Z})$, entrada por entrada, obtenemos un homomorfismo de grupos $\Gamma(1) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ que resulta ser sobre (c.f. [**?**, §1.6, lema 1.38]). Por lo tanto tenemos la siguiente sucesión exacta:

$$1 \longrightarrow \Gamma(N) \hookrightarrow \mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\bmod N} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow 1.$$

Como consecuencia directa de esto tenemos que

$$(\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)) = \# \frac{\mathrm{SL}_2(\mathbb{Z})}{\Gamma(N)} = \# \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) < \infty$$

y por lo tanto $X(N)$ es compacto.

Podemos calcular explícitamente el índice de $\Gamma(N)$. Es conocido que $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ tiene $(p^2-1)(p^2-p)$ elementos (c.f. [?, Teorema 8.5, pg 219]) y en general:

$$\begin{aligned}
\#\mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) &= p^{4\alpha}\left(1-\tfrac{1}{p}\right)\left(1-\tfrac{1}{p^2}\right),\\
\#\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) &= p^{3\alpha}\left(1-\tfrac{1}{p^2}\right),
\end{aligned} \tag{1}$$

(c.f. [?, §1.6]). Si $N=\prod p_i^{\alpha_i}$ es la factorización en primos, el teorema chino del residuo nos da el isomorfismo $\mathbb{Z}/N\mathbb{Z}\cong\prod(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$ que induce (otra vez por el teorema chino del residuo) el isomorfismo $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\cong\prod\mathrm{SL}_2(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$. Con la fórmula (1) podemos concluir que

$$(\mathrm{SL}_2(\mathbb{Z}):\Gamma(N)) = \#\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = N^3\prod_{p|N}\left(1-\tfrac{1}{p^2}\right). \tag{2}$$

Si $N=2$, tenemos que $-1\in\Gamma(2)$ mientras que $-1\notin\Gamma(N)$ para toda $N>2$. Por lo tanto, al tomar el cociente $\mathrm{SL}_2(\mathbb{Z})\twoheadrightarrow\mathrm{PSL}_2(\mathbb{Z})$, el índice de la imagen $\overline{\Gamma(N)}$ de $\Gamma(N)$ es la mitad del índice original para $N>2$ y no cambia cuando $N=2$. Más precisamente:

$$(\mathrm{PSL}_2(\mathbb{Z}):\overline{\Gamma(N)}) = \begin{cases}\frac{1}{2}N^3\prod_{p|N}(1-p^{-2}) & N>2\\ 6 & N=2\end{cases}$$

Ahora introducimos unas clases de subgrupos de congruencia que son muy importantes:

Definición 7. Sea $N\in\mathbb{Z}^+$. Definimos

$$\begin{aligned}
\Gamma_0(N) &:= \left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})\middle| c\equiv 0 \pmod N\right\},\\
\Gamma_1(N) &:= \left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})\middle| a\equiv d\equiv 1\ ,\ c\equiv 0 \pmod N\right\}.
\end{aligned}$$

A la curva asociada a $\Gamma_i(N)$ la denotamos por $X_i(N)$ $(i=1,2)$ y en particular, a $X_0(N)$ se le llama la *curva modular de nivel* N.

Claramente $\Gamma(N)\subseteq\Gamma_0(N)$, entonces $\Gamma_0(N)$ es un subgrupo de congruencia. Además $\Gamma(N)$ es un subgrupo normal de $\Gamma_0(N)$ porque es el núcleo del homomorfismo

$$\psi_N:\Gamma_0(N)\longrightarrow(\mathbb{Z}/N\mathbb{Z})^* \quad \text{definido por} \quad \begin{pmatrix}a & b\\ c & d\end{pmatrix}\mapsto d \pmod N.$$

Entonces podemos hablar del índice $(\Gamma_0(N):\Gamma(N))$. Para calcularlo observemos que, bajo la proyección $\mathrm{SL}_2(\mathbb{Z})\twoheadrightarrow\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, la imagen del grupo $\Gamma_0(N)$ es

$$\frac{\Gamma_0(N)}{\Gamma(N)} = \left\{\begin{pmatrix}a & b\\ 0 & a^{-1}\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\middle| a\in(\mathbb{Z}/N\mathbb{Z})^*,\, b\in\mathbb{Z}/N\mathbb{Z}\right\}$$

ya que si tomamos $\gamma\in\Gamma_0(N)$ con $\det\gamma=ad-bc=1$, la hipótesis de $c\equiv 0 \pmod N$ implica que $ad\equiv 1 \pmod N$. Para elegir un elemento arbitrario de $\Gamma_0(N)/\Gamma(N)$, solamente hay $\phi(N)$

maneras de elegir la entrada a y N maneras de elegir la entrada b.[§] Por lo tanto tenemos

$$(\Gamma_0(N) : \Gamma(N)) = \#\frac{\Gamma_0(N)}{\Gamma(N)} = N\phi(N) = N^2 \prod_{p|N}(1-p^{-1})$$

donde hemos usado una fórmula muy conocida de ϕ [**?**, Proposición 2.2.5].

Con la fórmula anterior y con la fórmula para $(\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N))$ que calculamos en (2), podemos calcular el índice de $\Gamma_0(N)$ en $\mathrm{SL}_2(\mathbb{Z})$:

$$(\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)) = \frac{(\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N))}{(\Gamma_0(N) : \Gamma(N))} = \frac{N^3 \prod(1-p^{-2})}{N^2 \prod(1-p^{-1})} = N \prod_{p|N}(1+p^{-1}).$$

Además, como $-1 \in \Gamma_0(N)$, tenemos que $(\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma_0(N)}) = (\mathrm{SL}_2(Z) : \Gamma_0(N))$.

Ejemplo 8. Un caso de interés para este trabajo es cuando $N = 15$. Aquí

$$(\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(15)) = 15\left(1+\tfrac{1}{3}\right)\left(1+\tfrac{1}{5}\right) = 24.$$

Por los resultados anteriores, la curva modular de nivel N es una superficie de Riemann compacta y por lo tanto es caracterizada topológicamente por el género. Para calcular el género de $X_0(N)$, necesitamos estudiar los puntos elípticos y las cúspides de la acción $\Gamma_0(N) \curvearrowright \mathbb{H}^*$. Abusamos un poco la notación y decimos que $z\Gamma_0(N) \in X_0(N)$ es un punto elíptico (resp. una cúspide) si $z \in \mathbb{H}^*$ es un punto elíptico (resp. una cúspide) de la acción $\Gamma_0(N) \curvearrowright \mathbb{H}^*$. Ahora, definimos ν_∞ como la cantidad de cúspides de $X_0(N)$ y ν_i como la cantidad de puntos elípticos de orden $i \in \{2,3\}$ en $X_0(N)$. Entonces tenemos el siguiente teorema:

Proposición 9. *Con la notación del párrafo anterior, la cantidad de puntos elípticos y cúspides de $X_0(N)$ se calculan con las siguientes fórmulas:*

$$\nu_2 = \begin{cases} \prod_{p|N}\left(1+\left(\frac{-1}{p}\right)\right) & 4 \nmid N \\ 0 & 4 \mid N \end{cases},$$

$$\nu_3 = \begin{cases} \prod_{p|N}\left(1+\left(\frac{-3}{p}\right)\right) & 9 \nmid N \\ 0 & 9 \mid N \end{cases},$$

$$\nu_\infty = \sum_{d|N} \phi\big((d, N/d)\big).$$

donde $\left(\frac{*}{p}\right)$ es el símbolo de Legendre, i.e. el caracter cuadrático $(\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$ que caracteriza si un elemento $a \in (\mathbb{Z}/p\mathbb{Z})^*$ es residuo cuadrático o no módulo p.

Proof. (c.f. [**?**, §1.6, proposición 1.43]) □

[§] La función aritmética $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ definido por $\phi(N) = \#\{1 \le k \le N \mid (N,k) = 1\}$ se llama la función de Euler y cumple $\phi(N) = \#(\mathbb{Z}/N\mathbb{Z})^*$.

Para calcular el género de $X_0(N)$, se usa la fórmula de Hurwitz[¶] aplicado a la función holomorfa $\varphi : X_0(N) = \mathbb{H}^*/\Gamma(N) \to \mathbb{H}^*/\Gamma(1) = X(1)$ inducida por la inclusión $\Gamma_0(N) \subset \Gamma(1)$. Primero sabemos que el género de $\mathbb{H}^*/\Gamma(1)$ es 0 porque $\mathbb{H}^*/\Gamma(1) \approx \widehat{\mathbb{C}}$ como espacios topológicos; esta afirmación es bien conocida y se puede deducir del dibujo del dominio fundamental de la acción $\Gamma(1) \curvearrowright \mathbb{H}^*$ que vimos en la prueba del teorema 5. Entonces la relación entre los géneros de $X_0(N)$ y de $\mathbb{H}^*/\Gamma(1)$ que establece la fórmula de Hurwitz se puede usar para calcular el género de $X_0(N)$ y así completamente caracterizar a $X_0(N)$ como superficie de Riemann. Como consecuencia de estas consideraciones, tenemos el siguiente teorema:

Teorema 10. *Con la notación de la proposición 9 y denotando* $\mu = (\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N))$*, el género* g *de la superficie de Riemann* $X_0(N)$ *es:*

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

Proof. La observación clave para aplicar la fórmula de Hurwitz es que el índice de ramificación de un elemento $z\Gamma_0(N) \in X_0(N)$ en la preimagen de $z\Gamma(1) \in X(1)$ bajo la función natural $X_0(N) \to X(1)$ es exactamente el índice $(\overline{\Gamma(1)_z} : \overline{\Gamma_0(N)_z})$ dentro de $\mathrm{PSL}_2(\mathbb{Z})$ (c.f. [**?**, §1.5, proposición 1.37]). Para una prueba completa de este teorema ve [**?**, §1.6, proposición 1.40] o ve [**?**, Teorema 3.1.1] para una prueba más detallada). □

Ejemplo 11. Aplicamos el teorema anterior al caso $N = 15$. Para calcular ν_2, ν_3 y ν_∞, usamos la proposición 9. Como -1 no es residuo cuadrático módulo 3 y -3 no es residuo cuadrático módulo 5, entonces la proposición 9 dice que

$$\nu_2 = \left(1 + \left(\tfrac{-1}{3}\right)\right)\left(1 + \left(\tfrac{-1}{5}\right)\right) = 0 \quad \text{y} \quad \nu_3 = \left(1 + \left(\tfrac{-3}{3}\right)\right)\left(1 + \left(\tfrac{-3}{5}\right)\right) = 0;$$

además,

$$\nu_\infty = \sum_{d|15} \phi\big((d, 15/d)\big) = \phi\big((1,15)\big) + \phi\big((3,5)\big) + \phi\big((5,3)\big) + \phi\big((15,1)\big) = 4.$$

Todo esto junto con $\mu = (\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(15)) = 24$ dado por el ejemplo 8 combina para dar:

$$g = 1 + \frac{24}{12} - \frac{0}{4} - \frac{0}{3} - \frac{4}{2} = 1.$$

Por lo tanto el género de $X_0(15)$ es 1, es decir $X_0(15)$ es una curva elíptica.

[¶] Fórmula de Hurwitz: Sea $f : X \to X'$ una función holomorfa no constante entre dos superficies de Riemann compactas con géneros g y g' respectivamente. Denota por e_x el índice de ramificación de f sobre $x' \in X'$, i.e. el mínimo exponente (necesariamente positivo) de la serie de Taylor de la función f expresada en coordenadas locales. Denotamos $n = e_{x_1} + \cdots + e_{x_m}$ donde $f^{-1}(x') = \{x_1, \ldots, x_m\}$ para alguna $x' \in X'$; el valor de n no depende de $x' \in X'$ y se llama el grado de f. La fórmula de Hurwitz dice que

$$2g - 2 = n(2g' - 2) + \sum_{x' \in X'} (e_{x'} - 1).$$

0.1.3 Formas Modulares y Operadores de Hecke

Ahora nos enfocamos en funciones holomorfas $f : \mathbb{H} \to \mathbb{C}$ que se transforman de cierta manera bajo la acción de un subgrupo de congruencia Γ. No podemos restringirnos solamente a tales funciones que son invariantes bajo la acción de Γ (i.e. las funciones holomorfas definidas sobre $\mathbb{H}/\Gamma$) porque dejamos afuera la gran mayoría de la teoría de formas modulares.

En esta sección iremos construyendo poco a poco los requerimientos que necesita tener f para poder llamarla una forma modular. Después estudiamos cierto operadores entre los espacios de formas modulares que nos permite "cambiar" de subgrupo de congruencia; estos operadores son ejemplos de operadores de Hecke.

Pimero definimos dos conceptos fundamentales:

Definición 12. El *factor de automorfía* se define como la función:

$$j : \mathrm{GL}_2(\mathbb{R}) \times \mathbb{C} \longrightarrow \mathbb{C} \qquad j(\gamma, z) = cz + d \quad \text{donde } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Para cada $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ definimos el $[\gamma]_k-$*operador de peso* k sobre el espacio de funciones holomorfas $f : \mathbb{H} \to \mathbb{C}$, como:

$$\big(f[\gamma]_k\big)(z) = (\det \gamma)^{k/2} j(\gamma, z)^{-k} f(\gamma z).$$

Notas. La fórmula de $f[\gamma]_k$ es multiplicativa, es decir $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$ como operadores. Además, como j restringido a $\mathrm{GL}_2(\mathbb{R}) \times \mathbb{H}$ no se anula, entonces f y $f[\gamma]_k$ tienen los mismos ceros y polos.

Ahora estudiamos funciones holomorfas $f : \mathbb{H} \to \mathbb{C}$ que son invariantes bajo ciertas clases de $[\gamma]_k-$operadores. En particular vamos a estudiar cuando $\gamma \in \Gamma$, un subgrupo de congruencia.

Definición 13. Sea $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ un subgrupo de congruencia y $f : \mathbb{H} \to \mathbb{C}$ una función holomorfa. Decimos que f es *débilmente modular de peso k con respecto de* Γ si es $[\gamma]_k-$invariante para toda $\gamma \in \Gamma$, es decir:

$$f[\gamma]_k = f \qquad \forall \gamma \in \Gamma.$$

Para abreviar, a veces decimos que f es débilmente $(\Gamma, k)-$modular.

Nota. Si $-1 \in \Gamma$, por ejemplo en el caso $\Gamma = \Gamma_0(N)$, entonces ser $(\Gamma, k)-$modular implica la ecuación $f(z) = (f[-1]_k)(z) = (-1)^k f(z)$. Si k es impar, la única función que cumple esa ecuación es 0. Por lo tanto, si k es impar y $-1 \in \Gamma$, la única función débilmente $(\Gamma, k)-$modular es la función cero.

Observa que si Γ es un subgrupo de congruencia, i.e. $\Gamma(N) \subseteq \Gamma$, entonces una función holomorfa $f : \mathbb{H} \to \mathbb{C}$ débilmente modular de peso k con respecto de Γ es una función $N\mathbb{Z}-$periódica, en efecto: la pertenencia de la matriz

$$\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma(N) \subseteq \Gamma,$$

que corresponde a la transformación $z \mapsto z + N$, implica que $f(z) = f(z + N)$. Por lo tanto f es $N\mathbb{Z}-$periódica.

Nuestro siguiente propósito es extender la noción de holomorfía de $f : \mathbb{H} \to \mathbb{C}$ al punto $z = \infty$ para poder hablar de funciones holomorfas sobre $X(\Gamma)$ inducidas por f's que sean débilmente modulares de peso k con respecto de Γ. Primero tomamos el mínimo entero positivo h tal que:

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma$$

y por lo anterior, f es $h\mathbb{Z}$-periódica. Esto quiere decir que f deciende a $\mathbb{H}/h\mathbb{Z}$, el espacio cociente de la acción $h\mathbb{Z} \curvearrowright \mathbb{H}$ de traslaciones $\{z \mapsto z + hk\}_{k\in\mathbb{Z}}$; por el momento, denotamos a este espacio cociente por $\widetilde{\mathbb{H}}$. Por lo tanto existe una función $\tilde{f} : \widetilde{\mathbb{H}} \to \mathbb{C}$ tal que $f = \tilde{f} \circ \pi$, donde $\pi : \mathbb{H} \twoheadrightarrow \widetilde{\mathbb{H}}$ es la proyección natural (véase el diagrama conmutativo 3).

Por otro lado, la función exponencial:

$$q_h : \mathbb{H} \longrightarrow D \qquad \text{definido por} \quad z \mapsto e^{2\pi iz/h},$$

donde $D = \{0 < |z| < 1\}$, es otra función $h\mathbb{Z}-$periódica, i.e. también se factoriza a través de $\widetilde{\mathbb{H}}$. Pero a diferencia de $\tilde{f}$, la función inducida $\widetilde{q_h} : \widetilde{\mathbb{H}} \to D$ tiene un inverso holomorfo

$$\widetilde{q_h}^{-1}(z + h\mathbb{Z}) = \frac{h \log z}{2\pi i}$$

que está bien definido módulo $h\mathbb{Z}$ porque $\log(z) = \log|z| + i \arg(z)$ está bien definido módulo $2\pi i\mathbb{Z}$.

Por lo tanto a f le podemos asociar la función holomorfa $f_{\text{cil}} : D \to \mathbb{C}$ definido por $f_{\text{cil}} = \tilde{f} \circ \widetilde{q_h}^{-1}$, aparece como la flecha punteada en el siguiente diagrama:

$$\begin{tikzcd}
\mathbb{H} \arrow[dr, two heads] \arrow[drr, bend left, "f"] \arrow[dd, "q_h"'] & & \\
& \widetilde{\mathbb{H}} \arrow[r, "\tilde{f}"'] \arrow[dl, bend right, "\widetilde{q_h}"'] & \mathbb{C} \\
D \arrow[ur, bend right, "\widetilde{q_h}^{-1}"'] \arrow[urr, dashed, bend right, "f_{\text{cil}}"'] & &
\end{tikzcd} \tag{3}$$

La notación viene de "cilindro" pues D es homeomorfo al cilindro.

La conmutatividad del diagrama implica que $f(z) = f_{\text{cil}}(e^{2\pi iz/h})$ para toda. $z \in \mathbb{H}$. Como $\Im(z) \to \infty$ si y solamente si $e^{2\pi iz/h} \to 0$, podemos interpretar que el comportamiento de f_{cil} cerca de 0 es análogo al comportamiento de f cerca de ∞. Esto nos sugiere la siguiente definición:

Definición 14. Sea $f : \mathbb{H} \to \mathbb{C}$ débilmente modular de peso k con respecto de un subgrupo de congruencia Γ. Decimos que una función f es *holomorfa en* ∞ si la función holomorfa $f_{\text{cil}} : D \to \mathbb{C}$ inducida admite una extensión holomorfa a $D \cup \{0\}$ y decimos que se *anula en* ∞ cuando la extensión holomorfa si anula en 0. Si f es holomorfa en ∞ la extensión $\widehat{f_{\text{cil}}} : D \cup 0 \to \mathbb{C}$ admite una serie de Taylor alrededor de 0; sus coeficientes los denotamos por $a_n(f)$ y la serie la denotamos por:

$$f_\infty(q) = \sum_{n=0}^{\infty} a_n(f) q^n \qquad \text{donde } \; q = e^{2\pi iz/h} \;\; (z \in \mathbb{H})$$

donde h es el mínimo entero positivo tal que $f(z) = f(z + h)$.

Notas. f se anula en ∞ si y solamente si $a_0(f) = 0$. Además, si $h = 1$, como en el caso $\Gamma_0(N)$, entonces $f(z) = f(z + 1)$ y la serie de Taylor $f_\infty(q)$ es simplemente la serie de Fourier de f. A veces decimos "Fourier" en lugar de "Taylor" si estamos en el caso de $\Gamma_0(N)$.

La existencia de una extensión holomorfa $\widehat{f_{\text{cil}}}$ implica que f_{cil} es acotado cuando $q \to 0$. Gracias al comentario sobre el diagrama conmutativo (3), esto es equivalente a que $\Im(f(z))$ es acotado cuando $\Im(z) \to \infty$. Por lo tanto tenemos una condición suficiente para que una función débilmente modular sea holomorfa en ∞:

$$f \text{ es holomorfa en } \infty \quad \Longrightarrow \quad \big\{f(z_n)\big\}_{n\in\mathbb{N}} \text{ es acotado si } \lim_{n\to\infty} \Im(z_n) = \infty.$$

Ahora que sabemos extender la noción de holomorfía a ∞, el siguiente paso es extenderlo a las cúspides de un subgrupo de congruencia Γ. La idea es reducir el problema a considerar holomorfía en ∞.

Sea $f : \mathbb{H} \to \mathbb{C}$ una funcíon débilmente $(\Gamma, k)-$modular con Γ de congruencia y sea $z \in \mathbb{Q}$ una cúspide de la accíon $\Gamma \curvearrowright \mathbb{H}$. Sabemos que z es de la forma $z = a/c$ donde a y c son enteros primos relativos, entonces existen $b, d \in \mathbb{Z}$ tales que $ad - bc = 1$ y así:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \frac{a\infty + b}{c\infty + d} = \frac{a}{c} = z.$$

En otras palabras, todas las cúspides de Γ están en la órbita de ∞ bajo la acción del grupo modular. Por lo tanto si $z \in \mathbb{Q}$ es una cúspide de $\Gamma \curvearrowright \mathbb{H}$, toma $\gamma \in \Gamma(1)$ tal que $z = \gamma\infty$. En este caso $\det\gamma = 1$ y la restricción $j(\gamma, *) : \mathbb{H} \to \mathbb{C}$ nunca se anula. Esto implica que $f[\gamma]_k$ es holomorfa siempre y cuando f lo sea.

Por otro lado, si $\tau \in \gamma^{-1}\Gamma\gamma$, entonces tiene la forma $\tau = \gamma^{-1}\tau'\gamma$ y así la igualdad:

$$\big(f[\gamma]_k\big)[\tau]_k = f[\gamma]_k[\gamma^{-1}\tau'\gamma]_k = f[\tau']_k[\gamma]_k \overset{*}{=} f[\gamma]_k,$$

donde (*) se sigue de $\tau' \in \Gamma$ y f siendo débilmente $(\Gamma, k)-$modular. Acabamos de probar que $f[\gamma]_k$ es invariante bajo los $[\tau]_k-$operadores cuando $\tau \in \gamma^{-1}\Gamma\gamma$, es decir $f[\gamma]_k$ es débilmente $(\gamma^{-1}\Gamma\gamma, k)-$modular.‖ Por lo tanto tiene sentido hablar de holomorfía en ∞ de la función $f[\gamma]_k$. Además, simbólicamente tenemos que

$$\text{“}\big(f[\gamma]_k\big)(\infty) = \det\gamma^{k/2} j(\gamma, \infty)^{-k} f(z)\text{”},$$

lo cual sugiere explícitamente cómo deberíamos de definir la holomorfía en una cúspide z a partir de la holomorfía de $f[\gamma]_k$ en ∞:

Definición 15. Sea $f : \mathbb{H} \to \mathbb{C}$ débilmente $(\Gamma, k)-$modular para alguna $\Gamma \subseteq \Gamma(1)$ de congruencia y $z \in \mathbb{Q}$ una cúspide. Decimos que f es *holomorfa* en z si $f[\gamma]_k$ es holomorfa en ∞ donde $\gamma \in \Gamma(1)$ es tal que $z = \gamma\infty$.

Observa que esta definición no depende de la elección de γ. En efecto, la holomorfía de $f[\gamma]_k$ es independiente de la elección de γ porque la acción $z \mapsto \gamma z$ siempre es holomorfa.

Aunque no es tan inmediato, la condición de anularse en ∞ también es independiente de γ. *A priori*, las series de Fourier de $f[\gamma]_k$ y $f[\gamma']_k$ son distintas, pero si $\gamma\infty = \gamma'\infty$, entonces las composiciones $f(\gamma z)$ y $f(\gamma' z)$ tiene el mismo comportamiento cerca de ∞. Por lo tanto se anulan simultaneamente.

Ahora estamos en posición para definir las formas modulares:

Definición 16. Decimos que $f : \mathbb{H} \to \mathbb{C}$ es una *forma modular* de peso k con respecto de un subgrupo de congruencia Γ (o brevemente $(\Gamma, k)-$modular) si cumple las siguientes tres cosas:

‖Podemos hablar de modularidad débil con respecto de $\gamma^1\Gamma\gamma$ porque éste es un subgrupo de congruencia cuando Γ lo es (c.f. [**?**, §1.4, lema 1.4.1]).

i) f es holomorfo.

ii) $f[\gamma]_k = f$ para toda $\gamma \in \Gamma$, i.e. f es débilmente $(\Gamma, k)-$modular.

iii) $f[\tau]_k$ es holomorfo en ∞ para toda $\tau \in \Gamma(1)$.

Al conjunto de formas modulares de peso k con respecto de Γ se denota por $M_k(\Gamma)$. Si además cumple

iv) $f[\tau]_k$ se anula en ∞ para toda $\tau \in \Gamma(1)$, i.e. $a_0(f[\tau]_k) = 0$ para toda $\tau \in \Gamma(1)$.

Decimos que f es *cuspidal*; el conjunto de formas modulares cuspidales se denota $S_k(\Gamma)$.

En seguida enunciamos algunas propiedades básicas de $M_k(\Gamma)$ y $S_k(\Gamma)$:

Proposición 17. *Sea $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ un subgrupo de congruencia. Entonces:*

i) $M_k(\Gamma)$ y $S_k(\Gamma)$ son $\mathbb{C}-$espacios vectoriales de dimensión finita.

ii) $\dim S_2(\Gamma) = g$ donde g es el género de $X(\Gamma)$. En particular $S_2(\Gamma(1)) = 0$.

iii) $M(\Gamma) := \bigoplus_{k\geq 0} M_k(\Gamma)$ es un anillo graduado y $S(\Gamma) := \bigoplus_{k\geq 0} S_k(\Gamma)$ es un ideal.

iv) El espacio $S_k(\Gamma)$ admite un producto interior Hermitiano positivo-definido llamado el producto interior de Petersson*, definido por*

$$\langle \_, \_ \rangle_\Gamma : S_k(\Gamma) \times S_k(\Gamma) \longrightarrow \mathbb{C} \quad , \quad \langle f, g \rangle_\Gamma = \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(z)\overline{g(z)} \mathrm{Im}\,(z)^k \, d\mu(z)$$

*donde $\mu z = dxdy/y^2$ (donde $z = x + iy$) es la medida hiperbólica de $\mathbb{H}$ y V_Γ es el volumen hiperbólico** de $X(\Gamma)$. i.e. $V_\Gamma = \int_{X(\Gamma)} d\mu$. A veces quitamos el "$\Gamma$" de la notación del producto interior cuando Γ es claro del contexto.* buscar cita

Proof. El inciso (i) es una aplicación clásica del teorema de Riemann-Roch††. El inciso (ii) se sigue de que $f \mapsto f dz$ es un isomorfismo entre $S_2(\Gamma)$ y el espacio de 1-formas diferenciales sobre $X_0(N)$ (c.f. el corolario 2.17 de [**?**]). La igualdad $\dim S_2(\Gamma) = g$ se deduce (otra vez) de Riemann-Roch y el caso particular se sigue de que $X(\Gamma(1)) = \mathbb{H}^*/\Gamma(1) \approx \widehat{\mathbb{C}}$, la esfera de Riemann. El (iii) es trivial pues $M_k(\Gamma) \cdot M_{k'}(\Gamma) \subseteq M_{k+k'}(\Gamma)$. La prueba del inciso ($iv$) es elemental pero un poco técnica, entonces referimos al lector a §5.4 de [**?**]. □

Ahora estudiamos cómo transformar formas modulares en $M_k(\Gamma)$ a formas modulares en $M_k(\Gamma')$ donde Γ y Γ' son dos subgrupos de congruencia. Primero necesitamos lenguaje técnico de teoría de grupos:

Como $X(\Gamma)$ es una superficie de Riemann de primer tipo, su volumen es finito (c.f. [?**])

††Sea X una curva completa, no singular sobre un campo algebraicamente cerrado de género g (e.g. una superficie de Riemann compacta como una curva elíptica o $X(\Gamma)$). Sea K el divisor canónico sobre X y D cualquier divisor. Entonces

$$\ell(D) - \ell(K - D) = \deg D + 1 - g \quad , \quad \ell(D) := \dim H^0(X, \mathcal{L}(D))$$

donde $H^0(X, \mathcal{L}(D))$ es el primer grupo de cohomología de la gavilla invertible $\mathcal{L}(D)$ asociada a D bajo el isomofismo $\mathrm{Cl}(X) \cong \mathrm{Pic}(X)$ entre el grupo de divisores módulo divisores principales y el grupo de Picard (c.f. el teorema 1.3 del capítulo IV de [**?**] para una prueba).

Definición 18. Sean $\Gamma, \Gamma' \subseteq \mathrm{SL}_2(\mathbb{Z})$ subgrupos de congruencia y sea $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. Definimos la *clase bilateral* de α con respecto de Γ y Γ' como el conjunto:

$$\Gamma\alpha\Gamma' = \{\gamma\alpha\gamma' \in \mathrm{GL}_2^+(\mathbb{Q}) \mid \gamma \in \Gamma,\ \gamma' \in \Gamma'\}.$$

La multiplicación por la izquierda induce una acción $\Gamma \curvearrowright \Gamma\alpha\Gamma'$. Como Γ y Γ' son de congruencia, entonces esta acción particiona a la clase bilateral en una cantidad finita de órbitas (c.f. lemas 5.1.1 y 5.1.2 de [**?**]), más precisamente:

$$\exists \beta_1, \ldots, \beta_n \in \Gamma\alpha\Gamma' \text{ tal que } \Gamma\alpha\Gamma' = \bigsqcup_{i=1}^{n} \Gamma\beta_i, \tag{4}$$

donde $\sqcup$ denota la unión disjunta. Esta descomposición de la clase bilateral nos permite definir el siguiente operador:

Definición 19. Sean $k \in \mathbb{N}$, $\Gamma, \Gamma' \subseteq \mathrm{SL}_2(\mathbb{Z})$ subgrupos de congruencia y sea $\Gamma\alpha\Gamma'$ una clase bilateral para alguna $\alpha \in \mathrm{GL}_2(\mathbb{Q})$. Definimos el $[\Gamma\alpha\Gamma']_k-$operador como la función $[\Gamma\alpha\Gamma']_k : M_k(\Gamma) \to M_k(\Gamma')$ definida por

$$f[\Gamma\alpha\Gamma']_k = \sum_{i=1}^{n} f[\beta_i]_k,$$

donde $\Gamma\alpha\Gamma' = \sqcup\Gamma\beta_i$ es una descomposición como en (4).

Nota. La definición del $[\Gamma\alpha\Gamma']_k-$operador es independiente de la descomposición $\Gamma\alpha\Gamma' = \sqcup\Gamma\beta_i$. En efecto, si $\Gamma\beta = \Gamma\beta'$ para dos $\beta, \beta' \in \Gamma\alpha\Gamma'$ donde $\beta = \gamma\alpha\gamma'$ y $\beta' = \delta\alpha\delta'$, tenemos que

$$\alpha\gamma' = \gamma^{-1}\beta \in \Gamma\beta = \Gamma\beta' \quad \Longrightarrow \quad \alpha\gamma' = \sigma\beta' \quad \text{para alguna } \sigma \in \Gamma.$$

De esta manera:

$$f[\beta]_k = f[\gamma]_k[\alpha\gamma']_k = f[\gamma]_k[\sigma\beta']_k = f[\gamma\sigma]_k[\beta']_k \stackrel{*}{=} f[\beta']_k$$

donde (*) se sigue de que $\gamma\sigma \in \Gamma$ y $f \in M_k(\Gamma)$. La igualdad anterior garantiza que $\sum f[\beta_i]_k$ es independiente de los representantes $\beta_1, \ldots, \beta_n$.

Además, tenemos que el codominio de $[\Gamma\alpha\Gamma']_k$ efectivamente es $M_k(\Gamma')$. Para verificar esto observa que la multiplicación por la derecha por $\gamma' \in \Gamma'$ en el espacio cociente $\Gamma \setminus \Gamma\alpha\Gamma'$ de la acción izquierda $\Gamma \curvearrowright \Gamma\alpha\Gamma'$ es una biyección bien definida:

$$\Gamma \setminus \Gamma\alpha\Gamma' \longrightarrow \Gamma \setminus \Gamma\alpha\Gamma' \qquad \text{definido por} \quad \Gamma\delta \mapsto \Gamma\delta\gamma'.$$

Por lo tanto sumar sobre los representantes $\{\beta_1, \ldots, \beta_n\}$ de $\Gamma \setminus \Gamma\alpha\Gamma'$ es lo mismo que sumar sobre los representantes $\{\beta_1\gamma', \ldots, \beta_n\gamma'\}$. Por lo tanto si $f \in M_k(\Gamma)$, entonces para toda $\gamma' \in \Gamma'$ tenemos que:

$$\left(f[\Gamma\alpha\Gamma']_k\right)[\gamma']_k = \left(\sum f[\beta_i]_k\right)[\gamma']_k = \sum f[\beta_i\gamma']_k = \sum f[\beta_i]_k = f[\Gamma\alpha\Gamma']_k.$$

Esto quiere decir que $f[\Gamma\alpha\Gamma']_k$ es invariante bajo el $[\gamma']_k-$operador para toda $\gamma' \in \Gamma'$, es decir que $f[\Gamma\alpha\Gamma']_k$ es débilmente $(\Gamma', k)-$modular. Lo que le falta a $f[\Gamma\alpha\Gamma']_k$ para ser una forma modular es que sea holomorfo en ∞, pero esto se sigue del siguiente lema sencillo:

Lema 20. *Sean $f_1, \ldots, f_m : \mathbb{H} \to \mathbb{C}$ funciones donde cada f_i es $h_i\mathbb{Z}-$periódica y holomorfa en ∞. Entonces $f_1 + \cdots + f_m$ es holomorfa en ∞.*

Proof. Toma $h \in \mathbb{Z}^+$ como el mínimo común múltiplo de $h_1, \ldots, h_m$. Entonces $f := f_1 + \cdots + f_m$ es $h\mathbb{Z}-$periódico. Por lo tanto f_{cil} existe y su extensión holomorfa $\widehat{f_{\text{cil}}}$ es la suma de las extensiones holomorfas $\widehat{f_{i,\text{cil}}}$ de cada $f_{i,\text{cil}}$ inducida por cada f_i. Como la suma de funciones holomorfas es holomorfa, f_{cil} admite una extensión holomorfa al cero y por lo tanto $f_1 + \cdots + f_m$ es holomorfa en ∞. □

Hemos probado que el codominio del $[\Gamma\alpha\Gamma']_k-$operador es efectivamente $M_k(\Gamma')$.

Enseguida estudiamos un caso importante de los $[\Gamma\alpha\Gamma']_k-$operadores. Primero sea

$$\alpha_p = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}), \tag{5}$$

que corresponde a la transformación $z \mapsto z/p$. Entonces el $[\Gamma\alpha_p\Gamma']-$operador es muy importante:

Definición 21. Sea p un número primo, $k \in \mathbb{N}$ y $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ un subgrupo de congruencia. El *$p-$ésimo operador de Hecke de peso k con respecto de* Γ es el operador $T_p : M_k(\Gamma) \to M_k(\Gamma)$ definido por la clase lateral $\Gamma\alpha_p\Gamma$, i.e. $T_p = [\Gamma\alpha_p\Gamma]_k$ (véase (5) para la definición de α_p).

Resulta que si p y q son primos distintos, entonces sus respectivos operadores de Hecke conmutan (véase la proposición 24 más adelante). Entonces si pudieramos extender la definición del $p-$ésimo operador de Hecke para incluir potencias de primos p^β entonces podríamos usar la factorización única de los enteros para extender la definición de operador de Hecke para que incluya a todo entero. Pero para esto necesitamos introducir otro tipo de operador:

Recuerde que hay un epimorfismo $\Gamma_0(N) \twoheadrightarrow (\mathbb{Z}/N\mathbb{Z})^*$ con núcleo $\Gamma_1(N)$ (c.f. la sección 0.1.2). Entonces $\Gamma_1(N)$ es un subgrupo normal de $\Gamma_0(N)$. Así, cuando $\alpha \in \Gamma_0(N)$, tenemos que $\alpha^{-1}\Gamma_1(N)\alpha = \Gamma_1(N)$ y por lo tanto el cociente $\Gamma_1(N) \setminus \Gamma_1(N)\alpha\Gamma_1(N)$ tiene solamente un elemento: $\Gamma_1(N)\alpha$. De esta manera, si $f \in M_k(\Gamma_1(N))$, entonces:

$$f[\Gamma_1(N)\alpha\Gamma_1(N)]_k = f[\alpha]_k \qquad (\alpha \in \Gamma_0(N)).$$

Esta fórmula induce una acción de grupos $\Gamma_0(N) \curvearrowright M_k(\Gamma_1(N))$ que, restringido a $\Gamma_1(N)$ actúa trivialmente por definición de $M_k(\Gamma_1(N))$. Por lo tanto la acción desciende al cociente $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^*$. Esto quiere decir que podemos definir la siguiente clase de operadores:

Definición 22. Sea $d \in (\mathbb{Z}/N\mathbb{Z})^*$ (o en general $d \in \mathbb{Z}$ con $(d, N) = 1$). El operador *diamante* se define como la función $\langle d \rangle : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$ definido por:

$$\langle d \rangle f = f[\alpha]_k \quad \text{donde} \quad \alpha = \begin{pmatrix} a & b \\ c & d' \end{pmatrix} \in \Gamma_0(N) \ \text{ y } \ d \equiv d' \pmod{N}.$$

Una propiedad importante que cumplen los operadores diamante es:

Proposición 23. *Sea G el grupo dual de Pontryagin del grupo finito $\mathbb{Z}/N\mathbb{Z}$, i.e. $G = \mathrm{Hom}((\mathbb{Z}/N\mathbb{Z})^*, \mathbb{C}^*)$. Entonces $M_k(\Gamma_1(N))$ admite la siguiente descomposición:*

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi \in G} M_k(\Gamma_1(N), \chi),$$

donde definimos

$$M_k(\Gamma_1(N), \chi) = \left\{ f \in M_k(\Gamma_1(N)) \,\middle|\, \langle d \rangle f = \chi(d) f \quad \forall d \in (\mathbb{Z}/N\mathbb{Z})^* \right\}.$$

Proof. Definimos una función $G \to \mathrm{End}(M_k(\Gamma_1(N)))$ con $\chi \mapsto \pi_\chi$ donde

$$\pi_\chi = \frac{1}{\phi(N)} \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^*} \chi(d)^{-1} \langle d \rangle$$

como operadores. Para $\chi, \chi' \in G$ y $f \in M_k(\Gamma_1(N))$ tenemos que:

$$\begin{aligned}
\pi_{\chi'}\pi_\chi(f) = \pi_{\chi'}\left(\frac{1}{\phi(N)}\sum_d \chi(d)^{-1}\langle d\rangle f\right) &= \frac{1}{\phi(N)}\sum_d \chi(d)^{-1}\pi_{\chi'}\big(\langle d\rangle f\big) \\
&= \frac{1}{\phi(N)}\sum_d \chi(d)^{-1}\left(\frac{1}{\phi(N)}\sum_e \chi'(e)^{-1}\langle e\rangle\langle d\rangle f\right) \\
&= \frac{1}{\phi(N)}\sum_d \chi(d)^{-1}\chi'(d)\left(\frac{1}{\phi(N)}\sum_e \chi'(ed)^{-1}\langle ed\rangle f\right),
\end{aligned}$$

donde $\langle e\rangle\langle d\rangle = \langle ed\rangle$ por la proposición 24 abajo. Como $e \mapsto de$ es una permutación de $(\mathbb{Z}/N\mathbb{Z})^*$, lo que está en paréntesis es simplemente $\pi_{\chi'}(f)$ que, por cierto, no depende de d. De las relaciones de ortogonalidad bien conocidas que cumplen los caracteres de grupos finitos[‡‡] obtenemos:

$$\pi_{\chi'}\pi_\chi(f) = \pi_{\chi'}(f)\left(\frac{1}{\phi(N)}\sum_d \chi(d)^{-1}\chi'(d)\right) = \begin{cases}\pi_{\chi'}(f) & \chi = \chi' \\ 0 & \chi \neq \chi'\end{cases}.$$

Simbólicamente

$$\pi_\chi^2 = \pi_\chi \quad \text{y} \quad \pi_{\chi'}\pi_\chi = 0 \quad (\chi \neq \chi'). \tag{6}$$

Ahora, si $f \in M_k(\Gamma_1(N))$ tenemos las siguientes dos igualdades:

$$\begin{gathered}
\langle d\rangle\pi_\chi(f) = \frac{1}{\phi(N)}\sum_e \chi(e)^{-1}\langle de\rangle(f) = \frac{\chi(d)}{\phi(N)}\left(\sum_e \chi(de)^{-1}\langle de\rangle f\right) = \chi(d)\pi_\chi f, \\
\left(\sum_{\chi\in G}\pi_\chi\right)(f) = \sum_\chi \frac{1}{\phi(N)}\sum_d \chi(d)^{-1}\langle d\rangle f = \sum_d\left(\frac{1}{\phi(N)}\sum_\chi \chi(d)^{-1}\right)\langle d\rangle f \overset{*}{=} \langle 1\rangle f = f,
\end{gathered}$$

donde $(*)$ se sigue del hecho de que la suma dentro de los paréntesis suma 0 cuando $d \neq 1$.[§§] Estas dos igualdades implican respectivamente que

$$\pi_\chi(M_k(\Gamma_1(N))) \subseteq M_k(\Gamma_1(N), \chi) \quad \text{y} \quad \sum_{\chi\in G}\pi_\chi = \mathrm{Id}. \tag{7}$$

Por último, si además $f \in M_k(\Gamma_1(N), \chi)$ entonces:

$$\pi_\chi(f) = \frac{1}{\phi(N)}\sum_d \chi(d)^{-1}\langle d\rangle f = \frac{1}{\phi(N)}\sum_d \chi(d)^{-1}\chi(d) f = f\left(\frac{1}{\phi(N)}\sum_d 1\right) = f$$

[‡‡]Véase, por ejemplo, el capítulo 16, §3 de [**?**] y en particular la proposición 16.3.1.

[§§]Como $d \neq 1$, d determina un caracter no trivial del grupo finito G y es conocido que la suma de todos los valores un caracter no trivial es 0. Este argumento está en la prueba de la proposición 16.3.1 de [**?**].

y por lo tanto

$$\pi_\chi|_{M_k(\Gamma_1(N),\chi)} = \mathrm{Id}. \tag{8}$$

De (6), (7) y (8) se sigue que $M_k(\Gamma_1(N),\chi)$ es un sumando directo de $M_k(\Gamma_1(N))$. De la segunda parte de (7) se sigue que los subespacios $M_k(\Gamma_1(N),\chi)$ generan a $M_k(\Gamma_1(N))$ y de la segunda parte de (6) se sigue que la intersección de esos subespacios es trivial. Por lo tanto $M_k(\Gamma_1(N))$ es la suma directa de sus subespacios $M_k(\Gamma_1(N),\chi)$ donde χ corre sobre G. □

Estos dos tipos de operadores cumplen muchas propiedades, entre ellas:

Proposición 24. *Sean $e, d \in (\mathbb{Z}/N\mathbb{Z})^*$ y $p, q \in \mathbb{Z}$ primos. Entonces:*

i) $\langle d\rangle T_p = T_p\langle d\rangle$.

ii) $\langle d\rangle\langle e\rangle = \langle de\rangle = \langle e\rangle\langle d\rangle$

iii) $T_pT_q = T_qT_p$ *cuando* $p \neq q$.

iv) Si $f \in M_k(\Gamma_1(N))$ entonces la serie de Fourier de T_pf es:

$$(T_pf)_\infty(q) = \sum_{n=0}^{\infty} a_{pn}(f)q^n + p^{k-1}\sum_{n=0}^{\infty} a_n\big(\langle p\rangle f\big)q^{np} \quad (q = e^{2\pi iz}).$$

Proof. Esto es exactamente la proposición 5.2.4 de [?]. □

De una manera similar a los caracteres de Dirichlet, podemos extender la definición del operador diamante $\langle d\rangle : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$ para d cualquier entero. Además, para extender la definición de T_p, requerimos definir T_{p^β} inductivamente usando los operadores diamante $\langle p\rangle$.

Definición 25. Sea $n \in \mathbb{Z}^+$, entonces definimos el operador diamante $\langle n\rangle : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$ como

$$\langle n\rangle = \begin{cases} \langle n\rangle & (N,n) = 1 \\ 0 & (N,n) > 1 \end{cases}.$$

Además, si $n = p_1^{\beta_1}\cdots p_m^{\beta_m}$ definimos $T_n : M_k(\Gamma) \to M_k(\Gamma)$ como el producto $T_n = T_{p_1^{\beta_1}}\cdots T_{p_m^{\beta_m}}$ donde cada $T_{p_i^{\beta_i}}$ se define inductivamente como:

$$T_{p^\beta} = T_pT_{p^{\beta-1}} - p^{k-1}\langle p\rangle T_{p^{\beta-2}}.$$

Notas. El operador $\langle n\rangle$ es completamente multiplicativa, i.e. $\langle nm\rangle = \langle n\rangle\langle m\rangle$ para todas $n, m \in \mathbb{Z}$. Además es inmediato que $\langle n\rangle$ sigue conmutando con T_m como en la proposición 24.*i*:

$$T_m\langle n\rangle = \langle n\rangle T_m \qquad \forall n, m \in \mathbb{Z}^+. \tag{9}$$

Por otro lado las T_m's no siempre conmutan. Solamente tenemos

$$T_mT_n = T_{nm} = T_nT_m \qquad \forall (n,m) = 1 \tag{10}$$

por un argumento de inducción sobre la definición de T_{p^β}.

Nota. Con respecto del producto interior de Petersson, si $p \nmid N$, el operador adjunto de $\langle p \rangle$ es $\langle p^{-1} \rangle$ (donde p^{-1} es el inverso de $p \mod N$) y el operador adjunto de T_p es $\langle p^{-1} \rangle T_p$ (c.f. el teorema 5.5.3 de [**?**]). Por lo tanto la proposición 24 nos garantiza que $\langle p \rangle$ y T_p son operadores normales (i.e. conmutan con su operador adjunto) de la cual se sigue el siguiente resultado:

Proposición 26. *Sea $(n, N) = 1$. Los operadores de Hecke $\langle n \rangle, T_n : S_k(\Gamma_1(N)) \to S_k(\Gamma_1(N))$ son operadores normales con respecto del producto interior de Petersson.*

Corolario 27. *El espacio $S_k(\Gamma_1(N))$ tiene una base ortogonal de vectores propios simultáneos para los operadores de Hecke $\{\langle n \rangle, T_n \mid (n, N) = 1\}$.*

Proof. El teorema espectral de álgebra lineal para operadores normales. □

Los operadores de Hecke actúan sobre las series de Fourier de la siguiente manera:

Proposición 28. *Sea $f \in M_k(\Gamma_1(N))$ con serie de Fourier $f_\infty(q) = \sum_{m \geq 1} a_m(f) q^m$ donde $q = e^{2\pi i z}$. Entonces los coeficientes de Fourier de $T_n f$ están dados por*

$$a_m(T_n f) = \sum_{d \mid (m,n)} d^{k-1} a_{nm/d^2}\big(\langle d \rangle f\big).$$

En particular, si $(n, m) = 1$, la fórmula anterior se reduce a:

$$a_m(T_n f) = a_{nm}(f).$$

Proof. c.f. a la proposición 5.3.1 de [**?**]. □

0.1.4 Formas primitivas

En esta sección vamos a fijar el subgrupo de congruencia a $\Gamma_0(N)$. Todos los resultados de esta sección si pueden probar análogamente para $\Gamma_1(N)$, pero como $\Gamma_1(N) \subset \Gamma_0(N)$, mejor estudiamos $\Gamma_0(N)$.

En la sección pasada vimos cómo cambiar de subgrupo de congruencia con los $[\Gamma \alpha \Gamma']-$operadores. Ahora estudiamos un caso particular muy importante: cambiar de nivel.

Sean N y M dos niveles con $M \mid N$. Entonces hay dos maneras de encajar $S_k(\Gamma_0(M))$ en $S_k(\Gamma_0(N))$. La más sencilla es simplemente la inclusión: si

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

entonces $N \mid c$ y por la transitividad de la divisibilidad tenemos que $M \mid c$. Por lo tanto $\gamma \in \Gamma_0(M)$. De esta manera $\Gamma_0(N) \subseteq \Gamma_0(M)$ y así

$$M \mid N \quad \Longrightarrow \quad S_k(\Gamma_0(M)) \subseteq S_k(\Gamma_0(N)).$$

La otra manera de encajar $S_k(\Gamma_0(M))$ en $S_k(\Gamma_0(N))$ es "multiplicando el nivel por un divisor de N/M". Más precisamente, sea d un divisor de N/M y definimos

$$\beta_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}).$$

Observe que, si $f \in S_k(\Gamma_0(M))$, entonces $f[\beta_d]_k(z) = d^{k/2} f(dz)$. Afirmamos que $f[\beta_d]_k \in S_k(\Gamma_0(Md)) \subseteq S_k(\Gamma_0(N))$. De hecho se cumple algo más general:

Lema 29. *Si $f \in S_k(\Gamma_0(M))$ y $g(z) = f(dz)$, entonces $g \in S_k(\Gamma_0(Md))$.*

Proof. Sea $\gamma \in \Gamma_0(Md)$. Observe que $g(z) = f(dz) = f(\beta_d z)$. Entonces calculamos:

$$\big(g[\gamma]_k\big)(z) = j(\gamma, z)^{-k} g(\gamma z) = j(\beta_d\gamma, z)^{-k} f(\beta_d \gamma z)$$

donde hemos usado $j(\gamma, z) = j(\gamma\beta_d, z)$ porque multiplicar γ por β_d no altera el segundo renglón de γ. Ahora, observe que:

$$\underbrace{\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}}_{\beta_d} \underbrace{\begin{pmatrix} a & b \\ c & e \end{pmatrix}}_{\gamma} = \underbrace{\begin{pmatrix} a & bd \\ c/d & e \end{pmatrix}}_{\gamma'} \underbrace{\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}}_{\beta_d}$$

donde $\gamma' \in \Gamma_0(M)$ poque $Md \mid c$. Entonces

$$\big(g[\gamma]_k\big)(z) = j(\gamma'\beta_d, z)^{-k} f(\gamma'\beta_d z) = j(\gamma' z)^{-k} f(\gamma'\beta_d z) = f[\gamma']_k(\beta_d z) = f(dz) = g(z)$$

porque $f \in S_k(\Gamma_0(M))$. Por lo tanto $g \in S_k(\Gamma_0(Md))$. □

En conclusión, si $M \mid N$ y $d \mid N/M$, la función $S_k(\Gamma_0(M)) \to S_k(\Gamma_0(N))$ definida por $f \mapsto f[\beta_d]_k$ está bien definida. Además, la función es inyeciva porque si $f[\beta_d]_k = 0$ claramente $f = 0$; está la segunda manera de encajar $S_k(\Gamma_0(M))$ en $S_k(\Gamma_0(N))$.

Sea d es un divisor de N definimos la función:

$$\iota_d : S_k(\Gamma_0(N/d)) \times S_k(\Gamma_0(N/d)) \longrightarrow S_k(\Gamma_0(N)) \quad \text{definido por} \quad (f, g) \mapsto f + g[\beta_d]_k.$$

Definimos:

Definición 30. El subespacio de $S_k(\Gamma_0(N))$ generado por las imágenes de $\{\iota_d : d \mid N\}$ se llama el *subespacio de formas viejas* y se denota por:

$$S_k^{\text{old}}(\Gamma_0(N)) = \sum_{d \mid N} \iota_d\big(S_k(\Gamma_0(N/d)) \times S_k(\Gamma_0(N/d))\big).$$

El complemento ortogonal del subespacio de formas viejas (con respecto del producto interior de Petersson) se llama el *subespacio de formas nuevas* y se denota por:

$$S_k^{\text{new}}(\Gamma_0(N)) = \big(S_k^{\text{old}}(\Gamma_0(N))\big)^{\perp}.$$

Intuitivamente el espacio de fomas viejas son todas las fomas de $\Gamma_0(N)$ que provienen de un $\Gamma_0(M)$ de nivel más bajo mediante una combinación lineal de los dos métodos anteriormente mencionados.

Estos dos subespacios cumplen tres propiedades importantes:

Proposición 31. *Sean $T_n, \langle n\rangle : S_k(\Gamma_0(N)) \to S_k(\Gamma_0(N))$ los operadores de Hecke para toda $n \in \mathbb{Z}^+$, entonces:*

i) Los subespacios $S_k^{\text{new}}(\Gamma_0(N))$ y $S_k^{\text{old}}(\Gamma_0(N))$ son estables bajo todos los operadores de Hecke.

ii) En particular, $S_k^{\text{new}}(\Gamma_0(N))$ y $S_k^{\text{old}}(\Gamma_0(N))$ ambos tienen bases ortogonales formadas por vectores propios simultáneos de los operadores $\{T_n, \langle n\rangle \mid (n, N) = 1\}$.

iii) (Atkin-Lehner) Sea $f \in S_k(\Gamma_0(N))$ con serie de Fourier $f_\infty(q) = \sum_{n\geq 1} a_n(f)q^n$, entonces:

$$a_n(f) = 0,\ \forall (n, N) = 1 \quad \Longleftrightarrow \quad \forall p \mid N,\ \exists f_p \in S_k(\Gamma_0(N/p)) \quad \text{tales que} \quad f(z) = \sum_{p\mid N} f_p(pz).$$

En este caso tenemos que $f \in S_k^{\mathrm{old}}(\Gamma_0(N))$.

Proof. Los primeros dos incisos vienen en [?, §5.7]. La dirección "$\Longleftarrow$" es relativamente sencillo de verificar a diferencia de la dirección "$\Longrightarrow$" que es mucho más complicado. Atkin y Lehner publicaron la primera prueba de (*iii*) en 1970 [?]. En [?, §5.7] viene una prueba detallada debida a David Carlton. □

Definición 32. Sea $f \in S_k(\Gamma_0(N))$ distinto de 0. Decimos que es una *eigenforma* si es un vector propio simultaneo de todos los operadores de Hecke $\{T_n, \langle n\rangle\}_{n\geq 1}$. Si además $f \in S_k^{\mathrm{new}}(\Gamma_0(N))$ y está *normalizada*, i.e. $a_1(f) = 1$, decimos que f es una *forma primitiva*.

Nota. Puede suceder que una forma $f \in S_k(\Gamma_0(N))$ no sea eigenforma pero sí sea un vector propio simultaneo de los operadores $\{T_n, \langle n\rangle \mid (n, N) = 1\}$. En este caso decimos que f es una *eigenforma fuera de N*. Similarmente, si f es además una forma nueva normalizada, decimos que es una *forma primitiva fuera de N*.

Los coeficientes de Fourier de una forma primitiva determinan sus valores propios. Para probar esto primero necesitamos un lema que es consecuencia del teorema de Atkin-Lehner:

Lema 33. *Si $f \in S_k(\Gamma_0(N))$ es una eigenforma fuera de N y $a_1(f) = 0$, entonces $f \in S_k^{\mathrm{old}}(\Gamma_0(N))$.*

Proof. Por hipótesis f es vector propio simultaneo para los operadores $\{T_n, \langle n\rangle \mid (n, N) = 1\}$, es decir existen $b_n, c_n \in \mathbb{C}$ tales que

$$T_n f = b_n f \quad \text{y} \quad \langle n\rangle f = c_n f \qquad \text{donde } (n, N) = 1. \tag{11}$$

Por un lado tenemos:

$$c_{nm} f = \langle nm\rangle f = \langle n\rangle\langle m\rangle f = \langle n\rangle(c_m f) = c_m c_n f,$$

entonces $c_{nm} = c_n c_m$. Lo cual quiere decir que la función $n \mapsto c_n$ es un caracter $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$. En particular $\langle n\rangle f = c_n f = \chi(n) f$ y así $f \in S_k(\Gamma_0(N), \chi)$.

Ahora, usamos la proposición 28 para calcular $a_1(T_n f)$ para cualquier $n \in \mathbb{Z}^+$. Obtenemos

$$a_1(T_n f) = a_n(f) \qquad \forall n \in \mathbb{Z}^+. \tag{12}$$

Además, como f es una eigenforma fuera de N, tenemos por otro lado que

$$a_1(T_n f) = a_1(b_n f) = b_n a_1(f). \tag{13}$$

Si juntamos las dos fórmulas anteriores concluimos que

$$a_n(f) = b_n a_1(f) \qquad \forall\ (n, N) = 1. \tag{14}$$

Por hipótesis $a_1(f) = 0$, entonces la fórmula (14) implica que $a_n(f) = 0$ para toda $(n, N) = 1$. Por el teorema de Atkin-Lehner (proposición 31) tenemos que $f \in S_k^{\mathrm{old}}(\Gamma_0(N))$. □

Teorema 34. *Sea $f \in S_k^{\text{new}}(\Gamma_0(N))$ una forma primitiva fuera de N, entonces los coeficientes de Fourier de f fuera de N son sus valores propios con respecto a los operadores de Hecke fuera de N, es decir $T_n f = a_n(f)f$ para toda $(n, N) = 1$.*

Proof. Fijamos $m \geq 1$ tal que $(m, N) = 1$ y definimos $g_m = T_m f - a_m(f)f$; queremos probar que $g_m = 0$. Como $S_k^{\text{new}}(\Gamma_0(N))$ es estable bajo T_m (por la proposición 31) entonces $T_m f \in S_k^{\text{new}}(\Gamma_0(N))$ y así $g_m \in S_k^{\text{new}}(\Gamma_0(N))$. Por otro lado g_m es una eigenforma fuera de N. Para ver esto, sea n tal que $(n, N) = 1$. Primero calculamos

$$\langle n \rangle g_m = \langle n \rangle (T_m f - a_m(f)f) = T_m \langle n \rangle f - a_n(f) \langle n \rangle f = c_n(T_m f - a_m(f)f) = c_n g_m,$$

donde c_n es el valor propio de f bajo $\langle n \rangle$ (c.f. la prueba lema 33). Por lo tanto g_m es un vector propio de $\langle n \rangle$ para toda $(n, N) = 1$.

Para ver que g_m es un vector propio de T_n, tenemos que considerar primero el caso $n = p^\alpha$ para algún primo p y un exponente $\alpha \geq 1$, y después usamos la definición de T_n para reducir la cuestión al caso anterior. Primero sea $n = p^\alpha$ y hacemos inducción. Para $\alpha = 1$ tenemos

$$\begin{aligned} T_p g_m &= T_p(T_m f - a_m(f)f) = T_p T_m f - a_m(f) T_p f = T_p(b_m f) - a_m(f) b_p f = b_p(b_m f - a_m(f)f) \\ &= b_p g_m, \end{aligned}$$

donde hemos usado la notación de la ecuación (11).

Ahora supongamos que g_m es vector propio para los operadores $\{T_p, T_{p^2}, \ldots, T_{p^{\alpha-1}}\}$ con valores propios $b_p, b_{p^2}, \ldots, b_{p^{\alpha-1}}$ respectivamente. Con la fórmula recursiva de T_{p^α} obtenemos:

$$\begin{aligned} T_{p^\alpha} g_m &= (T_p T_{p^{\alpha-1}} + p^{\alpha-1} \langle p \rangle T_{p^{\alpha-2}}) g_m = T_p T_{p^{\alpha-1}} g_m + p^{\alpha-1} T_{p^{\alpha-2}} \langle p \rangle g_m \\ &= T_p(b_{p^{\alpha-1}} g_m) + p^{\alpha-1} T_{p^{\alpha-2}}(c_p g_m) = \big(b_p b_{p^{\alpha-1}} + p^{\alpha-1} b_{p^{\alpha-2}} c_p\big) g_m. \end{aligned}$$

Hemos probado que g_m es un vector propio para todo operador en $\{T_{p^\alpha} \mid \alpha \geq 1, \, (p, N) = 1\}$.

Con esto podemos probar que g_m es vector propio de T_n para toda $(n, N) = 1$. Primero sea $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ la factorización única de n. Como g_m es vector propio de cada $T_{p_i^{\alpha_i}}$ por lo anterior, existen constantes $d_1, \ldots, d_t \in \mathbb{C}$ tales que $T_{p_i^{\alpha_i}} g_m = d_i g_m$. Con esto calculamos:

$$T_n g_m = T_{p_1^{\alpha_1}} \cdots T_{p_t^{\alpha_t}} g_m = T_{p_1^{\alpha_1}} \cdots T_{p_{t-1}^{\alpha_{t-1}}}(d_t g_m) = \cdots = (d_1 \cdots d_t) g_m$$

y por lo tanto g_m es un vector propio de T_n para toda $(n, N) = 1$, i.e. g_m es una eigenforma fuera de N.

Para poder aplicar el lema anterior, necesitamos calcular $a_1(g_m)$. Como la función $f \mapsto a_1(f)$ es $\mathbb{C}-$lineal, tenemos:

$$a_1(g_m) = a_1(T_m f - a_m(f)f) = a_1(T_m f) - a_m(f) a_1(f) \overset{(12)}{=} a_m(f)\big(1 - a_1(f)\big).$$

Como f es primitivo, está normalizado, entonces la ecuación anterior se reduce a $a_1(g_m) = 0$. Aplicamos el lema 33 y deducimos que $g_m \in S_k^{\text{old}}(\Gamma_0(N))$. Ya teníamos que $g_m \in S_k^{\text{new}}(\Gamma_0(N)) = S_k^{\text{old}}(\Gamma_0(N))^\perp$, entonces $g_m = 0$ y terminamos. $\square$

Cerramos la sección con una propiedad más que cumplen las eigenformas:

Proposición 35. *Sea $f \in S_k^{\mathrm{new}}(\Gamma_0(N), \chi)$ una forma primitiva. Entonces si denotamos $\lambda = \{a_n(f), \chi(n)\}_{n\geq 1}$, la extensión $\mathbb{Q}(\lambda)$ de $\mathbb{Q}$ es finita. Al campo $\mathbb{Q}(\lambda)$ se denota por K_f y se llama el* campo numérico de f.

Proof. Para una prueba con geometría algebráica, consulte [**?**, proposición 2.7.3 de §2] o [**?**, §6.5]. En seguida escribimos una prueba elemental debida a Serre que aparece en [**?**, §2.5].

buscar cita y poner prueba

Primero comentamos que por definición de T_n podemos asumir que $n = p$ es primo. Introducimos la siguiente notación: a cada forma primitiva $g \in S_k(\Gamma_0(N), \chi)$ le asociamos su sistema de valores propios:

$$\lambda(g) = \{b_p \in \mathbb{C} \mid T_p g = b_p g\}$$

Al conjunto de sistemas de valores propios lo denotamos por:

$$\Lambda = \{\lambda(g) \subset \mathbb{C} \mid g \in S_k(\Gamma_0(N), \chi) \text{ es una forma primitiva}\}.$$

Como $S_k(\Gamma_0(N), \chi)$ es de dimensión finita, solamente puede haber una cantidad finita de sistemas de valores propios (pues una infinidad de sistemas de valores propios induce un conjunto linealmente independiente inifinto). Escribimos $\mathbb{Q}(\chi)$ para denotar la extensión de $\mathbb{Q}$ por la imagen del caracter χ y denotamos $G = \mathrm{Gal}(\mathbb{C}|\mathbb{Q}(\chi))$. Este gupo de Galois actúa sobre los coeficientes de Fourier de las forma primitiva. Más precisamente, si $g \in S_k(\Gamma_0(N), \chi)$ es una forma primitiva con serie de Fouier $g(z) = \sum a_m(g) q^m$ y $\sigma \in G$, entonces definimos g^σ con la serie de Fourier:

$$g^\sigma(z) = \sum_{m=1}^{\infty} a_m(g)^\sigma q^m,$$

o en otras palabras, $a_m(g^\sigma) = a_m(g)^\sigma$. Además, si escibimos $h := \chi(n) g$, tenemos que:

$$a_m(h^\sigma) = a_m(h)^\sigma = (\chi(n) a_m(g))^\sigma = \chi^\sigma(n) a_m(g)^\sigma = \chi(n) a_m(g^\sigma) = a_m(\chi(n) g^\sigma) \quad \big(\forall m \geq 1\big)$$

y por lo tanto $(\chi(n)g)^\sigma = \chi(n) g^\sigma$. Esto, junto con

$$f \in S_k(\Gamma_0(N), \chi) \quad \Longrightarrow \quad f^\sigma \in S_k(\Gamma_0(N), \chi^\sigma) = S_k(\Gamma_0(N), \chi)$$

(c.f. [**?**, teorema 6.5.4] o [**?**, §3.5]), tenemos que

$$\langle n \rangle g^\sigma = \chi^\sigma(n) g^\sigma = \chi(n) g^\sigma = (\chi(n) g)^\sigma = (\langle n \rangle g)^\sigma \tag{15}$$

Con esta notación y con la fórmula para calcular coeficientes de Fourier de $T_p g$ (la proposición 28), tenemos que para $\sigma \in G$

$$\begin{aligned}
a_m(T_p g)^\sigma &= \left(\sum_{d|(m,p)} d^{k-1} a_{pm/d^2}(\langle d \rangle g) \right)^\sigma = \sum_d (d^{k-1})^\sigma \chi^\sigma(d) \big(a_{pm/d^2}(g)\big)^\sigma \\
&= \sum_d d^{k-1} \chi(d) \big(a_{pm/d^2}(g)\big)^\sigma \qquad \big(\text{porque } \ \chi^\sigma = \chi\big) \\
&= \sum_d d^{k-1} \chi(d) a_{pm/d^2}(g^\sigma) = \sum_d d^{k-1} a_{pm/d^2}(\chi(d) g^\sigma) \\
&\overset{(15)}{=} \sum_d d^{k-1} a_{pm/d^2}(\langle d \rangle g^\sigma) \\
&= a_m(T_p g^\sigma) \quad \forall m \geq 1. \\
\therefore \quad T_p g^\sigma = (T_p g)^\sigma &= \big(a_p(g) g\big)^\sigma = a_p(g)^\sigma g^\sigma.
\end{aligned}$$

En otras palabras, $a_p(g)^\sigma$ es el valor propio de g bajo T_p. Por lo tanto tenemos una acción de grupos $G \curvearrowright \Lambda$ definido por $\lambda(g) \mapsto \lambda(g^\sigma)$.

Ahora fijamos $f \in S_k^{\text{new}}(\Gamma_0(N), \chi)$. La órbita de $\lambda(f) \in \Lambda$, que es finita porque Λ es finita, está en biyección con $G/G_{\lambda(f)}$ donde $G_{\lambda(f)} = \{\sigma \in G \mid \lambda(f) = \lambda(f^\sigma)\}$ es el estabilizador de $\lambda(f)$. Por lo tanto $G_{\lambda(f)}$ es de índice finito y así K, el campo fijo de $G_{\lambda(f)}$ es una extensión finita de $\mathbb{Q}(\chi)$. Claramente $\lambda(f) \subset K$ pues si $\sigma \in G_{\lambda(f)}$ tenemos que

$$\{a_p(f)\}_p = \lambda(f) = \lambda(f^\sigma) = \{a_p(f)^\sigma\}_p \quad \Longrightarrow \quad a_p(f) = a_p(f)^\sigma \quad \Longrightarrow \quad a_p(f) \in K \quad \forall p.$$

Como K es una extensión finita de $\mathbb{Q}(\chi)$, también es finita sobre $\mathbb{Q}$ así $K_f \subseteq K$ y K_f es una extensión finita de $\mathbb{Q}$. $\square$

0.1.5 Series de Eisenstein

Unos buenos ejemplos de formas modulares son las series de Eisenstein. Hay varios estilos de series de Eisenstein, el más sencillo se define como

$$E_{2k}(z) := \frac{1}{2}\sum_{n,m\in\mathbb{Z}}{}' \frac{1}{(mz+n)^{2k}} \qquad (k \geq 2),$$

donde la notación Σ' excluye el sumando $n = m = 0$. Calculamos cómo se transforman E_{2k} bajo la acción $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{H}$.

Toda matriz

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

induce una permutación

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z} \quad \text{definido por} \quad (m,n) \mapsto \gamma^t(m,n) = (am + cn, bm + dn)$$

con inverso $(m,n) \mapsto (\gamma^t)^{-1}(m,n)$. En particular, como $(0,0) \mapsto (0,0)$, la función anterior permuta los elementos de $\mathbb{Z} \times \mathbb{Z} - \{(0,0)\}$. Por lo tanto:

$$\begin{aligned} E_{2k}\left(\frac{az+b}{cz+d}\right) &= \frac{1}{2}\sum_{n,m\in\mathbb{Z}}{}' \frac{1}{(m\frac{az+b}{cz+d} + n)^{2k}} = \frac{1}{2}\sum_{n,m\in\mathbb{Z}}{}' \frac{(cz+d)^{2k}}{(maz + mb + ncz + d)^{2k}} \\ &= \frac{(cz+d)^{2k}}{2}\sum_{n,m\in\mathbb{Z}}{}' \frac{1}{((ma+nc)z + (mb+nd))^{2k}} \\ &= \frac{(cz+d)^{2k}}{2}\sum_{n,m\in\mathbb{Z}}{}' \frac{1}{(mz+n)^{2k}} \\ &= (cz+d)^{2k} E_{2k}(z). \end{aligned} \tag{16}$$

Para justificar la permutación de los sumandos, debemos probar que la serie definida por E_{2k} es absolutamente convergente. Para esto sean $\omega_1, \omega_2 \in \mathbb{C}^*$ tales que $\frac{\omega_1}{\omega_2} = z$, entonces $L := \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subset \mathbb{C}$ es una retícula, ie. $\{\omega_1, \omega_2\}$ es una $\mathbb{R}$-base de $\mathbb{C}$ (esto sucede porque $\Im(\omega_1/\omega_2) = \Im(z) > 0$ implica que ω_1 y ω_2 no son colineales). De esta manera, si $\sigma \in \mathbb{R}$:

$$\sum_{n,m\in\mathbb{Z}}{}' \frac{1}{|mz+n|^\sigma} = \sum_{n,m\in\mathbb{Z}}{}' \frac{\omega_2^\sigma}{|m\omega_1 + n\omega_2|^\sigma} = \omega_2^\sigma \sum_{\lambda\in L}{}' \frac{1}{|\lambda|^\sigma},$$

otra vez, la notación Σ' excluye el sumando $\lambda = 0$ de la suma. Por lo tanto la convergencia absoluta de la serie E_{2k} se reduce a probar la convergencia del lado derecho. Este fenómeno es bien conocido:

Proposición 36. *Sea $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subset \mathbb{C}$ una retícula, entonces:*

$$\sum_{\lambda \in L}{}' \frac{1}{|\lambda|^{\sigma}} \text{ converge} \quad \Longleftrightarrow \quad \sigma > 2$$

Nota. Serre da dos pruebas en [**?**, §VII.2.2] y Shimura da otra prueba en [**?**, §III.8].

Por lo tanto, cuando $k \geq 2$, la fórmula (16) es válida y concluimos que la serie de Eisenstein E_{2k} es débilmente $(\Gamma(1), 2k)-$modular. Para terminar de probar que E_{2k} es una forma modular, debemos probar que es holomorfa en ∞ (recuerde que $\Gamma(1)$ solamente tiene una cúspide).

Es bien conocido (por ejemplo [**?**, §1.3, pg. 28]) que E_{2k} tiene la siguiente expansión en serie de Fourier:

$$E_{2k}(z) = \zeta(2k) + \frac{(-1)^k (2\pi)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \left(\sum_{d|n} d^{2k-1} \right) e^{2\pi i n z} \tag{17}$$

Esta fórmula claramente prueba que $E_{2k}(z)$ es holomorfa en ∞ porque no tiene coeficientes negativos de Fourier. Concluimos que las fórmulas (16) y (17) implican que $E_{2k} \in M_{2k}(\Gamma(1))$.

Si usamos los números de Bernoulli y la identidad famosa

$$B_{2n} = (-1)^{n+1} \frac{2(2n)!}{(2\pi)^{2n}} \zeta(2n) \qquad (n > 1)$$

descubierta por Euler en 1735 [**?**], podemos reescribir la serie de Fourier como:

$$\frac{1}{\zeta(2k)} E_{2k}(z) = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) e^{2\pi i n z}$$

donde $\sigma_{2k-1}(n)$ es la notación clásica para denotar $\sum_{d|n} d^{2k-1}$. Observa que el primer coeficiente es 1; en este caso se dice que la serie $E'_{2k}(z) := \zeta(2k)^{-1} E_{2k}(z)$ está normalizada.

En la prueba de STW semiestable, cuando se aplica el teorema de Langlands-Tunnell para probar la modularidad de $\bar{\rho}_{E,3}$, aparece una serie de Eisenstein generalizada obtenida "torciendo" a E_{2k} con un caracter de Dirichlet χ. Más precisamente definimos

$$E_{k,\chi}(z) := \sum_{n,m \in \mathbb{Z}}{}' \frac{\chi(m)}{(mz+n)^k}$$

donde χ es un caracter de Dirichlet. El problema con esta serie es que en la demostración de la modularidad de $\bar{\rho}_{E,3}$, necesitamos que el peso sea $k = 1$ y la serie anterior no converge para este valor de k. Para poder evadir este problema, introducimos un factor adicional que depende de un parametro complejo s:

Definición 37. Sea $k \in \mathbb{Z}$ y $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ un caracter de Dirichlet módulo N, entonces la *serie de Eisenstein de peso k y caracter χ y parametro s* se define como

$$E_{k,\chi}(z, s) := \sum_{n,m \in \mathbb{Z}} \frac{\chi(m)}{(mz+n)^k \, |mz+n|^{2s}}$$

donde $z \in \mathbb{H}$ y $s \in \mathbb{C}$.

Por proposición 36 la serie $E_{k,\chi}(z,s)$ es absolutamente convergente cuando $k+2\Re(s)>2$ o equivalentemente $\Re(s)>1-\frac{k}{2}$ (observa que el factor $\chi(m)$ no afecta la convergencia absoluta porque $|\chi(m)|=1$). Además la serie es uniformemente convergente en cualquier conjunto compacto K en el semiplano $\Re(s)>1-\frac{k}{2}$ porque para cualquier compacto en este semiplano, existe una $\varepsilon>0$ tal que $\Re(s)>1-\frac{k}{2}+\frac{\varepsilon}{2}$ para toda $s\in K$. De esta manera $k+2\Re(s)>2+\varepsilon$ y tenemos que:

$$\sum_{n,m\in\mathbb{Z}}{}' \frac{1}{|mz+n|^{k+2\Re(s)}} \leq \sum_{n,m\in\mathbb{Z}}{}' \frac{1}{|mz+n|^{2+\varepsilon}} < \infty \qquad (\forall s\in K).$$

Por lo tanto la serie $E_{k,\chi}(z,s)$ es uniformemente convergente en s sobre cualquier compacto contenido en el semiplano $\Re(s)>1-\frac{k}{2}$. Por el teorema de Weierstrass, esto implica que $E_{k,\chi}(z,s)$ define una función holomorfa en s sobre el semiplano $\Re(s)>1-\frac{k}{2}$.

Sea

$$\gamma=\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in\Gamma_0(N)$$

entonces:

$$\begin{aligned}
E_{k,\chi}(\gamma z,s) &= \sum_{n,m\in\mathbb{Z}}{}' \frac{\chi(m)}{\left(m\frac{az+b}{cz+d}+n\right)^k \left|m\frac{az+b}{cz+d}+n\right|^{2s}}\\
&= \sum_{n,m\in\mathbb{Z}}{}' \frac{\chi(m)(cz+d)^k\,|cz+d|^{2s}}{((ma+nc)z+(mb+nd))^k\,|(ma+nc)z+(mb+nd)|^{2s}}\\
&= (cz+d)^k\,|cz+d|^{2s}\sum_{n,n\in\mathbb{Z}}{}' \frac{\chi(m)}{((ma+nc)z+(mb+nd))^k\,|(ma+nc)z+(mb+nd)|^{2s}}.
\end{aligned} \tag{18}$$

Ahora, como $\gamma\in\Gamma_0(N)\subset \mathrm{SL}_2\mathbb{Z}$ entonces $ad-bc=1$ lo cual implica que

$$\begin{aligned}
1\equiv ad-bc\equiv ad \pmod N \quad &\Longrightarrow \quad \chi(ma+cn)=\chi(ma)=\chi(m)\chi(a)\\
&\Longrightarrow \quad \chi(m)=\chi(ma+cn)\chi(d).
\end{aligned}$$

Sustituimos esta fórmula para $\chi(m)$ en (18) y recordamos que $(m,n)\mapsto(ma+nc,mb+nd)$ permuta los elementos de $\mathbb{Z}\times\mathbb{Z}$ para concluir que:

$$\begin{aligned}
E_{k,\chi}(\gamma z,s) &= (cz+d)^k\,|cz+d|^{2s}\,\chi(d)\sum_{n,n\in\mathbb{Z}} \frac{\chi(ma+nc)}{((ma+nc)z+(mb+nd))^k\,|(ma+nc)z+(mb+nd)|^{2s}}\\
&= (cz+d)^k\,|cz+d|^{2s}\,\chi(d)\sum_{n,m\in\mathbb{Z}} \frac{\chi(m)}{(mz+n)^k\,|mz+n|^{2s}}
\end{aligned}$$

Por lo tanto

$$E_{k,\chi}(\gamma z,s)=(cz+d)^k\,|cz+d|^{2s}\,\chi(d)E_{k,\chi}(z,s). \tag{19}$$

Si hacemos $s=0$, entonces la fórmula anterior implicaría que $E_{k,\chi}(z,s)$ se transforma adecuadamente para ser una forma modular en $M_k(\Gamma(1),\chi)$. El problema es que la serie definida por $E_{k,\chi}(z,0)$ no converge si $k=1$ que es el caso que nos interesa para la prueba de la modularidad de $\bar{\rho}_{E,3}$. Entonces lo que haremos es continuar analíticamente $E_{k,\chi}(z,s)$ a $s=0$ y que la continuación sea holomorfo en $s=0$. De esta manera obtendremos una forma modular.

Este proceso es parte de un fenómeno más general; nos referimos a [**?**, §7.2] para los detalles del caso general. En la aplicación del teorema de Langlands-Tunnel, se usa una serie de Eisenstein particular de peso $k = 1$ torcida por el símbolo de Legendre módulo 3 definido por

$$\chi(m) = \left(\frac{m}{3}\right) = \begin{cases} 1 & m \equiv 1 \pmod 3 \\ -1 & m \equiv -1 \pmod 3 \\ 0 & m \equiv 0 \pmod 3 \end{cases}.$$

Observemos que $\chi(-1) = -1$ implica que

$$\frac{\chi(-m)}{(-mz+n)\left|-mz+n\right|^{2s}} = \frac{\chi(m)}{(mz-n)\left|mz-n\right|^{2s}}.$$

Como la serie $E_{1,\chi}(z,s)$ converge absolutamente cuando $\Re(s) > 1/2$, podemos usar la identidad anterior para calcular:

$$\begin{aligned}
E_{1,\chi}(z,s) &= \sum_{n,m\in\mathbb{Z}}{}' \frac{\chi(m)}{(mz+n)\left|mz+n\right|^{2s}} \\
&= \sum_{n=-\infty}^{\infty} \frac{\chi(0)}{n\left|n\right|^{2s}} + \sum_{\substack{m=-\infty \\ m\neq 0}}^{\infty} \sum_{n=-\infty}^{\infty} \frac{\chi(m)}{(mz+n)\left|mz+n\right|^{2s}} \\
&= \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{\chi(m)}{(mz+n)\left|mz+n\right|^{2s}} + \frac{\chi(-m)}{(-mz+n)\left|-mz+n\right|^{2s}} \\
&= \sum_{m=1}^{\infty} \chi(m) \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)\left|mz+n\right|^{2s}} + \frac{1}{(mz-n)\left|mz-n\right|^{2s}} \\
\therefore E_{1,\chi}(z,s) &= 2\sum_{m=1}^{\infty} \chi(m) \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)\left|mz+n\right|^{2s}} \qquad (\Re(s) > \tfrac{1}{2})
\end{aligned} \tag{20}$$

Podemos reescribir la serie $\sum (mz+n)^{-1}\left|mz+n\right|^{-2s}$ en otra serie que nos permitirá expresar $E_{1,\chi}(z,s)$ como una serie de Fourier. Primero observemos que:

$$\begin{aligned}
(mz+n)^{-1}\left|mz+n\right|^{-2s} &= (mz+n)^{-1}(mz+n)^{-s}(\overline{mz+n})^{-s} = (mz+n)^{-1-s}(m\bar{z}+n)^{-s} \\
&= m^{-1-2s}\left(z+\tfrac{n}{m}\right)^{-1-s}\left(\bar{z}+\tfrac{n}{m}\right)^{-s}.
\end{aligned}$$

Ahora fijamos un m y dividimos $\mathbb{Z}$ en las m clases laterales $0+m\mathbb{Z}, 1+m\mathbb{Z}, \ldots, (m-1)+m\mathbb{Z}$. De esta manera, si $n \in r + m\mathbb{Z}$, entonces $n = n'm + r$ para alguna $n' \in \mathbb{Z}$ y así:

$$(mz+n)^{-1}\left|mz+n\right|^{-2s} = m^{-1-2s}\left(z+\tfrac{r}{m}+n'\right)^{-1-s}\left(\bar{z}+\tfrac{r}{m}+n'\right)^{-s}$$

Por lo tanto:

$$\sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)\left|mz+n\right|^{2s}} = \sum_{r=0}^{m-1} \sum_{n'\in\mathbb{Z}} \frac{m^{1+2s}}{\left(z+\frac{r}{m}+n'\right)^{1+s}\left(\bar{z}+\frac{r}{m}+n'\right)^{s}}. \tag{21}$$

Si denotamos:

$$\phi(z;s) := \frac{1}{z^{1+s}\,\overline{z}^s} \qquad (z \in \mathbb{H})$$

podemos reescribir la ecuación (21) como

$$\sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)\left|mz+n\right|^{2s}} = m^{1+2s} \sum_{r=0}^{m-1} \sum_{n'=-\infty}^{\infty} \phi\left(z + \tfrac{r}{m} + n'; s\right)$$

para que la ecuación (20), se reduzca a:

$$E_{1,\chi}(z,s) = 2\sum_{m=1}^{\infty} \chi(m) m^{1+2s} \sum_{r=1}^{m-1} \sum_{n'=-\infty}^{\infty} \phi\left(z + \tfrac{r}{m} + n'; s\right) \qquad (\Re(s) > \tfrac{1}{2}) \tag{22}$$

Introducimos aun más notación: escribimos

$$S(z;s) := \sum_{n=-\infty}^{\infty} \phi(z+n;s). \tag{23}$$

Esta notación nos resume la ecuación (22) a:

$$E_{1,\chi}(z,s) = 2\sum_{m=1}^{\infty} \chi(m) m^{1+2s} \sum_{r=1}^{m-1} S\big(z + \tfrac{r}{m}; s\big). \qquad (\Re(s) > \tfrac{1}{2}) \tag{24}$$

Esta ecuación dice que si encontramos una serie de Fourier para $S(z;s)$, obtenemos una para $E_{1,\chi}(z,s)$ y así una posibilidad de extenderlo analíticamente a $s=0$. La ventaja de usar $S(z;s)$ es que un ejemplo de función al que le podemos asociar la fórmula de sumación de Poisson:

Teorema 38. *(Fórmula de Sumación de Poisson) Sea $f : \mathbb{R} \to \mathbb{R}$ una función asbolutamente integrable sobre $\mathbb{R}$, i.e. $\int_{\mathbb{R}} |f(x)|\, dx < \infty$, entonces:*

$$\sum_{n=-\infty}^{\infty} |\hat{f}(n)| < \infty \quad \Longrightarrow \quad \sum_{n=-\infty}^{\infty} f(x+n) = \sum_{n=-\infty}^{\infty} \hat{f}(n) e^{2\pi i n x}.$$

Proof. Véase el teorema 4.2.8 de [?] para una prueba. □

Para aplicar FSP, primero observe que

$$|\phi(x+iy;s)| = |x+iy|^{-\Re(s)-1}\, |x-iy|^{-\Re(s)} = \mathcal{O}(x^{-2\Re(s)-1}) \tag{25}$$

implica que la integral de $|\phi(x+iy;s)|$ sobre $\mathbb{R}$ es convegente cuando $\Re(s) > 0$ en otras palabras, la función $\phi_{y,s}(x) := \phi(x+iy;s)$ es absolutamente integrable sobre $\mathbb{R}$ (como función de x) y admite una transformada de Fourier:

$$\hat{\phi}_{y,s}(t) = \int_{-\infty}^{\infty} \phi_{y,s}(x) e^{-2\pi i t x} dx \qquad \big(y > 0,\ \Re(s) > 0\big).$$

Por lo tanto queremos aplicar la FSP a (23) para obtener

$$
\begin{aligned}
S(x+iy;s) &= \sum_{n=-\infty}^{\infty} \phi(x+n+iy;s) = \sum_{n=-\infty}^{\infty} \phi_{y,s}(x+n) \\
&= \sum_{n=-\infty}^{\infty} \hat{\phi}_{y,s}(n) e^{2\pi i n x} \qquad (y>0, \Re(s)>0). \qquad (26)
\end{aligned}
$$

Para poder aplicar la FSP, necesitamos probar que la serie (26) converge absolutamente. Esto se prueba calculando explícitamente la transformada de Fourier de $\phi_{y,s}$ para poder aproximalo. Para este fin tenemos el siguiente lema técnico:

Lema 39. *Para $\Re(s) > 0$ y $y > 0$ tenemos la siguiente fórmula:*

$$
\hat{\phi}_{y,s}(t) = \begin{cases} 2\pi i (2\pi t)^{2s} e^{-2\pi y t} \Gamma(s)^{-1} \Gamma(s+1)^{-1} \sigma(4\pi y t; s, s+1) & (t>0) \\ 2\pi i \Gamma(2s)(2y)^{-2s} \Gamma(s)^{-1}\Gamma(s+1)^{-1} & (t=0) \\ 2\pi i (2\pi t)^{2s} e^{-2\pi y|t|} \Gamma(s)^{-1}\Gamma(s+1)^{-1} \sigma(4\pi y\,|t|\,; s+1, s) & (t<0) \end{cases} \qquad (27)
$$

donde

$$
\sigma(z;\alpha,\beta) = \int_0^{\infty} e^{-zw}(w+1)^{\alpha-1} w^{\beta-1} dw \qquad (\Re(z), \Re(\beta) > 0, \alpha \in \mathbb{C}),
$$

es una representación integral de la función hipergeométrica confluente *(cf.* **??***)*

Proof. Viene el en apéndice **??**. □

La ventaja de escribir $\hat{\phi}$ en términos de función hipergeométrica confluente σ es que éste tiene las siguientes propiedades (probadas en el apéndice **??**, cf. teorema **??**):

Proposición 40. *La función $\sigma(z;\alpha,\beta)$ admite una continuación meromorfa a $\mathbb{H}' \times \mathbb{C} \times \mathbb{C}$ con polos cuando $\beta = 0, -1, -2, \ldots$, i.e. $\widetilde{\sigma}(z;\alpha,\beta) := \Gamma(\beta)^{-1} z^{\beta} \sigma(z;\alpha,\beta)$ es una función holomorfa y para cualquier compacto $Q \subset \mathbb{C} \times \mathbb{C}$ existen constantes $A, B > 0$ tales que*

$$
|\sigma(y;\alpha,\beta)| \leq A y^{-\Re(\beta)}(1+y^{-B}) \qquad \forall (\alpha,\beta) \in \mathbb{C} \times \mathbb{C}\,,\, y>0.
$$

y en particular

$$
\left|\widetilde{\sigma}(y;\alpha,\beta)\right| \leq A(1+y^{-B}).
$$

Nota. Este teorema nos dice que el lado derecho de (27) es una función entera de s cuando $t \neq 0$ (observa los factores $\Gamma(s)^{-1}\Gamma(s+1)^{-1}$ cancelan los polos de $\sigma(4\pi y t; s, s+1)$ y de $\sigma(4\pi\,|t|\,; s+1, s)$) y meromorfa con polos en $2s = 0, -1, -2, \ldots$ cuando $t = 0$. Por lo tanto $\hat{\phi}_{y,s}(t)$ es una función meromorfa de s. Otra consecuencia de la proposición 40 (y del lema 39) es que podemos acotar $|\hat{\phi}_{y,s}(t)|$ para probar la convergencia absoluta de la serie (26). Todo esto lo juntamos en un teorema.

Teorema 41. *Como función de s, $S(z;s)$ tiene a continuación meromorfa a $\mathbb{C}$ y cumple la fórmula:*

$$
S(z;s) = \hat{\phi}_{y,s}(0) + \sum_{\substack{n=-\infty \\ n\neq 0}}^{\infty} \hat{\phi}_{y,s}(n) e^{2\pi i n x} \qquad (z = x+iy \in \mathbb{H}). \qquad (28)
$$

Además la serie del lado derecho converge uniformemente y absolutamente sobre cualquier conjunto compacto de $\mathbb{H} \times \mathbb{C}$ y $\Gamma(2s)^{-1} S(z;s)$ es una función entera.

Proof. Primero probamos que la serie del lado derecho define una función entera de s. Para eso separamos la serie en dos y probaremos que ambas series convergen uniformemente y absolutamente sobre cualquier subconjunto compacto $Q \subset \mathbb{H}' \times \mathbb{C}$.

Usamos el lema 39 y la cota de la proposición 40 para calcular la serie

$$\begin{aligned}
\sum_{n=1}^{\infty} \left| \hat{\phi}_{y,s}(n) e^{2\pi i n x} \right| &= \sum_{n=1}^{\infty} \left| \hat{\phi}_{y,s}(n) \right| \\
&= \sum_{n=1}^{\infty} 2\pi (2\pi n)^{2\Re(s)} e^{-2\pi y n} \left| \Gamma(s)^{-1} \right| \left| \Gamma(s+1)^{-1} \sigma(4\pi y n; s, s+1) \right| \\
(\exists A, B > 0) \qquad &\leq (2\pi)^{2\Re(s)+1} \left| \Gamma(s)^{-1} \right| A \sum_{n=1}^{\infty} n^{2\Re(s)} e^{-2\pi y n} (4\pi y n)^{-\Re(s)-1} (1 + y^{-B}) \\
&\leq \frac{A}{2} \pi^{\Re(s)} \left| \Gamma(s)^{-1} \right| y^{-\Re(s)-1} (1 + y^{-B}) \sum_{n=1}^{\infty} n^{\Re(s)-1} e^{-2\pi y n}.
\end{aligned}$$

Por lo tanto, si $(z, s) \in Q \subset \mathbb{H} \times \mathbb{C}$ con Q compacto, entonces existen constantes positivas C_1 y C_2 tales que $0 < C_1 < y = \Im(z)$ y $\Re(s) < C_2$. Además, como $|\Gamma(s)^{-1}|$ es una función continua de (z, s), alcanza su máximo, por ejemplo C_3, sobre Q y así podemos acotar la serie anterior por:

$$\sum_{n=1}^{\infty} \left| \hat{\phi}_{y,s}(n) e^{2\pi i n x} \right| \leq \underbrace{\frac{A}{2} \pi^{C_2} C_3 C_1^{-C_2-1} (1 + C_1^{-B})}_{C} \sum_{n=1}^{\infty} n^{C_2-1} e^{-2\pi C_1 n}$$

$$\therefore \quad \sum_{n=1}^{\infty} \left| \hat{\phi}_{y,s}(n) e^{2\pi i n x} \right| \leq C \sum_{n=1}^{\infty} n^{C_2-1} e^{-2\pi C_1 n} < \infty,$$

Así la serie $\sum_{n>0} \hat{\phi}_{y,s}(n) e^{2\pi i n x}$ converge absolutamente y uniformemente sobre cualquier compacto $Q \subset \mathbb{H} \times \mathbb{C}$. De manera análoga la serie $\sum_{n<0} \hat{\phi}_{y,s}(n) e^{2\pi i n z}$ también converge absolutamente y uniformemente. Esto implica que podemos aplicar la FSP a S para conluir la igualdad

$$S(z; s) = \sum_{n=-\infty}^{\infty} \hat{\phi}_{y,s}(n) e^{2\pi i n x} = \hat{\phi}_{y,s}(0) + \sum_{\substack{n=-\infty \\ n \neq 0}}^{\infty} \hat{\phi}_{y,s}(n) e^{2\pi i n x};$$

observa que

$$\sum_{\substack{n=-\infty \\ n \neq 0}}^{\infty} \hat{\phi}_{y,s}(n) e^{2\pi i n x} \qquad (z = x + iy \in \mathbb{H})$$

define una función holomorfa sobre $\mathbb{H} \times \mathbb{C}$. Por último, el lema 39 dice que el sumando $\hat{\phi}_{y,s}(0)$ es una función meromorfa sobre $\mathbb{H} \times \mathbb{C}$ con polos cuando $2s = 0, -1, -2, \ldots$. Entonces $\Gamma(2s)^{-1} \hat{\phi}_{y,s}(0)$ es una función entera. Por lo tanto el lado derecho de (28) es una función meromorfa sobre $\mathbb{H} \times \mathbb{C}$ y da la continuación meromorfa de $S(z; s)$ a $\mathbb{H} \times \mathbb{C}$. $\square$

Corolario 42. *La serie de Eisenstein $E_{1,\chi}(z; s)$ admite una continuación analítica a $s = 0$ y por lo tanto $E_{1,\chi}(z; 0)$ es una forma $(\Gamma(1), 1)-$modular.*

Proof. Recordemos la fórmula (24) dice que cuando $\Re(s) > \frac{1}{2}$,

$$E_{1,\chi}(z,s) = 2\sum_{m=1}^{\infty} \chi(m) m^{1+2s} \sum_{r=1}^{m-1} S\left(z + \tfrac{r}{m}; s\right).$$

Si sustituimos nuestra fórmula para $S(z;s)$ del teorema 41 obtenemos:

$$E_{1,\chi}(z,s) = 2\sum_{m=1}^{\infty} \chi(m) m^{1+2s} \sum_{r=1}^{m-1} \left(\hat{\phi}_{y,s}(0) + \sum_{\substack{n=-\infty \\ n\neq 0}}^{\infty} \hat{\phi}_{y,s}(n) e^{2\pi i n (x + \frac{r}{m})} \right).$$

En particular ambos lados de igualdad son funciones meromorfas que coinciden sobre un abierto del plano complejo, por lo tanto coinciden en todo su dominio de definición.

□