Universitat de Barcelona
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

FORMES I SÍMBOLS MODULARS

Autor: Gonzalo Revilla Mut

Director: Dr. Xavier Guitart Morales
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 20 de juny de 2021

"There are five fundamental operations in mathematics: addition, subtraction, multiplication, division, and modular forms."

Martin Eichler (1912-1992)

Abstract

In this Bachelor's Final Project we present simply and understandably the basic properties of modular forms for different weights and levels. Furthermore, we define and treat Hecke operators, the Petersson inner product and the Atkin–Lehner theory. In the last section, we introduce modular symbols and we study their relation with modular forms.

Resum

En aquest Treball Final de Grau presentem d'una forma senzilla i accessible les propietats bàsiques de les formes modulars per a diferents pesos i nivells. A més, definim i tractem els anomenats operadors de Hecke, el producte escalar de Petersson i la teoria d'Atkin-Lehner. En l'última secció, introduïm els símbols modulars i estudiem la seva relació amb les formes modulars.

2010 Mathematics Subject Classification: 11F11, 11F67, 11F25

Agraïments

En primer lloc a tota la meva família, especialment als meus pares pel suport constant que sempre m'han donat.

A totes aquelles persones que han estat al meu costat i m'han acompanyat durant els quatre anys del grau, tant a Barcelona, com a Tarragona i Lausanne.

No em puc oblidar de les treballadores de la biblioteca de la facultat. Gràcies Montserrat, Elena i Marta.

Finalment vull agrair al meu tutor Xevi per haver-me tutoritzat el treball. Sempre ha mostrat una gran disposició a guiar-me, orientar-me, ensenyar-me i corregir-me en tots els moments que ha fet menester. Gràcies per la teva paciència i dedicació. Et desitjo molta sort en la teva tasca com investigador.

Índex

1 Introducció

Aquest treball introdueix la teoria clàssica de formes modulars, així com presenta els símbols modulars. Dos camps que, tal com veurem, estan relacionats entre si.

La teoria de formes modulars, desenvolupada a partir del segle XIX, forma part d'una de les branques més importants de la teoria de nombres. Són diversos els camps en què aquesta teoria es veu involucrada: superfícies de Riemann, corbes el·líptiques, geometria, teoria de la representació, etc. A més, el seu estudi ha permès establir relacions entre diferents disciplines matemàtiques. Un dels resultats més coneguts en el camp és el Teorema de Modularitat, sent la peça clau de la demostració del famós Últim Teorema de Fermat.

Una forma modular és una funció holomorfa definida en el semiplà superior que es transforma d'una manera específica sota l'acció d'un grup de matrius, i que satisfà certes propietats de creixement. Els espais de formes modulars tenen estructura d'espai vectorial complex de dimensió finita, a més, les seves dimensions es poden calcular explícitament. El matemàtic alemany Erich Hecke, ja en el segle XX, es va submergir en l'estudi de les formes modulars i va construir uns endomorfismes que actuen en aquests espais vectorials, els anomenats operadors de Hecke. Un dels resultats més importants del treball ens afirma que l'espai de formes modulars té una base formada per vectors propis d'aquests endomorfismes. Per a provar-ho, necessitem dotar l'espai amb un producte escalar, el producte escalar de Petersson.

Degut a la seva definició, les formes modulars són objectes abstractes i moltes vegades difícils de construir, sent els símbols modulars una eina eficaç per poder-les calcular. La noció de símbol modular va ser introduïda per Bryan John Birch mentre estudiava la conjectura de Birch i Swinnerton-Dyer (un dels problemes del mil·lenni) i ens subministra una eina teòrica poderosa per tractar espais de formes modulars. Yuri Manin i Barry Mazur, l'any 1972, de forma independent, també van definir el concepte. Ens els podem imaginar com un conjunt formal de símbols que satisfan certes relacions algebraiques, i en els que també hi actuen els operadors de Hecke. Una de les principals característiques és que aquests espais són computables, és a dir, mitjançant algorismes programables en ordinador els podem calcular. A més, hi ha una relació entre formes i símbols modulars que ens proporciona mètodes per obtenir bases d'espais de formes modulars. Autors com J. E. Cremona han utilitzat aquesta teoria per treballar amb corbes el·líptiques.

En el present treball ens submergim en aquest camp, enunciant, i (no sempre) demostrant els teoremes més importants d'aquesta branca de les matemàtiques. Finalment, com a part més pràctica, descrivim com utilitzar el programari SAGE per calcular (mitjançant símbols modulars) espais de formes modulars.

2 Formes Modulars per a $\mathrm{SL}_2(\mathbb{Z})$

2.1 El Grup Modular

Comencem per donar una sèrie de definicions. La primera de totes és el *semiplà superior* $\mathbb{H}$:

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

on $\Im(z)$ denota la part imaginària de $z \in \mathbb{C}$.
Seguidament, definim el *grup modular* $\mathrm{SL}_2(\mathbb{Z})$:

$$\mathrm{SL}_2(\mathbb{Z}) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z}) \mid ad - bc = 1\},$$

així com el *grup general lineal* $\mathrm{GL}_2(\mathbb{R})$:

$$\mathrm{GL}_2(\mathbb{R}) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{R}) \mid ad - bc \neq 0\}.$$

Per a $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ i $z \in \mathbb{H}$ definim la *transformació lineal fraccionària*:

$$\gamma z := \frac{az + b}{cz + d} .$$

La següent proposició ens dona una forma curiosa de trobar elements del grup modular:

Lema 2.1. Donats $a, b \in \mathbb{Z}$ coprimers, existeix almenys un element a $\mathrm{SL}_2(\mathbb{Z})$ que es pot expressar de la forma $\left(\begin{smallmatrix} a & * \\ b & * \end{smallmatrix}\right)$.
Demostració: Resolem $ay - bx = 1$ usant l'Algorisme d'Euclides per a $x, y \in \mathbb{Z}$, aleshores $\left(\begin{smallmatrix} a & x \\ b & y \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. □

La transformació lineal fraccionària defineix una acció de $\mathrm{SL}_2(\mathbb{Z})$ en $\mathbb{H}$. Per a veure-ho, necessitem un resultat previ.

Lema 2.2. Siguin $\gamma \in \mathrm{GL}_2(\mathbb{R})$ i $z \in \mathbb{C} - \mathbb{R}$. Aleshores $\Im(\gamma z) = \frac{\det(\gamma)\Im(z)}{|cz+d|^2}$.
Demostració: Sigui $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$. Tenim:

$$\Im(\gamma z) = \Im\left(\frac{az + b}{cz + d}\right) = \Im\left(\frac{(az + b)(c\bar{z} + d)}{|cz + d|^2}\right) = \frac{\Im(ac|z|^2 + bd + adz + bc\bar{z})}{|cz + d|^2} = \frac{\det(\gamma)\Im(z)}{|cz + d|^2} .$$

□

Proposició 2.3. L'aplicació

$$\begin{array}{rcl} \mathrm{SL}_2(\mathbb{Z}) \times \mathbb{H} & \longrightarrow & \mathbb{H} \\ (\gamma, z) & \longmapsto & \gamma z \end{array}$$

defineix una acció de grup (per l'esquerra) al conjunt $\mathbb{H}$ [2].
Demostració: Deduïm del Lema 2.2 que l'aplicació està ben definida. A més, per a qualsevol $z \in \mathbb{H}$, $\mathrm{I}_2 z = z$, on I_2 denota la matriu identitat $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Finalment, donats $\gamma_1 = \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right), \gamma_2 = \left(\begin{smallmatrix} a_2 & b_2 \\ c_2 & d_2 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ i $z \in \mathbb{H}$:

$$\gamma_1(\gamma_2 z) = \gamma_1\left(\frac{a_2 z + b_2}{c_2 z + d_2}\right) = \frac{a_1\left(\frac{a_2 z + b_2}{c_2 z + d_2}\right) + b_1}{c_1\left(\frac{a_2 z + b_2}{c_2 z + d_2}\right) + d_1} = \frac{a_1(a_2 z + b_2) + b_1(c_2 z + d_2)}{c_1(a_2 z + b_2) + d_1(c_2 z + d_2)} = (\gamma_1\gamma_2)z .$$

□

[2] La proposició continua sent certa canviant $\mathrm{SL}_2(\mathbb{Z})$ per $\mathrm{GL}_2^+(\mathbb{R}) = \{\gamma \in \mathrm{GL}_2(\mathbb{R}) \mid \det(\gamma) > 0\}$.

2.2 Domini Fonamental per a $\mathrm{SL}_2(\mathbb{Z})$

A continuació, definim l'anomenat *domini fonamental per l'acció de* $\mathrm{SL}_2(\mathbb{Z})$ i el denotem per $\mathcal{F}$.

$$\mathcal{F} := \{z \in \mathbb{H} \ : \ |\Re(z)| \leq \frac{1}{2}, |z| \geq 1\},$$

on $\Re(z)$ representa la part real de $z \in \mathbb{C}$.

Cada punt de $\mathbb{H}$ té un punt de la seva $\mathrm{SL}_2(\mathbb{Z})$-òrbita en $\mathcal{F}$, els únics punts del domini fonamental diferents, que pertanyen a la mateixa $\mathrm{SL}_2(\mathbb{Z})$-òrbita es troben a la frontera de $\mathcal{F}$. Les següents proposicions expliquen de forma rigorosa aquest concepte.

Proposició 2.4. Sigui $\mathcal{F}$ la regió definida anteriorment, i siguin $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ i $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ elements de $\mathrm{SL}_2(\mathbb{Z})$, aleshores:

1. Sota l'acció de l'espai generat per S i T: $\langle S, T\rangle$, cada punt de $\mathbb{H}$ és equivalent a un punt de $\mathcal{F}$.
2. Si $z_1 \neq z_2$ es troben a la mateixa $\langle S, T\rangle$-òrbita, aleshores o bé $z_2 = z_1 \pm 1$ (és a dir, pertanyen a la recta vertical de la frontera del domini), o bé $z_2 = \frac{-1}{z_1}$ (és a dir, pertanyen a la frontera del cercle unitat).
3. Sigui $z \in \mathcal{F}$, $\mathrm{Stab}_{\langle S,T\rangle}(z) = \{\gamma \in \langle S, T\rangle \mid \gamma z = z\}$ i $\rho = e^{\frac{2\pi i}{3}}$. Aleshores tenim:

$$\mathrm{Stab}_{\langle S,T\rangle}(z) = \begin{cases} \text{cíclic d'ordre 6 generat per } \mathrm{ST} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) & \text{si } z = \rho \\ \text{cíclic d'ordre 6 generat per } \mathrm{TS} = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right) & \text{si } z = -\bar{\rho} \\ \text{cíclic d'ordre 4 generat per } \mathrm{S} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) & \text{si } z = i \\ \text{cíclic d'ordre 2 generat per } -\mathrm{I}_2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) & \text{altrament} \end{cases}$$

4. $\mathrm{SL}_2(\mathbb{Z})$=$\langle S, T\rangle$.

Demostració: (*1*). Fixem $z \in \mathbb{H}$.
Donat que només hi ha un nombre finit de $(c, z) \in \mathbb{Z}^2$ tals que $|cz+d| < 1$, podem garantir que existeix alguna $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \langle S, T\rangle$ tal que

$$|cz + d| \leq |c'z + d'| \ \text{ per a tot } \gamma' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in \langle S, T\rangle.$$

En el cas que el nombre de $(c, z) \in \mathbb{Z}^2$ tals que $|cz + d| < 1$ sigui zero, prenem $\gamma = \mathrm{I}_2$.
Utilitzant el Lema 2.2, obtenim:

$$\Im(\gamma z) \geq \Im(\gamma' z) \ \text{ per a tot } \gamma' \in \langle S, T\rangle. \tag{2.1}$$

Tenint en compte que $T^{\pm n}\gamma z = \left(\begin{smallmatrix} 1 & \pm n \\ 0 & 1 \end{smallmatrix}\right)\gamma z = \gamma z \pm n$ per a tot $n \in \mathbb{Z}$, podem suposar que γ compleix:

$$\frac{-1}{2} \leq \Re(\gamma z) \leq \frac{1}{2} \ .$$

En particular $T^{\pm n}\gamma = \left(\begin{smallmatrix} a\pm cn & b\pm dn \\ c & d \end{smallmatrix}\right)$, per tant, multiplicar per l'esquerra per $T^{\pm n}$ no afecta a (2.1). Finalment,

$$\Im(\gamma z) \geq \Im\left(S\gamma z\right) = \frac{\Im(\gamma z)}{|\gamma z|^2} \ .$$

Per tant, $|\gamma z| \geq 1$, així que $\gamma z \in \mathcal{F}$, amb $\gamma \in \langle S, T \rangle$.
Per demostrar (*2*) i (*3*): Siguin $z_1, z_2 \in \mathcal{F}$ diferents, pertanyent a la mateixa $\langle S, T \rangle$-òrbita. Sense pèrdua de generalitat, podem suposar que $\Im(z_2) \geq \Im(z_1)$. Sigui també $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \langle S, T \rangle$ tal que $z_2 = \gamma z_1$. Utilitzant el Lema 2.2, es compleix:

$$\Im(z_2) = \frac{\Im(z_1)}{|cz_1 + d|^2} \leq \frac{\Im(z_2)}{|cz_1 + d|^2} ,$$

per tant $|cz_1 + d| \leq 1$. A més, si $z_1 = x_1 + iy_1$, pel *Teorema de Pitàgores*, tenim:

$$|cz_1 + d|^2 = |cx_1 + d|^2 + |cy_1|^2,$$

com $z_1 \in \mathcal{F}$, tenim $y_1 > \frac{1}{2}$, per tant $|cz_1 + d| \leq 1$ només es dona si $|c| \leq 1$.

- **Cas $\boldsymbol{c = 0}$:** L'equació $ad - bc = 1$ implica $a = d = \pm 1$, per tant $z_2 = z_1 \pm b$. Com $\Re(z_1)$ i $\Re(z_2)$ pertanyen a $\left[\frac{-1}{2}, \frac{1}{2}\right]$, l'única possibilitat és $z_2 = z_1 + 1$ amb $\gamma = \pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = \pm T$, o bé $z_2 = z_1 - 1$ amb $\gamma = \pm \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) = \pm T^{-1}$.
- **Cas $\boldsymbol{c = 1}$:** Tenim:
$$1 \geq |cz_1 + d| = |z_1 + d|.$$
Com $z_1 \in \mathcal{F}$, només és possible si:
  - **Cas $\boldsymbol{|z_1| = 1}$ i $\boldsymbol{d = 0}$:** L'equació $ad - bc = 1$ implica $b = -1$ i $z_2 = \frac{az_1 - 1}{z_1} = a - \frac{1}{z_1}$, amb $\gamma = \left(\begin{smallmatrix} a & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Això només és possible si: $a = 0$ ($\gamma = S$ i $z_2 = \frac{1}{z_1}$), si $z_1 = \rho$ i $a = -1$ ($\gamma = T^{-1}S$ i $z_2 = z_1$), o si $z_1 = \rho + 1$ i $a = 1$ ($\gamma = TS$ i $z_2 = z_1$).
  - **Cas $\boldsymbol{z_1 = \rho}$ i $\boldsymbol{d = 1}$:** L'equació $ad - bc = 1$ implica $a - b = 1$. Com que $\frac{a\rho + b}{\rho + 1}$ ha de pertànyer a $\mathcal{F}$, ens limitem als casos $a = 1$ i $b = 0$ (amb $z_2 = \rho + 1$ i $\gamma = TST$) o a $a = 0$ i $b = -1$ (amb $z_2 = \rho$ i $\gamma = ST$).
  - **Cas $\boldsymbol{z_1 = \rho + 1}$ i $\boldsymbol{d = -1}$:** Anàlogament, l'equació $ad - bc = 1$ implica $a + b = -1$. Com que $\frac{a\rho + b}{\rho - 1}$ ha de pertànyer a $\mathcal{F}$, ens limitem als casos $a = -1$ i $b = 0$ (amb $z_2 = \rho$ i $\gamma = T^{-1}ST^{-1}$) o a $a = 0$ i $b = -1$ (amb $z_2 = \rho + 1$ i $\gamma = ST^{-1}$).
- **Cas $\boldsymbol{c = -1}$:** Es pot veure trivialment que $-\gamma$ actua sobre $\mathbb{H}$ de la mateixa manera que ho fa γ. Per tant aquest cas és anàleg a l'anterior.

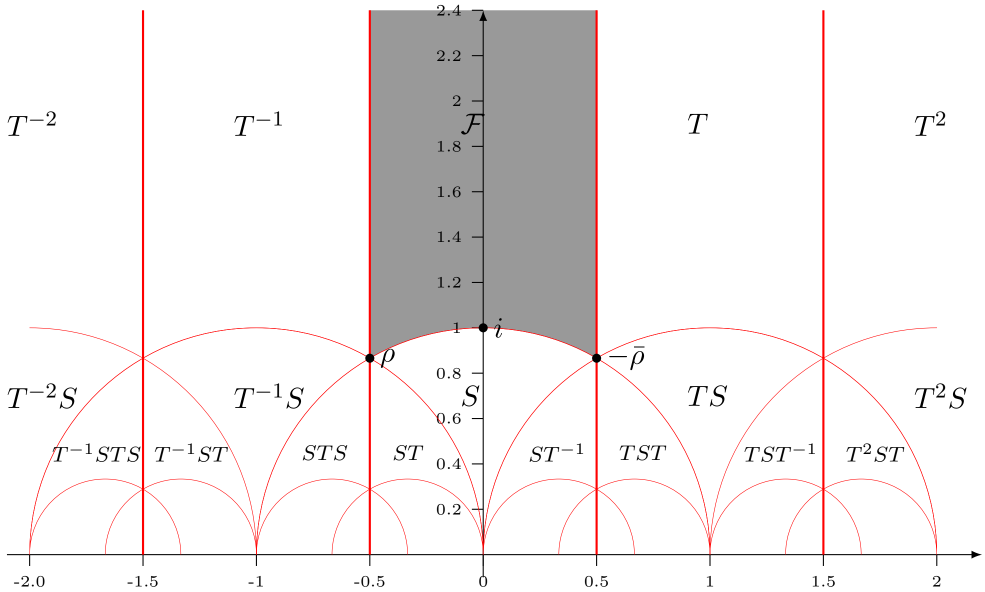
Podem resumir els tres casos en la taula:

γ	z_1	$z_2 = \gamma z_1$	punts fixos
$\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	tot $z \in \mathcal{F}$	z	tot $z \in \mathcal{F}$
$\pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$	$\Re(z) = \frac{-1}{2}$	$z + 1$	cap
$\pm \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$	$\Re(z) = \frac{1}{2}$	$z - 1$	cap
$\pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$	$\|z\| = 1$	$\frac{1}{z}$	i
$\pm \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$	ρ	ρ	ρ
$\pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$	ρ	ρ	ρ
$\pm \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$	$\rho + 1$	$\rho + 1$	$\rho + 1$
$\pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$	$\rho + 1$	$\rho + 1$	$\rho + 1$

Veient la taula, queden provats els apartats *2* i *3*.
Finalment, per a provar (*4*): Sigui z un element de l'interior de $\mathcal{F}$ i sigui $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ una matriu qualsevol. Volem veure que $\gamma \in \langle S, T \rangle$. Utilitzant (*1*), exiteix $\gamma' \in \langle S, T \rangle$ tal que $\gamma'(\gamma z) \in \mathcal{F}$. Tant z com $\gamma'(\gamma z)$ estan a $\mathcal{F}$, i com z no pertany a la frontera, per (*2*) i (*3*), $\gamma' \gamma = \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Com $S^2 = -\mathrm{I}_2$, concloem que $\gamma = \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \gamma'^{-1} \in \langle S, T \rangle$.

$\square$

Per acabar la secció, en la següent figura podem veure una divisió de $\mathbb{H}$ en diverses seccions corresponents a $\gamma(\mathcal{F})$, on γ pren diversos valors dins de $\mathrm{SL}_2(\mathbb{Z})$. Les diferents parts en què es divideix $\mathbb{H}$ s'anomenen *triangles ideals*, ja que aquestes tenen tres costats i dos punts a $\mathbb{H}$, i un darrer punt que és un nombre racional, o bé $i\infty$ (si la secció és $T^n(\mathcal{F})$ per a un cert $n \in \mathbb{Z}$).



2.3 Formes Modulars per a $\mathrm{SL}_2(\mathbb{Z})$

Definició 2.5. Sigui f una funció meromorfa en $\mathbb{H}$. Diem que f és *feblement modular de pes* $k \in \mathbb{Z}$ si satisfà:

$$f(\gamma z) = (cz + d)^k f(z) \quad \text{per a tot } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \text{ i } z \in \mathbb{Z}. \tag{2.2}$$

Seguidament introduïm una acció del grup $\mathrm{SL}_2(\mathbb{Z})$ al conjunt de funcions meromorfes a $\mathbb{H}$. Denotem per $\mathcal{M}(\mathbb{H})$ a aquest conjunt.

Proposició 2.6. Sigui $k \in \mathbb{Z}$. L'aplicació

$$\begin{array}{rcl} \mathcal{M}(\mathbb{H}) \times \mathrm{GL}_2^+(\mathbb{Q}) & \longrightarrow & \mathcal{M}(\mathbb{H}) \\ (f, \gamma) & \longmapsto & f|_k\gamma \ , \end{array}$$

on per a $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$,

$$(f|_k\gamma)(z) := \det(\gamma)^{k-1}(cz + d)^{-k} f(\gamma z), \tag{2.3}$$

defineix una acció de grup (per la dreta) al conjunt $\mathcal{M}(\mathbb{H})$. Anomenem a aquesta acció *operador barra de pes* k [3].

Demostració: Clarament $(f|_k\gamma) \in \mathcal{M}(\mathbb{H})$. A més, per a qualsevol $f \in \mathcal{M}(\mathbb{H})$, $(f|_k\mathrm{I}_2) = f$. Finalment, donats $\gamma_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \gamma_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$ i $f \in \mathcal{M}(\mathbb{H})$:

$$((f|_k\gamma_1)|_k\gamma_2)(z) = \det(\gamma_1\gamma_2)^{k-1}(c_2 z + d_2)^{-k}(c_1\gamma_2 z + d_1)^{-k} f(\gamma_1\gamma_2 z) = (f|_k\gamma_1\gamma_2)(z).$$

□

[3] La proposició continua sent certa substituint $\mathrm{GL}_2^+(\mathbb{Q})$ per $\mathrm{GL}_2^+(\mathbb{R})$.

Per tant, donada $f \in \mathcal{M}(\mathbb{H})$ dir que és feblement modular de pes k, és equivalent a dir que f és invariant sota l'operador barra de pes k, és a dir, $f|_k\gamma = f$, per a tot $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Les següents proposicions ens permeten simplificar (2.2) per no haver de comprovar la fórmula un nombre infinit de vegades. Comprovant la condició en S i T, és suficient per garantir que es compleix en totes les matrius de $\mathrm{SL}_2(\mathbb{Z})$.

Lema 2.7. Si una funció $f \in \mathcal{M}(\mathbb{H})$ satisfà (2.2) per γ_1 i γ_2 de $\mathrm{SL}_2(\mathbb{Z})$, aleshores també ho satisfan $\gamma_1\gamma_2$ i γ_1^{-1}.
Demostració: Utilitzant que $f|_k\gamma_1 = f$, que $f|_k\gamma_2 = f$ i la Proposició 2.6 obtenim la igualtat: $f|_k\gamma_1\gamma_2 = (f|_k\gamma_1)|_k\gamma_2 = f|_k\gamma_2 = f$, per tant $\gamma_1\gamma_2$ satisfà (2.2).
Sigui $\gamma_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$, aleshores $\gamma_1^{-1} = \begin{pmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{pmatrix}$. A més, $f(\gamma_1 z) = (c_1 z + d_1)^k f(z)$, per a tot $z \in \mathbb{H}$. Substituint a $\gamma_1^{-1}z$, obtenim: $f(\gamma_1^{-1}z) = \frac{f(z)}{(c_1(\gamma_1^{-1}z)+d_1)^k} = (-c_1 z + a_1)^k f(z)$. Per tant, γ_1^{-1} satisfà (2.2) com volíem. $\square$

Corol·lari 2.8. Sigui $f \in \mathcal{M}(\mathbb{H})$, per a provar que és feblement modular de pes k és suficient comprovar les condicions per a S i T.
Demostració: Pel Lema 2.7, el conjunt de totes les matrius de $\mathrm{SL}_2(\mathbb{Z})$ per a les que f satisfà (2.2) és un subgrup de $\mathrm{SL}_2(\mathbb{Z})$. Com per la Proposició 2.4, S i T generen el grup modular, és suficient comprovar les condicions per aquestes dues matrius. $\square$

En el següent exemple, veiem que si k és imparell, aleshores l'única forma feblement modular de pes k és la funció 0. La noció de forma feblement modular es pot estendre a certs subgrups del grup modular (aquest concepte el tractarem en el quart capítol del treball), en aquests casos, poden existir formes feblement modulars de pes imparell no trivials.

Exemple 2.9. Si f és una forma feblement modular, considerant $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, (2.2) s'interpreta com; per a tot $z \in \mathbb{H}$ $f(z) = (-1)^k f(z)$. És a dir, l'única forma feblement modular de pes imparell és la funció 0.

Exemple 2.10. Si f és una forma feblement modular, considerant la matriu T, (2.2) s'interpreta com, per a tot $z \in \mathbb{H}$ $f(z+1) = f(z)$. Per tant, totes les formes feblement modulars de pes k són periòdiques de període 1.

Considerem la següent funció:

$$\begin{aligned} q : \mathbb{H} &\longrightarrow \mathbb{C} \\ z &\longmapsto e^{2\pi i z}. \end{aligned}$$

Donada f feblement modular, podem observar que tant f com q són periòdiques de període 1. Aquest fet ens permet escriure formes modulars com una sèrie de potències, tal com veurem tot seguit.

Expressant $z = x + iy$, tenim $q(z) = e^{-2\pi y} e^{2\pi i x}$, per tant $|q(z)| = e^{-2\pi y} \in (0,1)$, ja que $y > 0$. Concloem que l'espai d'arribada de q és $D^* = \{q \in \mathbb{C} \mid 0 < |q| < 1\}$. A més, l'inversa d'un element de D^* és un conjunt discret de valors en $\mathbb{H}$.
Transformem la funció $f : \mathbb{H} \to \mathbb{C}$, en $\tilde{f} : D^* \to \mathbb{C}$, definint $\tilde{f}(q) = f(z)$ per a algun $z \in \mathbb{H}$ complint $e^{2\pi i z} = q$. Aquesta funció està ben definida degut a que si z' també ho compleix, aleshores $z = z' + n$ per un cert $n \in \mathbb{Z}$, per tant $f(z') = f(z+n) = f(z)$. Durant tot el document, fem un abús de notació i escrivim f també referint-nos a $\tilde{f}$.

Definició 2.11. Sigui $f \in \mathcal{M}(\mathbb{H})$ feblement modular de pes k. Diem que és *meromorfa en l'infinit* si $\tilde{f}$ admet una continuació meromorfa en el disc unitat,

$$\mathbb{D} = \{q \in \mathbb{C} \mid |q| < 1\}.$$

Equivalentment, si existeix un $M \in \mathbb{Z}$ tal que podem expressar $\tilde{f}$ com una sèrie de Laurent centrada en el 0, convergent en un entorn $\{q \in \mathbb{C} \mid 0 < |q| < \varepsilon\}$ per un cert $\varepsilon > 0$,

$$\tilde{f}(q) = \sum_{n=-M}^{\infty} a_n q^n,$$

on $a_n \in \mathbb{C}$.

El fet que $\lim_{z \to i\infty} f(z) = \lim_{q \to 0} \tilde{f}(z)$ motiva la següent definició.

Definició 2.12. Diem que f és *holomorfa en l'infinit* si aquesta continuació meromorfa de $\tilde{f}$ és holomorfa en $q = 0$. Equivalentment, per a tot $n < 0$, $a_n = 0$. En aquest cas, definim el *valor de f a l'infinit* com

$$f(\infty) := \tilde{f}(0) = a_0.$$

Definició 2.13. Sigui $k \in \mathbb{Z}$. Una *forma modular de pes k per a* $\mathrm{SL}_2(\mathbb{Z})$ és una funció holomorfa $f : \mathbb{H} \to \mathbb{C}$ que és feblement modular de pes k i holomorfa en l'infinit. Anomenem *forma cuspidal de pes k per a* $\mathrm{SL}_2(\mathbb{Z})$ a una forma modular f de pes k que satisfà $f(\infty) = 0$.

Intuïtivament, ens podem imaginar que una forma feblement modular f és holomorfa en l'infinit com que $\lim_{z \to i\infty} f(z)$ està acotat. En particular, una forma cuspidal és una forma feblement modular que compleix $\lim_{z \to i\infty} f(z) = 0$.

Definició 2.14. Anomenem *q-expansió d'una forma modular f* a la sèrie $\sum_{n \geq 0} a_n q^n$ que compleix $f(z) = \sum_{n \geq 0} a_n e^{2\pi i n z}$. Els termes a_n s'anomenen els *coeficients de Fourier de f*.

2.4 Sèries d'Eisenstein

El primer exemple de formes modulars no-constants ni trivials per $\mathrm{SL}_2(\mathbb{Z})$ són les anomenades sèries d'Eisenstein.
Sigui $k \in \mathbb{Z}$ parell complint $k \geq 4$. Definim la *sèrie d'Eisenstein de pes k per* $\mathrm{SL}_2(\mathbb{Z})$ com:

$$\begin{array}{rcl} G_k : \mathbb{H} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & G_k(z) := \displaystyle\sum_{\substack{(m,n) \in \mathbb{Z}^2 \\ (m,n) \neq (0,0)}} \frac{1}{(mz+n)^k}. \end{array}$$

Lema 2.15. G_k convergeix absolutament i uniformement en subconjunts de $\mathbb{H}$ de la forma

$$R_{r,s} = \{x + iy \mid |x| \leq r, y \geq s\}.$$

Demostració: Donarem la demostració de ([BD16], §2.2).
Sigui $z = x + iy \in R_{r,s}$. Utilitzant de nou el *Teorema de Pitàgores*, tenim

$$|mz+n|^2 = (mx+n)^2 + m^2y^2 \geq (mx+n)^2 + m^2s^2.$$

Per a m i n fixats, distinguim dos casos: $|n| \leq 2r|m|$ i $|n| \geq 2r|m|$. En el primer, tenim

$$|mz+n|^2 \geq m^2s^2 \geq \frac{s^2m^2}{2} + \frac{s^2n^2}{2(2r)^2} \geq \min\left\{\frac{s^2}{2}, \frac{s^2}{8r^2}\right\}(m^2+n^2).$$

Mentre que, en el segon, utilitzant la desigualtat triangular inversa (si z i $w \in \mathbb{C}$, aleshores $|\,|z| - |w|\,| \leq |z+w|$),

$$|mz+n|^2 \geq (|mx| - |n|)^2 + m^2s^2 \geq \left(\frac{|n|}{2}\right)^2 + m^2s^2 \geq \min\left\{\frac{1}{4}, s^2\right\}(m^2+n^2).$$

Definint

$$c^2 = \min\left\{\frac{1}{4}, s^2, \frac{s^2}{2}, \frac{s^2}{8r^2}\right\},$$

i combinant els dos casos, obtenim

$$|mz+n| \geq c(m^2+n^2)^{\frac{1}{2}} \quad \text{per a tot } m,n \in \mathbb{Z} \ \text{ i } z \in R_{r,s}.$$

Aplicant la definició de G_k, tenim

$$|G_k(z)| \leq \frac{1}{c^k} \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(m^2+n^2)^{\frac{k}{2}}} \quad \text{per a tot } z \in R_{r,s}.$$

A continuació, reordenem el sumatori. Per a cada $j \in \mathbb{Z}$ amb $j \geq 1$ hi ha exactament $8j$ parelles (m,n) complint $j = \max\{|m|,|n|\}$. A més, cadascuna d'aquestes compleix $j^2 \leq m^2+n^2 \leq 2j^2$. Obtenim

$$|G_k(z)| \leq \frac{1}{c^k}\sum_{j\geq 1}\frac{8j}{j^k} = \frac{8}{c^k}\sum_{j\geq 1}\frac{1}{j^{k-1}},$$

utilitzant que $k \geq 4$, la sèrie és finita i independent de $z \in R_{r,s}$. □

Lema 2.16. Sigui $k \in \mathbb{Z}$ parell complint $k \geq 4$. Aleshores G_k és una forma modular de pes k per a $\mathrm{SL}_2(\mathbb{Z})$.
Demostració: Pel Lema 2.15, $G_k(z)$ convergeix a una funció holomorfa en $\mathbb{H}$ [4]. Per a veure que és feblement modular, usant el Corol·lari 2.8, veiem que només hem de comprovar $G_k(z+1) = G_k(z)$ i $G_k(\frac{-1}{z}) = z^kG_k(z)$.
Com a conseqüència de la convergència absoluta de $G_k(z)$, podem reordenar l'ordre de sumació dels termes com vulguem. Comprovem la primera igualtat:

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

[4] Un teorema d'anàlisis complexa ens assegura que donada una seqüència $f_n : \mathbb{H} \to \mathbb{C}$ de funcions holomorfes que convergeixen uniformement sobre compactes de $\mathbb{H}$ a $f : \mathbb{H} \to \mathbb{C}$, aleshores f és holomorfa.

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

on hem reordenat els termes observant que hi ha una relació 1-1 entre (m,n) i $(m,m+n)$. Per a la segona condició, obtenim:

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

on, en aquest cas, la relació 1-1 és entre (m,n) i $(n,-m)$.
Per a veure que $G_k(z)$ és una forma modular per a $\mathrm{SL}_2(\mathbb{Z})$ només ens cal veure que és holomorfa en l'infinit, o equivalentment, que $\lim\limits_{z\to i\infty} G_k(z)$ està acotat.
Com $G_k(z+1) = G_k(z)$, és suficient comprovar-ho per a $z \in \mathbb{H}$ complint $|\Re(z)| \leq \frac{1}{2}$ i $\Im(z) \geq 1$. Utilitzant el mateix argument de la demostració del Lema 2.15, prenem $R_{\frac{1}{2},1}$, en particular tenim $c = 1$

$$\lim_{z\to i\infty} |G_k(z)| \leq \frac{8}{c^k} \sum_{j\geq 1} \frac{1}{j^{k-1}} = 8 \sum_{j\geq 1} \frac{1}{j^{k-1}} < +\infty.$$

□

Abans de donar la q-expansió de $G_k(z)$, donem una sèrie de definicions.

Anomenem *funció zeta de Riemann* $\zeta(s)$ a la funció holomorfa en $\{s \in \mathbb{C} \mid \Re(s) > 1\}$, definida per:

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

També definim $\sigma_t(n)$ com la suma de les t-potències dels divisors d'un enter n,

$$\sigma_t(n) := \sum_{\substack{d\mid n\\ d>0}} d^t.$$

Proposició 2.17. Per a $k \geq 4$ parell, la q-expansió de $G_k(z)$ ve donada per la fórmula

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

Demostració: Hi ha llibres que ho demostren utilizant la fórmula de sumació de Poisson, i n'hi ha d'altres que utilitzen la descomposició fraccional de $\pi\cot(\pi z)$. En aquest treball no la demostrarem, aquell que estigui interessat pot consultar ([Con16], §4.7).

Definició 2.18. Els *nombres de Bernoulli* són els nombres racionals B_k $(k \geq 0)$ definits per l'equació

$$\frac{x}{e^x - 1} = \sum_{k=1}^{\infty} \frac{B_k}{k!} x^k = 1 - \frac{1}{2}x + \frac{1}{12}x^2 - \frac{1}{720}x^4 + \cdots .$$

La següent taula resumeix els primers valors de B_k:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
B_k	1	$\frac{-1}{2}$	$\frac{1}{6}$	0	$\frac{-1}{30}$	0	$\frac{1}{42}$	0	$\frac{-1}{30}$	0	$\frac{5}{66}$	0	$\frac{-691}{2730}$	0	$\frac{7}{6}$	0	$\frac{-3617}{510}$

Utilitzant la *fórmula d'Euler per $\zeta(k)$ quan $k \geq 2$ és parell*

$$\zeta(k) = -\frac{(2\pi i)^k B_k}{2k!} \ ,$$

podem esciure la q-expansió de $G_k(z)$ com

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

Definició 2.19. Per a $k \geq 4$ parell definim la *sèrie d'Eisenstein normalitzada de pes k* com la sèrie G_k reescalada per tal que el coeficient de q sigui 1 [5].

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

Es pot observar que el producte de formes modulars de pes k i l és una forma modular de pes $k+l$, i la seva q-expansió és el producte de les dues q-expansions. També es pot veure que el conjunt de les formes modulars de pes k formen un $\mathbb{C}$-espai vectorial, més endavant veurem que és de dimensió finita.

2.5 Forma Modular Δ

Definim

$$\Delta := \frac{(240E_4)^3 - (-504E_6)^2}{1728} \ ^6.$$

És una forma modular de pes 12, amb la característica que el seu terme independent s'anul·la. Per tant Δ és una forma cuspidal de pes 12 per a $\mathrm{SL}_2(\mathbb{Z})$. Els coeficients de Fourier de Δ són enters; els denotem per $\tau(n)$.

$$\Delta = \sum_{n=1}^{\infty} \tau(n) q^n = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + 16744q^7 + \cdots .$$

La funció $n \mapsto \tau(n)$ rep el nom de *funció tau de Ramanujan* [7].

2.6 Fórmula de la València

La Fórmula de la València és molt útil per a donar forma als espai vectorials de formes modulars. Abans però, cal recordar uns resultats d'anàlisi complexa que ens permetran demostrar-la.

[5] Alguns llibres defineixen E_k de tal manera que el coeficient del terme independent sigui 1.

[6] Es pot demostrar que una definició equivalent és $\Delta = q \prod_{n=1}^{\infty} (1-q^n)^{24}$.

[7] Utilitzant els operadors de Hecke, que veurem més endavant, es pot demostrar que τ és multiplicativa i que compleix $\tau(p^r) = \tau(p)\tau(p^{r-1}) - p^{11}\tau(p^{r-2})$ per a tot p primer i $r \geq 2$ enter.

Teorema 2.20. (*Desenvolupament en sèries de Laurent*). Sigui $f \neq 0$ una funció meromorfa definida en un obert $U \subset \mathbb{C}$ i sigui $w \in U$. Aleshores, existeix un $M \in \mathbb{Z}$ tal que podem expressar localment f com la següent sèrie de potències al voltant de w:

$$f(z) = \sum_{n=M}^{\infty} a_n (z-w)^n,$$

amb $a_n \in \mathbb{C}$ i $a_M \neq 0$. Anomenem a M *l'ordre de* f *a* w i ho denotem per $\mathrm{ord}_w f$. El coeficient a_{-1} és el *residu de* f *a* w (per conveni és 0 si $M \geq 0$), denotat per $Res_w(f)$.

La derivada logarítmica de f ve donada per

$$\frac{f'(z)}{f(z)} = \frac{M}{z-w} + \frac{(M+1)a_{M+1}}{a_M} + \frac{(M+2)a_{M+2}}{a_M}(z-w) + \cdots .$$

Per tant, té un pol simple allà on f té un zero o un pol, en particular,

$$Res_w\left(\frac{f'}{f}\right) = M = \mathrm{ord}_w f.$$

Teorema 2.21. (*Principi de l'argument*). Sigui $f \neq 0$ meromorfa definida en un obert $U \subset \mathbb{C}$ simplement connex [8], i sigui $\mathcal{D}$ un contorn de U. Suposem que $\mathcal{D}$ no passa per cap zero ni pol de f, aleshores

$$\oint_{\mathcal{D}} \frac{f'(z)}{f(z)} dz = 2\pi i \sum_{z \in \mathring{\mathcal{D}}} \mathrm{ord}_z f,$$

on $\mathring{\mathcal{D}}$ denota els punts de l'interior de $\mathcal{D}$.

Seguidament donem tres resultats previs que ens serviran en la Fórmula de la València que veurem tot seguit.

Lema 2.22. Sigui $f \neq 0$ meromorfa en $\mathbb{H}$ i feblement modular de pes k, sigui $w \in \mathbb{H}$ i sigui $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Aleshores:

$$\mathrm{ord}_w f = \mathrm{ord}_{\gamma w} f.$$

Demostració: Sigui $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, tenim:

$$\lim_{z \to \gamma w} \frac{f(z)}{(z-\gamma w)^n} = (cw+d)^n \lim_{z \to \gamma w} \frac{(c\gamma^{-1}z+d)^k f(\gamma^{-1}z)}{(-cz+a)^n(\gamma^{-1}z-w)^n} = (cw+d)^{2n+k} \lim_{z \to w} \frac{f(z)}{(z-w)^n} \ ,$$

a més, $cw + d \neq 0$, i per tant els ordres coincideixen tal com volíem. □

Si a més, f és meromorfa en l'infinit, definim l'ordre de f a l'infinit de la següent manera:

$$\mathrm{ord}_\infty f = \mathrm{ord}_0 \tilde{f},$$

on $\tilde{f}$ és la funció de la Definició 2.11.

[8] Un domini simplement connex és aquell que és connex i en el que qualsevol corba tancada és homotòpicament equivalent a un punt.

Lema 2.23. Sigui $f \neq 0$ meromorfa en $\mathbb{H}$, feblement modular de pes k (per a $\mathrm{SL}_2(\mathbb{Z})$) i meromorfa en l'infinit. Aleshores existeix un $\tilde{C}$ amb $0 < \tilde{C} < +\infty$ tal que f és holomorfa i no s'anul·la quan $\Im(z) > \tilde{C}$.
Demostració: Al ser f meromorfa en l'infinit, existeix un $\varepsilon_1 > 0$ tal que $\tilde{f}$ és holomorfa en $\{z \in \mathbb{C} \mid 0 < |z| < \varepsilon_1\}$. A més, com que $f \neq 0$, $\tilde{f} \neq 0$, 0 no pot ser un punt d'acumulació dels zeros de $\tilde{f}$ (pel principi de la prolongació analítica). Per tant, existeix un $\varepsilon_2 > 0$ tal que $\tilde{f}$ és holomorfa i no s'anul·la en $\{z \in \mathbb{C} \mid 0 < |z| < \varepsilon_2\}$. Concloem que f és holomorfa i no s'anul·la si:

$$|q(z)| = |e^{2\pi i z}| = e^{-2\pi\Im(z)} < \varepsilon_2,$$

i això es dona si i només si

$$\Im(z) > \frac{-\log(\varepsilon_2)}{2\pi}.$$

Simplement definim $\tilde{C} := \frac{-\log(\varepsilon_2)}{2\pi}$. □

Lema 2.24. Sigui $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ amb $c \neq 0$ i sigui $f \neq 0$ meromorfa en $\mathbb{H}$, feblement modular de pes k (per a $\mathrm{SL}_2(\mathbb{Z})$) i meromorfa en l'infinit i sigui $\mathcal{D}$ una corba rectificable[9] en $\mathbb{H}$. Aleshores, tenim

$$\int_{\mathcal{D}} \frac{f'(z)}{f(z)} dz - \int_{\gamma(\mathcal{D})} \frac{f'(z)}{f(z)} dz = -k \int_{\mathcal{D}} \frac{1}{z + \frac{d}{c}} dz.$$

Demostració: Derivant $f(\gamma z) = (cz+d)^k f(z)$, obtenim

$$f'(\gamma z)\frac{d(\gamma z)}{dz} = f'(z)(cz+d)^k + ck(cz+d)^{k-1} f(z).$$

O equivalentment,

$$\frac{f'(\gamma z)}{f(\gamma z)} d(\gamma z) = \frac{f'(z)}{f(z)} dz + \frac{ck}{cz+d} dz.$$

Finalment,

$$\int_{\mathcal{D}} \frac{f'(z)}{f(z)} dz - \int_{\gamma(\mathcal{D})} \frac{f'(z)}{f(z)} dz = \int_{\mathcal{D}} \frac{f'(z)}{f(z)} dz - \int_{\mathcal{D}} \frac{f'(\gamma z)}{f(\gamma z)} d(\gamma z) = -k \int_{\mathcal{D}} \frac{1}{z + \frac{d}{c}} dz.$$

□

Teorema 2.25. (*Fórmula de la València*). Sigui $f \neq 0$ meromorfa en $\mathbb{H}$, feblement modular de pes k (per a $\mathrm{SL}_2(\mathbb{Z})$) i meromorfa en l'infinit. Llavors es compleix:

$$\mathrm{ord}_\infty f + \frac{1}{2}\mathrm{ord}_i f + \frac{1}{3}\mathrm{ord}_\rho f + \sum_{\substack{w \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \\ w \neq i, \rho}} \mathrm{ord}_w f = \frac{k}{12},$$

on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ denota el conjunt de $\mathrm{SL}_2(\mathbb{Z})$-òrbites en $\mathbb{H}$ i $\rho = \frac{-1}{2} + \frac{i\sqrt{3}}{2}$.
Demostració: Notem que pel Lema 2.22, el sumatori està ben definit. Per a calcular aquest sumatori integrem la derivada logarítmica de f al voltant de la corba de la Figura 1 i utilitzem el principi de l'argument. Denotem per $\mathcal{D}$ a la corba.

[9] Una corba rectificable és aquella que té longitud finita.

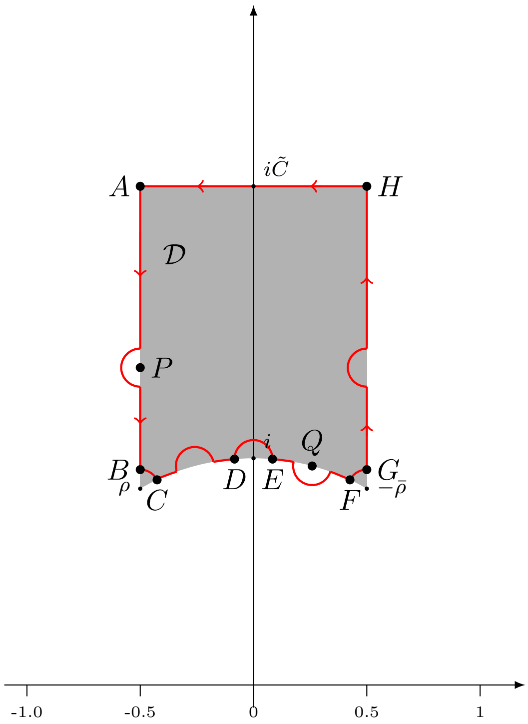


Figura 1

L'interior de la corba conté exactament un representant de cada zero i de cada pol de cada element de $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$, ja que pel Lema 2.23 no conté cap zero ni cap pol per a $\Im(z) > \tilde{C}$. Com que es tracta d'un conjunt discret sense punts d'acumulació en un compacte, el nombre de zeros i de pols és finit.

Per evitar incloure i i ρ a l'interior de la corba, els envoltem amb un cercle de radi suficientment petit que ens asseguri que no conté cap altre zero ni pol al seu interior. En el cas que hi hagi un zero o un pol a la corba, l'envoltem com es pot veure amb el punt P o el punt Q, així com, envoltem també el seu punt $\mathrm{SL}_2(\mathbb{Z})$-equivalent que també pertany a $\mathcal{D}$. D'aquesta manera ens assegurem que només el comptem una vegada.

Utilitzant ja el principi de l'argument, obtenim

$$\oint_{\mathcal{D}} \frac{f'(z)}{f(z)}dz = 2\pi i \sum_{z\in\mathring{\mathcal{D}}} \mathrm{ord}_z f = 2\pi i \sum_{\substack{w\in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}\\ w\neq i,\rho}} \mathrm{ord}_w f. \tag{2.4}$$

Per a evaluar la integral de l'esquerra dividim la corba $\mathcal{D}$ en diferents segments.

Degut al comportament periòdic de f: $f(z+1) = f(z)$, tenim

$$\int_G^H \frac{f'}{f}(z)dz = \int_B^A \frac{f'}{f}(z)dz = -\int_A^B \frac{f'}{f}(z)dz,$$

per tant les integrals entre GH i AB es cancel·len.

Seguidament, evaluem la integral entre H i A. Utilitzant que $f = \tilde{f}\circ q$, tenim

$$\frac{f'}{f}(z) = 2\pi i e^{2\pi i z}\frac{\tilde{f}'}{\tilde{f}}(e^{2\pi i z}).$$

Per tant, fent el canvi de variable $q = e^{2\pi i z}$ i fent servir el principi de l'argument a $\tilde{f}$,

$$\int_H^A \frac{f'}{f}(z)dz = -\oint_{|q|=e^{-2\pi C}} \frac{\tilde{f}'}{\tilde{f}}(q)dq = -2\pi i\ \mathrm{ord}_0\tilde{f} = -2\pi i\ \mathrm{ord}_\infty f.$$

A continuació, entre BC, DE i FG utilitzem de nou el principi de l'argument:

$$-3\int_B^C \frac{f'}{f}(z)dz - 3\int_F^G \frac{f'}{f}(z)dz = 2\pi i\ \mathrm{ord}_\rho f$$

$$-2\int_D^E \frac{f'}{f}(z)dz = 2\pi i \ \mathrm{ord}_i f.$$

Finalment, només ens queda calcular les integrals entre CD i EF. Per a fer-ho, fem servir el Lema 2.24.

En el nostre cas, tenim $\gamma = S$, $\mathcal{D} = CD$, $\gamma(\mathcal{D}) = FE$ i $f = f$. Sigui també ε el radi dels petits cercles que hem dibuixat. Utilitzant la definició d'integral de línia [10] i fent tendir ε a zero, obtenim

$$\frac{1}{2\pi i}\left(\int_C^D \frac{f'(z)}{f(z)}dz + \int_E^F \frac{f'(z)}{f(z)}dz\right) = \frac{1}{2\pi i}\left(\int_C^D \frac{f'(z)}{f(z)}dz - \int_F^E \frac{f'(z)}{f(z)}dz\right)$$

$$= -\frac{k}{2\pi i}\int_C^D \frac{1}{z}dz \overset{\varepsilon\to 0}{\longrightarrow} -\frac{k}{2\pi i}\left(\int_{\frac{1}{3}}^{\frac{1}{4}} \frac{1}{e^{2\pi i t}} 2\pi i e^{2\pi i t}dt\right) = \frac{k}{12}.$$

Juntant totes les parts de la demostració, tenim

$$\oint_{\mathcal{D}} \frac{f'(z)}{f(z)}dz = 2\pi i\left(-\frac{1}{3}\mathrm{ord}_\rho f - \mathrm{ord}_\infty f - \frac{1}{2}\mathrm{ord}_i f + \frac{k}{12}\right).$$

Per tant, utilitzant (2.4) i dividint per $2\pi i$, concloem el resultat

$$-\frac{1}{3}\mathrm{ord}_\rho f - \mathrm{ord}_\infty f - \frac{1}{2}\mathrm{ord}_i f + \frac{k}{12} = \sum_{\substack{w\in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \\ w\neq i,\rho}} \mathrm{ord}_w f.$$

□

2.7 Aplicacions de la Fórmula de la València: Espais de Formes Modulars

A partir d'ara, denotem per M_k al $\mathbb{C}$-espai vectorial de les formes modulars de pes k. El subespai de M_k de les formes cuspidals de pes k és S_k.

Proposició 2.26. Les següents afirmacions es compleixen:

1. E_4 té un zero simple a $z = \rho$ i no té cap altre zero.
2. E_6 té un zero simple a $z = i$ i no té cap altre zero.
3. Δ té un zero simple a $z = \infty$ i no té cap altre zero ($\Delta(z) \neq 0, \quad$ per a tot $z \in \mathbb{H}$).

Demostració: Tota forma modular, al ser holomorfa i holomorfa en l'infinit, compleix $\mathrm{ord}_z f \geq 0$ per a tot $z \in \mathbb{H}\cup\infty$. En particular, per a Δ, sabem que $\mathrm{ord}_\infty \Delta = 1$.

Substituint en la Fórmula de la València:

$$\mathrm{ord}_\infty f + \frac{1}{2}\mathrm{ord}_i f + \frac{1}{3}\mathrm{ord}_\rho f + \sum_{\substack{w\in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \\ w\neq i,\rho}} \mathrm{ord}_w f = \frac{k}{12},$$

veiem que les úniques combinacions possibles que satisfan la fórmula, són aquelles que es volen demostrar. □

[10]Sigui $U \in \mathbb{C}$ un obert, $\varrho : [a,b] \to U$ un camí i $f : U \to \mathbb{C}$ una funció contínua, aleshores definim la *integral de línia de f al llarg de ϱ* com $\int_\varrho f(z)dz = \int_a^b f(\varrho(t))\varrho'(t)dt$.

Corol·lari 2.27. Multiplicar per Δ ens dona un isomorfisme

$$\begin{array}{ccc} M_k & \longrightarrow & S_{k+12} \\ f & \longmapsto & \Delta \cdot f \ . \end{array}$$

Demostració: Clarament $\Delta \cdot f \in S_{k+12}$ i l'aplicació és lineal i injectiva. Per a l'exhaustivitat, sigui $g \in S_{k+12}$. Fem servir el fet que $\Delta(z) \neq 0$ per a tot $z \in \mathbb{H}$ i veiem que $\frac{g}{\Delta}$ és holomorfa i feblement modular de pes k. Com g s'anul·la a l'infinit, aquest zero cancel·la el zero simple de Δ i obtenim $\mathrm{ord}_\infty \frac{g}{\Delta} = \mathrm{ord}_\infty g - 1 \geq 0$, i per tant $\frac{g}{\Delta} \in M_k$. $\square$

Com a conseqüència del resultat anterior, per a tot $k \in \mathbb{Z}$, tenim $\dim M_k = \dim S_{k+12}$.

Teorema 2.28. *(Caracterització dels espais de formes modulars)* Els espais M_k i S_k són de dimensió finita per a tot $k \in \mathbb{Z}$. En particular:

1. $M_k = \{0\}$ si $k < 0$, si k és imparell o si $k = 2$.
2. $M_0 = \mathbb{C}$.
3. Per a $k = 4, 6, 8, 10, 14$ tenim $M_k = \mathbb{C}E_k$.
4. $S_k = \{0\}$ si $k < 16$ i $k \neq 12$.
5. $S_{12} = \mathbb{C}\Delta$.
6. $M_k = (\mathbb{C}E_k) \bigoplus S_k$, per a tot $k > 3$ parell.
7. La dimensió de M_k, per a $k \geq 0$ parell, ve donada per [11]

$$\dim M_k = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{si } k \equiv 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{si } k \not\equiv 2 \pmod{12} \end{cases}$$

Demostració:

1. Prèviament hem vist que $M_k = \{0\}$ per a k imparell. Per a $k < 0$ i per a $k = 2$ és una aplicació directa de la Fórmula de la València.
2. Sigui $f \in M_0$. Aleshores, existeix un $c \in \mathbb{C}$ tal que $f(z) - c \in M_0$ té almenys un zero. Per tant, utilitzant la Fórmula de la València, $f - c = 0$, que implica $f = c$, i per tant és constant.
3. Sigui $f \in M_k$ i sigui $a_0 = f(\infty)$. Amb el mateix mètode que hem vist a la demostració del Corol·lari 2.27, tenim $\frac{f(z) + \frac{a_0 2k}{B_k} E_k(z)}{\Delta} \in M_{k-12}$. Per l'apartat (1), $M_{k-12} = \{0\}$, per tant $f(z) = \frac{-a_0 2k}{B_k} E_k \in \mathbb{C}E_k$.
4. Aplicació directa del Corol·lari 2.27, fent servir que $M_k = \{0\}$.
5. Aplicació directa del Corol·lari 2.27, fent servir que $M_0 = \mathbb{C}$.
6. Per a qualsevol $f \in M_k$ existeix un únic $c \in \mathbb{C}$ tal que $f + cE_k \in S_k$. Per tant $f \in S_k \bigoplus \mathbb{C}E_k$.

[11] $\lfloor x \rfloor = max\{k \in \mathbb{Z} \mid k \leq x\}$.

7. Per l'apartat anterior i el Corol·lari 2.27, tenim dimM_k = dimS_k+1 = dimM_{k-12}+1 per a tot $k > 3$ parell. La demostració es redueix a una simple prova per inducció sobre k.

□

Lema 2.29. Sigui $k \in \mathbb{Z}$ i siguin f i g formes modulars de pes k. Siguin $\sum_{n\geq 0} a_n q^n$ i $\sum_{n\geq 0} b_n q^n$ les seves respectives q-expansions. Suposem que

$$a_j = b_j \quad \text{per a tot } j \in \left\{0, 1, ..., \left\lfloor \frac{k}{12} \right\rfloor \right\}.$$

Aleshores $f = g$.
Demostració: Suposem $f - g \neq 0$. Per hipòtesi, tenim $\mathrm{ord}_\infty(f - g) > \frac{k}{12}$, contradient el Teorema de la València, per tant $f = g$. □

Teorema 2.30. L'espai M_k admet com a base

$$M_k = \langle E_4^a E_6^b \mid a \geq 0,\ b \geq 0,\ 4a + 6b = k \rangle,$$

anomenada *base d'Eisenstein*.
Demostració: Sigui N_k el nombre d'elements de $\{a, b \in \mathbb{Z} \mid a \geq 0\ b \geq 0\ 4a + 6b = k\}$. Manualment podem veure que $N_k = \dim(M_k)$ per a $k \leq 14$. Per a $k \geq 14$, observem que si $4a + 6b = k - 12$, aleshores a partir de que $4a + 6(b + 2) = k$, i $4(a + 3) + 6b = k$, es dedueix la fórmula recursiva $N_k = 1 + N_{k-12}$. Per tant, $N_k = \dim(M_k)$ i la base proposada té la grandària correcta.
Per a veure que són linealment independents utilitzem un argument inductiu. Manualment podem comprovar-ho per a $k \leq 14$ (comparant els coeficients de les q-expansions). Per a $k \geq 14$, sigui

$$\sum_{\substack{4a+6b=k \\ a,b>0}} c_{a,b} E_4(z)^a E_6(z)^b = 0 \quad \text{per a certs } c_{a,b} \in \mathbb{C}.$$

Si tenim un terme amb $b = 0$, substituint $z = i$ obtenim $c_{a,0}E_4(i)^a = 0$ (recordem que $E_6(i) = 0$ i $E_4(i) > 0$), i per tant $c_{a,0} = 0$. És a dir, podem suposar que tots els termes del sumatori tenen $b \geq 1$. E_6 només s'anul·la a i, així que, dividint per E_6, obtenim

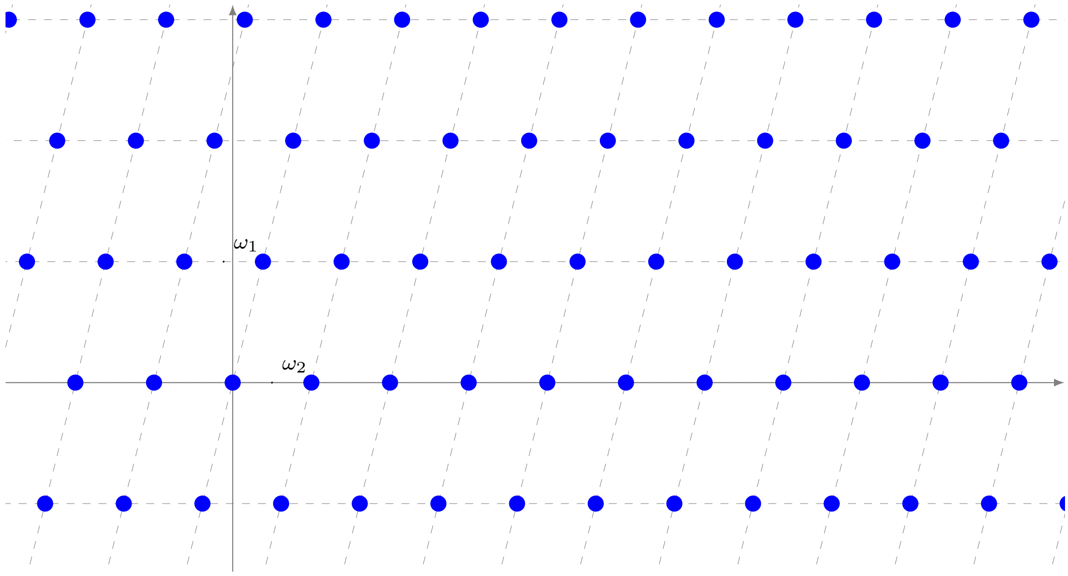
$$\sum_{\substack{4a+6b=k \\ a,b>0}} c_{a,b} E_4(z)^a E_6(z)^{b-1} = 0 \quad \text{per a tot } z \in \mathbb{H} - \{i\},$$

i per hipòtesi d'inducció, al ser una combinació lineal d'elements de M_{k-6}, $c_{a,b} = 0$, i concloem la demostració. □

3 Reticles i Operadors de Hecke

En aquesta secció, definirem uns operadors que actuen en l'espai de formes modulars. Abans però, introduïm uns conceptes matemàtics que ens ajudaran a entendre'ls.

3.1 Reticles



Definició 3.1. Un *reticle* Λ és un subgrup de $\mathbb{C}$ de la forma

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2,$$

on ω_1 i ω_2 són $\mathbb{R}$-linealment independents. Intercanviant, si cal, els rols de ω_1 i ω_2, sempre podem suposar que $\frac{\omega_1}{\omega_2} \in \mathbb{H}$. Denotem per $\mathcal{L}$ el conjunt de tots els reticles i per $\mathscr{M}$ el conjunt de parells (ω_1, ω_2) de $(\mathbb{C} - \{0\}) \times (\mathbb{C} - \{0\})$ tals que $\Im(\frac{\omega_1}{\omega_2}) > 0$.

Seguidament, donem una propietat important dels reticles. El següent fet ens permet identificar $\mathcal{L}$ amb el quocient de $\mathscr{M}$ per l'acció de $\mathrm{SL}_2(\mathbb{Z})$.

Lema 3.2. Siguin $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ i $\Lambda' = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$ dos reticles, amb $\frac{\omega_1}{\omega_2} \in \mathbb{H}$ i $\frac{\omega_1'}{\omega_2'} \notin \mathbb{R}$. Aleshores $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$ i $\frac{\omega_1'}{\omega_2'} \in \mathbb{H}$, si i només si

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix},$$

per a un cert $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.
Demostració: ($\Leftarrow$) Sigui $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Per hipòtesi, fent servir que γ és invertible, obtenim $\omega_1' = a\omega_1 + b\omega_2$, $\omega_2' = c\omega_1 + d\omega_2$, $\omega_1 = d\omega_1' - b\omega_2'$ i $\omega_2 = -c\omega_1' + a\omega_2'$, i per tant $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$. Finalment,

$$\frac{\omega_1'}{\omega_2'} = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\frac{\omega_1}{\omega_2} + b}{c\frac{\omega_1}{\omega_2} + d} = \gamma\left(\frac{\omega_1}{\omega_2}\right),$$

i concloem que $\Im(\frac{\omega_1'}{\omega_2'}) > 0$ usant el Lema 2.2.
($\Rightarrow$) Recíprocament, si $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$, aleshores existeixen γ i γ^{-1} pertayent a $\mathrm{M}_2(\mathbb{Z})$ tal que:

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \quad \text{i} \quad \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \gamma^{-1} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}.$$

Això implica que $\det(\gamma) = \pm 1$, però $\det(\gamma)$ no pot ser negatiu, ja que en aquest cas pel Lema 2.2 tindriem $\Im(\frac{\omega_1'}{\omega_2'}) < 0$ contradient la hipòtesi. $\square$

Per a $z \in \mathbb{H}$, definim $\Lambda_z := \mathbb{Z}z \oplus \mathbb{Z}$.
En particular, per a tot $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, $\Lambda = \omega_2 \Lambda_{\frac{\omega_1}{\omega_2}}$.

A continuació, definim un tipus de funció que ens permetrà relacionar la teoria de formes modulars introduïda a la secció anterior, amb els reticles.

Definició 3.3. Una funció $\mathcal{F} : \mathcal{L} \to \mathbb{C}$ és *homogènia de pes* $k \in \mathbb{Z}$, si compleix

$$\mathcal{F}(\lambda\Lambda) = \lambda^{-k}\mathcal{F}(\Lambda),$$

per a tot $\lambda \in \mathbb{C}^\times$ i $\Lambda \in \mathcal{L}$.

Teorema 3.4. Fixat un $k \in \mathbb{Z}$. Hi ha una correspondència $1-1$ entre el conjunt de funcions $f : \mathbb{H} \to \mathbb{C}$ que compleixen la fórmula (2.2) i el conjunt de funcions $\mathcal{F} : \mathcal{L} \to \mathbb{C}$ homogènies de pes k. Aquesta bijecció ve donada per:

$$\begin{array}{rcl} f : \mathbb{H} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \mathcal{F}(\Lambda_z) \end{array},$$

i

$$\begin{array}{rcl} \mathcal{F} : \mathcal{L} & \longrightarrow & \mathbb{C} \\ \Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 & \longmapsto & \omega_2^{-k} f\left(\frac{\omega_1}{\omega_2}\right) \end{array}.$$

Demostració: Per a la primera part, sigui $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ i sigui $z \in \mathbb{H}$. Usant el Lema 3.2 veiem que

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

Per tant,

$$\begin{aligned} f(\gamma z) &= \mathcal{F}(\Lambda_{\gamma z}) = \mathcal{F}((cz+d)^{-1}(\mathbb{Z}(az+b) \oplus \mathbb{Z}(cz+d))) \\ &= \mathcal{F}((cz+d)^{-1}\Lambda_z) = (cz+d)^k \mathcal{F}(\Lambda_z) = (cz+d)^k f(z). \end{aligned}$$

Per a la segona part, clarament $\mathcal{F}(\lambda\Lambda) = \lambda^{-k}\mathcal{F}(\Lambda)$. Només ens cal comprovar, que està ben definida, és a dir, no depèn de la base triada per a Λ. Sigui $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, suposem que es compleix

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix},$$

aleshores,

$$\mathcal{F}(\mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2') = \omega_2'^{-k} f\left(\frac{\omega_1'}{\omega_2'}\right) = (c\omega_1 + d\omega_2)^{-k} f\left(\gamma\left(\frac{\omega_1}{\omega_2}\right)\right) = \omega_2^{-k} f\left(\frac{\omega_1}{\omega_2}\right) = \mathcal{F}(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2).$$

$\square$

3.2 Operadors de Hecke

Denotem per $\mathrm{X}_{\mathcal{L}}$ el grup abelià lliure generat per $\mathcal{L}$, és a dir, les combinacions lineals de la forma $\sum n_i \Lambda_i$ amb $n_i \in \mathbb{Z}$ i $\Lambda_i \in \mathcal{L}$. Tota correspondència $\mathrm{X}_{\mathcal{L}} \to \mathrm{X}_{\mathcal{L}}$, que és un homomorfisme de grups, queda unívocament determinada pels seus valors als elements de $\mathcal{L}$. Per evitar confusió, denotem per $n \cdot \Lambda$ si ens referim a l'element de $\mathrm{X}_{\mathcal{L}}$ que denota n vegades Λ, i per $n\Lambda$ el subreticle de Λ que denota la multiplicació de cada element de Λ per n.

Sigui $\mathcal{F} : \mathcal{L} \to \mathbb{C}$ una funció i T una correspondència. Considerem l'extensió lineal de $\mathcal{F}$ a $\mathrm{X}_{\mathcal{L}}$, i denotem per $T\mathcal{F}$ a la següent funció:

$$\begin{array}{rcl} T\mathcal{F} : \mathrm{X}_{\mathcal{L}} & \longrightarrow & \mathbb{C} \\ \Lambda & \longmapsto & \mathcal{F}(T(\Lambda)) \end{array} .$$

Definició 3.5. Per a tot $n > 0$ natural, l'*operador de Hecke* T_n *en reticles* és la següent correspondència:

$$\begin{array}{rcl} T_n : \mathrm{X}_{\mathcal{L}} & \longrightarrow & \mathrm{X}_{\mathcal{L}} \\ \Lambda & \longmapsto & \displaystyle\sum_{[\Lambda:\Lambda']=n} \Lambda' \end{array} ,$$

on $[\Lambda : \Lambda'] = n$ denota els subgrups de Λ d'índex n. La suma és finita, ja que $n\Lambda \subseteq \Lambda' \subseteq \Lambda$ per a tot Λ', i utilitzant el teorema de correspondència per a grups notem que tot Λ' el podem fer correspondre a un únic subgrup de $\Lambda/n\Lambda \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$.

Finalment, ja ens trobem preparats per a definir els operadors de Hecke en formes modulars.

Definició 3.6. Sigui $f \in M_k$ i sigui $\mathcal{F}$ la funció homogènia de pes k donada pel Teorema 3.4. Per a tot $n \in \mathbb{Z}$, $n > 0$ definim *l'operador de Hecke* T_n *en* M_k, com:

$$T_n f(z) := n^{k-1} \mathrm{T}_n \mathcal{F}(\Lambda_z).$$

Clarament $T_n f$ satisfà (2.2), ja que $n^{k-1}\mathrm{T}_n\mathcal{F}$ és homogènia de pes $k \in \mathbb{Z}$. Per a veure que $T_n f \in M_k$ necessitem estudiar la seva q-expansió.

Sigui $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ una matriu amb coeficients enters i determinant $n > 0$ enter, i sigui un reticle $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Aleshores si

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix},$$

es té que $\Lambda' = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$ és un subreticle de Λ d'índex n. Utilitzant el Lema 3.2 veiem que dues matrius γ_1 i γ_2 determinen el mateix reticle si i només si existeix un element γ de $\mathrm{SL}_2(\mathbb{Z})$ tal que $\gamma_1 = \gamma\gamma_2$. Per tant, cada subgrup de Λ d'índex n el podem indentificar amb una òrbita de l'acció de $\mathrm{SL}_2(\mathbb{Z})$ (per la dreta) en $M_2^n(\mathbb{Z})$ (el conjunt de les matrius amb coeficients enters i determinant n). Notem que hi ha un nombre finit d'òrbites, ja que hi ha un nombre finit de subgrups de Λ d'índex n.
Siguin $\alpha_1, \ldots, \alpha_{s_n}$ representants de les òrbites, aleshores tenim la descomposició disjunta següent:

$$M_2^n(\mathbb{Z}) = \bigcup_{i=1}^{s_n} \mathrm{SL}_2(\mathbb{Z})\alpha_i \ .$$

Proposició 3.7. Siguin $\alpha_1, \dots, \alpha_{s_n}$ definits anteriorment. Donat $f \in M_k$ l'operador de Hecke, el podem escriure de la següent manera:

$$T_n f = \sum_{i=1}^{s_n} f|_k \alpha_i \ ,$$

on $f|_k\alpha_i$ denota l'operador barra de pes k definit a la Proposició 2.6. Per tant, $T_n f$ és holomorfa en $\mathbb{H}$.

Demostració: Sigui $z \in \mathbb{Z}$. Si $[\Lambda_z : \Lambda_i'] = n$, sigui $\alpha_i = \left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$ el representant de $\Lambda_i' = \mathbb{Z}\omega_1^{(i)} \oplus \mathbb{Z}\omega_2^{(i)}$, és a dir,

$$\begin{pmatrix} \omega_1^{(i)} \\ \omega_2^{(i)} \end{pmatrix} = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \begin{pmatrix} z \\ 1 \end{pmatrix},$$

aleshores,

$$T_n \mathcal{F}(\Lambda_z) = \mathcal{F}\left(\sum_{i=1}^{s_n} \omega_2^{(i)} \Lambda_{\frac{\omega_1^{(i)}}{\omega_2^{(i)}}} \right) = \sum_{i=1}^{s_n} (\omega_2^{(i)})^{-k} f\left(\frac{\omega_1^{(i)}}{\omega_2^{(i)}} \right) = n^{1-k} \sum_{i=1}^{s_n} f|_k \alpha_i \ .$$

A més, l'expressió no depèn dels representants α_i escollits, ja que si $\alpha_i = \gamma\alpha_j$ per un cert $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, aleshores $f|_k\alpha_i = f|_k(\gamma\alpha_j) = f|_k\alpha_j$. $\square$

El següent Lema, dona forma als subgrups de tot reticle d'índex n. Ens permetrà donar la q-expansió dels operadors de Hecke.

Lema 3.8. Les matrius de la forma $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ amb $ad = n$, $d > 0$ i $0 \le b < d$, formen un conjunt de representants de les òrbites de l'acció de $\mathrm{SL}_2(\mathbb{Z})$ (per la dreta) en $M_2^n(\mathbb{Z})$.

Demostració: Sigui $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in M_2^n(\mathbb{Z})$, busquem un $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, tal que $\gamma \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$ sigui de la forma buscada. Prenem x, y, z i w enters tals que $za' + wc' = 0$ i $xw + y(-z) = 1$. Aleshores $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. A més, $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b'' \\ 0 & d \end{smallmatrix}\right)$, per a certs a, b'', d enters. Sempre podem garantir que a i d són positius, multiplicant per l'esquerra, si cal, per $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Finalment, prenem q i b enters amb $0 \le b < d$, tals que $b'' = dq + b$, concloem

$$\left(\begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} \right) \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Seguidament veiem la unicitat. Suposem que dos elements de la forma del Lema pertanyen a la mateixa òrbita, és a dir,

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix},$$

amb $xw - yz = 1$, $ad = a'd' = n$, $d > 0$, $d' > 0$, $0 \le b < d$ i $0 \le b' < d'$. Veiem que $az = 0$, per tant $z = 0$. A més, $xw = 1$, i com $d' = dw$ amb $d > 0$ i $d' > 0$, es desprèn que $x = w = 1$. Finalment, $b + yd = b'$ amb b i b' entre 0 i $d - 1$, implica $y = 0$.

$\square$

Utilitzant els dos resultats anteriors, deduïm la següent expressió:

$$T_m f = m^{k-1} \sum_{\substack{ad=m \\ 0 \le b < d}} d^{-k} f\left(\frac{az+b}{d} \right).$$

Proposició 3.9. (*q-expansió dels operadors de Hecke*). Considerem $f \in M_k$ i la seva q-expansió $f(z) = \sum_{n=0}^{\infty} c_n q^n$, aleshores

$$T_m f(z) = \sum_{n=0}^{\infty} \sum_{\substack{a|\mathrm{mcd}(n,m)\\ a>0}} c_{\frac{nm}{a^2}} a^{k-1} q^n.$$

A més, $T_m f \in M_k$ i la seva restricció a S_k també pertany a S_k.
Demostració:

$$T_m f = m^{k-1} \sum_{\substack{ad=m\\ 0\leq b<d}} d^{-k} f\left(\frac{az+b}{d}\right) = m^{k-1} \sum_{\substack{ad=m\\ 0\leq b<d}} \sum_{n=0}^{\infty} d^{-k} c_n e^{2\pi i n \frac{az+b}{d}}$$

$$= m^{k-1} \sum_{n=0}^{\infty} \sum_{\substack{ad=m\\ 0\leq b<d}} d^{-k} c_n e^{2\pi i n \frac{az+b}{d}} = m^{k-1} \sum_{l=0}^{\infty} \sum_{\substack{ad=m\\ 0<d}} d^{-k+1} c_{ld} q^{la} = \sum_{l=0}^{\infty} \sum_{\substack{a|m\\ a>0}} c_{\frac{lm}{a}} a^{k-1} q^{la}.$$

En la penúltima igualtat, notem que

$$\sum_{b=0}^{d-1} e^{2\pi i n \frac{b}{d}} = \begin{cases} d & \text{si } d \mid n \\ 0 & \text{si } d \nmid n \end{cases}$$

i apliquem el canvi $l = \frac{n}{d}$.
Finalment, agrupant els coeficients de q, amb $la = n$, obtenim

$$\sum_{l=0}^{\infty} \sum_{\substack{a|m\\ a>0}} c_{\frac{lm}{a}} a^{k-1} q^{la} = \sum_{n=0}^{\infty} \sum_{\substack{a|\mathrm{mcd}(n,m)\\ a>0}} c_{\frac{nm}{a^2}} a^{k-1} q^n .$$

Com que el coeficient de q^0 és $c_0 \sum_{\substack{a|m\\ a>0}} a^{k-1}$, concloem que $T_m f \in M_k$. A més, si $f \in S_k$, aleshores $c_0 = 0$, i $T_m f \in S_k$. $\square$

A continuació, veurem com interactuen els operadors de Hecke entre si. Abans, però, definim un nou operador. Sigui $\lambda \in \mathbb{C}^\times$,

$$\begin{array}{rcl} R_\lambda : \mathrm{X}_\mathcal{L} & \longrightarrow & \mathrm{X}_\mathcal{L} \\ \Lambda & \longmapsto & \lambda\Lambda \end{array}.$$

Clarament, per a tot λ, $\mu \in \mathbb{C}^\times$ i $n > 0$ enter, $R_\lambda R_\mu = R_{\lambda\mu}$ i $R_\lambda T_n = T_n R_\lambda$. El comportament de les interaccions dels T_n entre si és més complex i l'estudiem a continuació.

Proposició 3.10. Els operadors T_n satisfan:

(1) $T_{p^r} T_p = T_{p^{r+1}} + p \cdot R_p T_{p^{r-1}}$ per a tot $r > 0$ enter i p primer,
(2) $T_m T_n = T_{mn}$ per a m i n enters positius coprimers.

Demostració: Per a la primera afirmació veiem que en els dos costats de la igualtat, donat un reticle Λ, ens retorna una combinació lineal de subreticles de Λ d'índex p^{r+1}. Sigui un tal subreticle Λ', veurem que el coeficient associat amb ell és el mateix als dos costats de la igualtat. Clarament, el coeficient associat a $T_{p^{r+1}}$ és 1. Seguidament, considerem dos casos:

- $\Lambda' \subseteq p\Lambda$: En aquest cas el coeficient associat a $R_pT_{p^{r-1}} = T_{p^{r-1}}R_p$ és 1, per tant, l'associat a la part dreta de la igualtat és $p+1$. Per a la part esquerra, tots els subreticles de Λ d'índex p contenen a $p\Lambda$, doncs a Λ' també. Per tant, el coeficient associat és igual a la quantitat de subreticles d'índex p de Λ. Utilitzant el Lema 3.8 amb $n = p$, veiem que n'hi ha $p+1$.
- $\Lambda' \not\subseteq p\Lambda$: El costat dret de la igualtat, en aquest cas, clarament és 1. Per a l'altre costat Λ' té el coeficient major o igual a 1. Suposem que hi ha dos subreticles de Λ diferents: Λ_1 i Λ_2, d'índex p que contenen a Λ'. En aquest cas $\Lambda' \subseteq \Lambda_1 \cap \Lambda_2 = p\Lambda$, contradient la hipòtesi.

Seguidament, provem la segona expressió. De la mateixa manera que amb la fórmula anterior, considerem $\Lambda' \subset \Lambda$ d'índex mn. Donat que Λ/Λ' és abelià de cardinalitat mn amb m i n coprimers, el podem expressar com

$$\Lambda/\Lambda' \cong G_1 \oplus G_2,$$

on G_1 i G_2 tenen cardinalitat m i n respectivament. A més G_1 és l'únic subgrup de Λ/Λ' d'ordre m. Utilitzant el teorema de correspondència per a grups notem que podem fer correspondre G_1 amb un únic Λ'' que conté Λ' i $[\Lambda : \Lambda''] = n$. Per tant, el coeficient que acompanya Λ' és 1, i concloem la demostració. $\square$

Teorema 3.11. Sigui $f \in M_k$. Aleshores es compleix:

(1) $T_mT_nf = T_{mn}f$	per a m i n enters positius coprimers,
(2) $T_pT_{p^r}f = T_{p^{r+1}}f + p^{k-1}T_{p^{r-1}}f$	per a tot $r > 0$ enter i p primer,
(3) $T_mT_nf = T_{mn}f$	per a m i n enters positius.

Demostració: Per a la primera observació, observem:

$$T_mT_nf(z) = T_mn^{k-1}T_n\mathcal{F}(\Lambda_z) = T_mn^{k-1}\mathcal{F}(T_n(\Lambda_z)) = m^{k-1}n^{k-1}\mathcal{F}(T_nT_m(\Lambda_z)) = T_{nm}f(z).$$

On hem utilitzat que $T_nT_m = T_{nm}$ vist a la Proposició anterior.
Per a la segona part, tenim:

$$\begin{aligned}T_pT_{p^r}f(z) &= p^{k-1}(p^r)^{k-1}\mathcal{F}(T_{p^r}T_p(\Lambda_z)) = (p^{r+1})^{k-1}\mathcal{F}(T_{p^{r+1}}(\Lambda_z) + p\cdot R_pT_{p^{r-1}}(\Lambda_z))\\ &= (p^{r+1})^{k-1}\mathcal{F}(T_{p^{r+1}}(\Lambda_z)) + (p^{r+1})^{k-1}p\mathcal{F}(R_pT_{p^{r-1}}(\Lambda_z))\\ &= T_{p^{r+1}}f + (p^{r+1})^{k-1}pT_{p^{r-1}}\mathcal{F}(R_p(\Lambda_z)) = T_{p^{r+1}}f + (p^{r+1})^{k-1}pT_{p^{r-1}}p^{-k}\mathcal{F}(\Lambda_z)\\ &= T_{p^{r+1}}f + (p^r)^{k-1}T_{p^{r-1}}\mathcal{F}(\Lambda_z) = T_{p^{r+1}}f + (p^r)^{k-1}(p^{r-1})^{1-k}T_{p^{r-1}}f = T_{p^{r+1}}f + p^{k-1}T_{p^{r-1}}f.\end{aligned}$$

On també hem utilitzat de nou el resultat de la Proposició 3.10.
Finalment, combinant els dos primers apartats, veiem que per a tot $r > 0$ enter, T_{p^r} és un polinomi en T_p i per tant concloem que tot els operadors de Hecke commuten. $\square$

3.3 Producte Escalar de Petersson

En aquesta secció dotem l'espai de les formes cuspidals, S_k, amb un producte escalar anomenat producte escalar de Petersson. Tal com veurem, aquest producte té diverses propietats, la principal és que els operadors de Hecke són autoadjunts respecte aquest. Desgraciadament, el producte no es pot generalitzar a l'espai de formes modulars.

El primer que fem, i que recull la lema de sota, és demostrar que la 2-forma diferencial $\frac{dx\wedge dy}{y^2}$ és $\mathrm{SL}_2(\mathbb{Z})$-invariant. En tota la secció $z \in \mathbb{H}$, l'expressem com $z = x + iy$.

Lema 3.12. Sigui $U \subset \mathbb{H}$ tal que la seva frontera està formada per un nombre finit de segments i arcs. Sigui $f : U \to \mathbb{C}$ continua i sigui $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Es compleix:

$$\int_U f(z)\frac{dx\ dy}{y^2} = \int_{\gamma^{-1}(U)} f(\gamma z)\frac{dx\ dy}{y^2}.$$

Demostració: Sigui $\gamma : \mathbb{H} \to \mathbb{H}$ la transformació holomorfa lineal fraccionària. En particular,

$$\gamma'(z) = \frac{1}{(cz+d)^2}\ ,$$

per a $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Si veiem $\mathbb{H}$ com un obert de $\mathbb{R}^2$ i γ com una aplicació real diferenciable, aleshores el Jacobià ve donat per:

$$J_\gamma(x,y) = \begin{pmatrix} \frac{\partial \gamma_1}{\partial x} & \frac{\partial \gamma_1}{\partial y} \\ \frac{\partial \gamma_2}{\partial x} & \frac{\partial \gamma_2}{\partial y} \end{pmatrix},$$

on $\gamma_1(x,y) = \Re(\gamma(x+iy))$ i $\gamma_2(x,y) = \Im(\gamma(x+iy))$. A més $\gamma'(z) = \frac{\partial \gamma_1}{\partial x} + i\frac{\partial \gamma_2}{\partial x}$. Combinant aquest resultat amb les equacions de Cauchy-Riemann, obtenim:

$$|\det J_\gamma(x,y)| = \left|\frac{\partial \gamma_1}{\partial x}\frac{\partial \gamma_2}{\partial y} - \frac{\partial \gamma_2}{\partial x}\frac{\partial \gamma_1}{\partial y}\right| = \left(\frac{\partial \gamma_1}{\partial x}\right)^2 + \left(\frac{\partial \gamma_2}{\partial x}\right)^2 = |\gamma'(z)|^2 = \frac{1}{|(cz+d)|^4} = \frac{\Im(\gamma z)^2}{\Im(z)^2}\ ,$$

on a la darrera igualtat hem utilitzat el Lema 2.2. Finalment,

$$\int_U f(z)\frac{dx\ dy}{y^2} = \int_{\gamma^{-1}(U)} f(\gamma z)|\det J_\gamma(x,y)|\frac{dx\ dy}{\Im(\gamma z)^2} = \int_{\gamma^{-1}(U)} f(\gamma z)\frac{dx\ dy}{y^2}\ .$$

□

Els següents dos lemes són senzills i ens recullen certes propietats que ajuden a veure que el producte escalar de Petersson estarà ben definit.

Lema 3.13. Siguin f i g pertanyent a M_k. Aleshores $F(z) = f(z)\overline{g(z)}\Im(z)^k$ és $\mathrm{SL}_2(\mathbb{Z})$-invariant, on $\overline{g(z)}$ denota el conjugat complex.
Demostració: Sigui $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Utilitzant la fórmula (2.2) i el Lema 2.2, obtenim:

$$F(\gamma z) = f(\gamma z)\overline{g(\gamma z)}\Im(\gamma z)^k = (cz+d)^k f(z)(\overline{cz+d})^k\overline{g(z)}|(cz+d)|^{-2k}\Im(z)^k = F(z).$$

Per tant, concloem el que volíem demostrar. □

Lema 3.14. Sigui $f \in S_k$ amb q-expansió $\displaystyle\sum_{n=1}^{\infty} c_n q^n$, aleshores $|f(z)|y^{\frac{k}{2}}$ està acotat en $\mathbb{H}$.
Demostració: És suficient comprovar que està acotat en el domini fonamental, per tant, ho comprovarem només per a $z \in \mathcal{F}$. Per a y suficientment gran, tenim:

$$\left|\sum_{n=1}^{\infty} c_n q^n\right| = \left|q\left(c_1 + \sum_{n=2}^{\infty} c_n q^{n-1}\right)\right| \le e^{-2\pi y}(c_1 + C),$$

per a una certa constant C. Per tant,

$$\lim_{y\to\infty} |f(x+iy)|y^{\frac{k}{2}} \le \lim_{y\to\infty} e^{-2\pi y}(c_1+C)y^{\frac{k}{2}} = 0.$$

Per tant existeix un $Y > 0$ tal que per a tot $y > Y$, $|f(z)|y^{\frac{k}{2}} < 1$. Com que la part de $\mathcal{F}$ per a $y \le Y$ és un compacte, també està acotada i concloem la demostració. □

Una vegada donats els lemes previs, ja estem en condicions de definir el producte escalar de Petersson.

Definició 3.15. Per a f i g pertanyent a S_k definim el *producte escalar de Petersson* com:

$$\langle f, g\rangle = \int_{\mathcal{F}} f(z)\overline{g(z)}y^k \frac{dx\ dy}{y^2},$$

Utilitzant els lemes previs, aquesta definició no depèn del domini fonamental que considerem. A més, utilitzant el Lema anterior, observem:

$$\left| \int_{\mathcal{F}} f(z)\overline{g(z)}y^k \frac{dx\ dy}{y^2} \right| \leq \int_{\mathcal{F}} |f(z)||g(z)|y^k \frac{dx\ dy}{y^2} \leq C_1C_2 \int_{\mathcal{F}} \frac{dx\ dy}{y^2} = C_1C_2\frac{\pi}{3},$$

on C_1 i C_2 són les cotes proporcionades pel Lema 3.14. Per tant la integral convergeix i el producte està ben definit. Clarament és un producte hermític definit-positiu en S_k. En particular, $(S_k, \langle\cdot,\cdot\rangle)$ és un espai de Hilbert.

No és difícil veure que es pot generalitzar el producte i definir el producte en $M_k \times S_k$, és a dir, si f o g pertanyen a S_k el producte continua convergint. En aquest cas podem definir el següent subespai vectorial.

Definició 3.16. El *subespai d'Eisenstein de* M_k el definim per:

$$\mathscr{E}_k = \{f \in M_k \mid \langle f, g\rangle = 0\ \forall g \in S_k\}.$$

Seguidament, estudiem una propietat important d'aquest producte escalar i és la seva interacció amb els operadors de Hecke.

Teorema 3.17. Els operadors de Hecke T_n en l'espai S_k són autoadjunts respecte al producte escalar de Petersson, és a dir,

$$\langle T_n f, g\rangle = \langle f, T_n g\rangle,$$

per a tot f i g pertanyent a S_k.
Demostració: La prova es pot trobar per exemple en ([Kna92], §VIII).

A continuació, enunciem un resultat d'àlgebra lineal:

Teorema 3.18. (*Teorema Espectral*) Sigui V un $\mathbb{C}$-espai vectorial de dimensió finita, i sigui $\phi \subseteq \mathrm{End}_{\mathbb{C}} V$ una familia d'endomorfismes de V normals, i que commuten. Aleshores existeix una $\mathbb{C}$-base de vectors propis simultanis per a tot $A \in \phi$.

Corol·lari 3.19. S_k té una base de vectors propis simultanis per a tots els operadors de Hecke T_n.
Demostració: Apliquem el Teorema Espectral amb $V = S_k$ i $\phi = \{T_n \mid n > 0,\ n \in \mathbb{Z}\}$. Els operadors de Hecke són normals pel Teorema 3.17 i commuten pel Teorema 3.11. □

Definició 3.20. Diem que $f \neq 0$, $f \in M_k$ és una *forma pròpia* si és un vector propi per a tots els operadors de Hecke T_n.

Finalment, donem una propietat que caracteritza als vectors propis simultanis.

Proposició 3.21. Sigui $f \in S_k$ una forma pròpia, és a dir, $T_n f = \lambda_n f$. Aleshores, si $f(z) = \sum_{n=1}^{\infty} c_n q^n$, es compleix:

$$c_n = \lambda_n c_1,$$

i, per tant, si $f \neq 0$ es té $c_1 \neq 0$.

Demostració: Utilitzant q-expansió de $T_n f$ donada per la Proposició 3.9 veiem que el coeficient que acompanya q és c_n, per tant concloem el que volíem demostrar. $\square$

4 Formes Modulars per a Subgrups de Congruència de $\mathrm{SL}_2(\mathbb{Z})$

4.1 Subgrups de Congruència de $\mathrm{SL}_2(\mathbb{Z})$

En aquest capítol generalitzem el concepte de forma modular, per a certs subgrups Γ de $\mathrm{SL}_2(\mathbb{Z})$. Sigui $N > 0$ un nombre natural.

Definició 4.1. El *subgrup de congruència principal de nivell* N és

$$\Gamma(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod N\}.$$

Clarament, $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. Alternativament, $\Gamma(N)$ és el nucli de π_N, on

$$\begin{aligned} \pi_N : \mathrm{SL}_2(\mathbb{Z}) &\longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) &\longmapsto \left(\begin{smallmatrix} a \pmod N & b \pmod N \\ c \pmod N & d \pmod N \end{smallmatrix}\right) \end{aligned}$$

és el morfisme induït per la reducció $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$.

Lema 4.2. El morfisme π_N és exhaustiu, i per tant, utilitzant el primer teorema d'isomorfia de grups

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}),$$

a més, $\Gamma(N)$ és un subgrup normal d'índex finit de $\mathrm{SL}_2(\mathbb{Z})$.
Demostració: Sigui $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z})$ un representant de $[\gamma] \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, aleshores $ad - bc \equiv 1 \pmod N$, equivalentment, $ad - bc + kN = 1$, per a un cert $k \in \mathbb{Z}$. Sense pèrdua de generalitat suposem que $d \neq 0$. Clarament $\mathrm{mcd}(c, d, N) = 1$, ja que si $p \mid d$ i $p \mid c$, aleshores $p(a\frac{d}{p} - b\frac{c}{p}) = 1 - kN$, que implica $p \nmid N$.
Sigui p un primer que divideix d. Afirmem que existeix un $g_p \in \mathbb{Z}$ tal que $p \nmid (c + g_p N)$. Si $p \mid c$, aleshores $p \nmid N$ i prenem $g_p = 1$, si $p \nmid c$, prenem $g_p = 0$.
Aplicant el *Teorema Xinès del Residu* a tots els primers p_i que divideixen d, trobem $g \in \mathbb{Z}$ tal que $g \equiv g_{p_i} \pmod{p_i}$ per a tot $p_i \mid d$. Com a conclusió, cap primer divideix $c + gN$ i d a la vegada, per tant $\mathrm{mcd}(c + gN, d) = 1$.
Finalment, usant la *Identitat de Bézout*, prenem $e, f \in \mathbb{Z}$ tals que $ed - f(c+gN) = k + bg$.
Afirmem que $\left(\begin{smallmatrix} a+eN & b+fN \\ c+gN & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.
Efectivament, $ad + eNd - bc - bgN - fcN - fgN^2 = 1 + N(-k + ed - bg - fc - fgN) = 1 + N(-k - bg + ed - f(c + gN)) = 1$.

□

Definició 4.3. Un subgrup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ és un *subgrup de congruència* si existeix un $N > 0$, $N \in \mathbb{Z}$, tal que $\Gamma(N) \subseteq \Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$. El menor N que ho compleix és el *nivell* de Γ.

Per tant, tot subgrup de congruència compleix:

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] < \infty$$ [12].

Exemple 4.4. Els següents subgrups són de congruència:

$$\Gamma_1(N) = \left\{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \pmod N\right\}.$$

[12] Cal destacar que existeixen subgrups d'índex finit que no són de congruència.

$$\Gamma_0(N) = \left\{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \pmod N\right\}.$$

a més, es compleix

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})\ ^{13}.$$

El subgrup $\Gamma_0(N)$ jugarà un paper important més endavant en el treball.

Lema 4.5. Es compleix:

1. L'aplicació $\pi_{1,N}$ és un morfisme de grups exhaustiu i el nucli de $\pi_{1,N}$ és $\Gamma(N)$,

$$\begin{aligned} \pi_{1,N} : \Gamma_1(N) &\longrightarrow \mathbb{Z}/N\mathbb{Z} \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) &\longmapsto b \pmod N, \end{aligned}$$

   per tant,

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

2. L'aplicació $\pi_{0,N}$ és un morfisme de grups exhaustiu i el nucli de $\pi_{0,N}$ és $\Gamma_1(N)$,

$$\begin{aligned} \pi_{0,N} : \Gamma_0(N) &\longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) &\longmapsto d \pmod N, \end{aligned}$$

   per tant,

$$[\Gamma_0(N) : \Gamma_1(N)] = \varphi(N)\ ^{14}.$$

3. $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p \mid N} \left(1 + \frac{1}{p}\right)$.

Demostració:

1. Clarament és un morfisme de grups i el seu nucli és $\Gamma(N)$. L'exhaustivitat, es desprèn veient que $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$.

2. Clarament $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, ja que si $\mathrm{mcd}(d, N) > 1$, aleshores $\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) > 1$. Trivialment, és un morfisme de grups. Per a l'exhaustivitat, sigui $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, i sigui d^{-1} el seu invers a $(\mathbb{Z}/N\mathbb{Z})^\times$, llavors, utilitzant el mateix argument que a la demostració del Lema 4.2 amb la matriu $\left(\begin{smallmatrix} d^{-1} & 0 \\ 0 & d \end{smallmatrix}\right)$, trobem un element $\gamma \in \Gamma_0(N)$ tal que $\pi_{0,N}(\gamma) = d$.
   Finalment, sigui $\gamma = \left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right) \in \Gamma_0(N)$, aleshores γ pertany al nucli de $\pi_{0,N}$, si i només si, $d \equiv 1 \equiv ad - bcN \equiv ad \pmod N$, per tant, γ pertany al nucli de $\pi_{0,N}$, si i només si, $a \equiv 1 \pmod N$, si i només si, $\gamma \in \Gamma_1(N)$.

3. Donem per coneguda la fórmula

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

[13] Totes les inclusions són estrictes, excepte per a $N = 1$ on tot són igualtats, i per a $\Gamma_1(2) = \Gamma_0(2)$.

[14] Anomenada *Funció Phi d'Euler*: $\varphi(N) = N \prod_{p \mid N} (1 - \frac{1}{p})$.

Combinant-la amb els apartats anteriors i el *Teorema de Lagrange* [15], tenim:

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

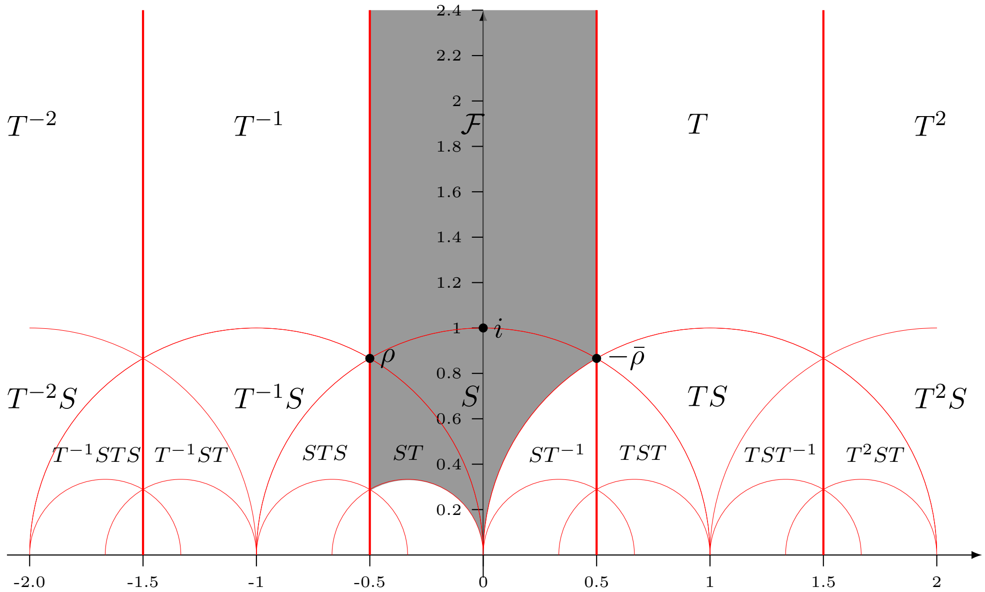
□

Definició 4.6. Sigui Γ un subgrup de congruència. Una funció $f : \mathbb{H} \to \mathbb{C}$ és *feblement modular de pes k respecte* Γ, si és meromorfa en $\mathbb{H}$ i satisfà:

$$f|_k\gamma = f \quad \text{per a tot } \gamma \in \Gamma. \tag{4.1}$$

4.2 Domini Fonamental i Puntes per a Subgrups de Congruència

En la Figura de sota es pot observar el domini fonamental per a $\Gamma_0(2)$, més endavant donarem una explicació a la construcció d'aquest domini. Observem, que a diferència del domini per a $\mathrm{SL}_2(\mathbb{Z})$, la frontera d'aquest conté 2 punts que no pertanyen a $\mathbb{H}$: $i\infty$ i 0.



Proposició 4.7. Sigui $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ un subgrup de congruència. Si existeix un conjunt finit R de representants de les classes laterals del quocient $\Gamma \backslash \mathrm{SL}_2(\mathbb{Z})$,

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{\gamma \in R} \Gamma\gamma,$$

aleshores, el conjunt,

$$\mathcal{F}_\Gamma = \bigcup_{\gamma \in R} \gamma(\mathcal{F})$$

compleix que per a tot $z \in \mathbb{H}$, existeix un $h \in \Gamma$ tal que $hz \in \mathcal{F}_\Gamma$.
Demostració: Sigui $z \in \mathbb{H}$. Utilitzant la Proposició 2.4, existeix un $z' \in \mathcal{F}$ i un $\varsigma \in \mathrm{SL}_2(\mathbb{Z})$,

[15] Siguin $K \subseteq H \subseteq G$ subgrups de G, aleshores $[G : K] = [G : H][H : K]$.

tal que $z = \varsigma z'$. A més, per ser R un conjunt finit de representants de les classes laterals del quocient $\Gamma\backslash\mathrm{SL}_2(\mathbb{Z})$, existeixen $\gamma \in R$ i $h \in \Gamma$, tals que $\varsigma = h^{-1}\gamma$. Tenim:

$$hz = h\varsigma z' = \gamma z' \in \mathcal{F}_\Gamma.$$

□

Definició 4.8. La *recta racional projectiva* és el conjunt $\mathbb{P}^1(\mathbb{Q}) := \mathbb{Q} \cup \{\infty\}$.

A continuació, estenem la definició de la *transformació lineal fraccionària* a la recta racional projectiva.

Per a $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ i $z \in \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, definim la *transformació lineal fraccionària*:

$$\gamma z := \frac{az+b}{cz+d}\ , \tag{4.2}$$

on, per conveni, $\gamma\infty = \frac{a}{c}$, i $\gamma x = \infty$ si $x = \frac{-d}{c}$.

Lema 4.9. $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) = \langle \pm T \rangle$.
Demostració:

$$\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid \frac{a}{c} = \infty \right\} = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \right\} = \langle \pm T \rangle.$$

□

Proposició 4.10. L'acció de $\mathrm{SL}_2(\mathbb{Z})$ en $\mathbb{P}^1(\mathbb{Q})$ és transitiva, en particular, tenim una bijecció

$$\begin{array}{rcl} \phi : \mathrm{SL}_2(\mathbb{Z})/\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) & \longrightarrow & \mathbb{P}^1(\mathbb{Q}) \\ {[\gamma]} & \longmapsto & \gamma\infty\ . \end{array}$$

Demostració: Està ben definida degut a que $\phi(\gamma\gamma') = \gamma\infty$ per a tot $\gamma' \in \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)$
La injectivitat es desprèn veient que si $\gamma_1 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ i $\gamma_2 = \left(\begin{smallmatrix} a & f \\ c & g \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, aleshores $\gamma_3 = \left(\begin{smallmatrix} 1 & df-bg \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)$ compleix $\gamma_1\gamma_3 = \gamma_2$.
Per a l'exhaustivitat, sigui $\frac{a}{c} \in \mathbb{P}^1(\mathbb{Q})$ amb $\mathrm{mcd}(a,c) = 1$, aleshores pel Lema 2.1, l'aplicació és exhaustiva. □

Definició 4.11. Sigui $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ un subgrup de congruència. Definim les *puntes de* Γ com el conjunt de $\Gamma-$òrbites en $\mathbb{P}^1(\mathbb{Q})$:

$$\mathrm{Puntes}(\Gamma) := \Gamma\backslash\mathbb{P}^1(\mathbb{Q}) \cong \Gamma\backslash\mathrm{SL}_2(\mathbb{Z})/\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty).$$

Per tant, $|\mathrm{Puntes}(\Gamma)| \leq [\mathrm{SL}_2(\mathbb{Z}) : \Gamma] < \infty$.

Sigui Γ un subgrup de congruència, sigui $P = \left[\frac{a}{c}\right]$ una punta, i sigui $\gamma_P \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\gamma_P(\infty) = P$.

Lema 4.12. El subgrup $H_P = \gamma_P^{-1}\Gamma\gamma_P \cap \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) \subseteq \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)$ no depèn del representant que escollim per a la punta P, ni de la matriu γ_P que triem. A més, $[\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) : H_P] < \infty$.
Demostració: Sigui $\frac{a'}{c'}$ un altre representant, aleshores existeix un $\gamma \in \Gamma$ tal que $\gamma\left(\frac{a}{c}\right) = \left(\frac{a'}{c'}\right)$, per tant $\gamma\gamma_P(\infty) = \left(\frac{a'}{c'}\right)$. Com $(\gamma\gamma_P)^{-1}\Gamma\gamma\gamma_P = \gamma_P^{-1}\Gamma\gamma_P$, la primera part queda provada.

Per a la segona, notem que per la Proposició 4.10, si γ_P i γ'_P compleixen $\gamma_P(\infty) = \gamma'_P(\infty) = \frac{a}{c}$, aleshores existeix un γ_∞ tal que $\gamma_P\gamma_\infty = \gamma'_P$. Aleshores,

$$(\gamma'_P)^{-1}\Gamma\gamma'_P \cap \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) = (\gamma_P\gamma_\infty)^{-1}\Gamma\gamma_P\gamma_\infty \cap \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)$$

$$= \gamma_\infty^{-1}(\gamma_P^{-1}\Gamma\gamma_P \cap \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty))\gamma_\infty = \gamma_P^{-1}\Gamma\gamma_P \cap \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty).$$

on hem utilitzat que $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)$ és un grup abelià.
Finalment, notem que els únics subgrups de $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ d'índex infinit són $\{0\}$ i $\mathbb{Z}/2\mathbb{Z}$. Clarament H_P no és cap d'aquests dos. $\square$

Lema 4.13. Tot subgrup $H \subseteq \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)$ d'índex finit és un dels següents casos:

- $H = \left\langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \right\rangle$.
- $H = \left\langle \left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right) \right\rangle$.
- $H = \{\pm I_2\} \times \left\langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \right\rangle$.

on $h = [\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) : \{\pm I_2\}H]$
Demostració:
Definim $\overline{H} := H/(H \cap \{\pm I_2\})$ i $\overline{\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)} := \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)/\{\pm I_2\} \cong \mathbb{Z}$.
Clarament,

$$h = [\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) : \{\pm I_2\}H] = [\overline{\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)} : \overline{H}].$$

Per tant $\overline{H} \cong h\mathbb{Z}$.
Prenem un element $g \in H$ tal que $\langle g \rangle = \overline{H}$. L'element g és de la forma $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ o bé $\left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right)$. Aleshores, se'ns presenten tres opcions:

1. Si $-I_2 \in H$, aleshores amb qualsevol dels dos g, $H = \langle -I_2, g \rangle$.
2. Si $-I_2 \notin H$ i $g = \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$, tenim $H = \langle g \rangle$.
3. Si $-I_2 \notin H$ i $g = \left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right)$, tenim $H = \langle g \rangle$.

$\square$

Definició 4.14. Anomenem *amplada de la punta* P *per a* Γ a l'enter $h_\Gamma(P) := h$ aplicant el Lema 4.13 a la matriu H_P, és a dir,

$$h_\Gamma(P) = [\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) : \{\pm I_2\}H_P].$$

És una *punta irregular* si H_P és de la forma $\left\langle \left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right) \right\rangle$, en cas contrari, és una *punta regular*.

Podem observar que en el cas en què $\Gamma \triangleleft \mathrm{SL}_2(\mathbb{Z})$, al complir-se $\gamma^{-1}\Gamma\gamma = \Gamma$ per a tot $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, tenim que totes les puntes tenen la mateixa amplada, i totes són regulars, o bé totes són irregulars.

4.3 Formes Modulars per a Subgrups de Congruència

Finalment, ja ens trobem preparats per definir el concepte de formes modulats en subgrups de congruència. Abans, però, demostrem un lema previ.

Lema 4.15. Sigui $f : \mathbb{H} \to \mathbb{C}$ una funció feblement modular de pes k per a un subgrup de congruència Γ (segons la Definició 4.6), i sigui $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Aleshores $f|_k\gamma$ és una funció feblement modular per a $\gamma^{-1}\Gamma\gamma$.
Demostració: Clarament $f|_k\gamma$ és meromorfa en $\mathbb{H}$. A més, sigui $s = \gamma^{-1}h\gamma \in \gamma^{-1}\Gamma\gamma$ un element qualsevol. Aleshores,

$$(f|_k\gamma)|_k s = f|_k\gamma s = f|_k\gamma\gamma^{-1}h\gamma = (f|_k h)\gamma = f|_k\gamma.$$

□

Sigui $f : \mathbb{H} \to \mathbb{C}$ una funció feblement modular de pes k per a un subgrup de congruència Γ. Sigui $P = \left[\frac{a}{c}\right] \in \mathrm{Puntes}(\Gamma)$, i sigui $\gamma_P \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\gamma_P(\infty) = P$. Pel Lema 4.15, $f|_k\gamma_P$ és feblement modular de pes k per a H_P. Clarament $f|_k\gamma_P$ és periòdica, amb període [16]

$$\tilde{h}_\Gamma(P) = \begin{cases} h_\Gamma(P) & \text{si la punta } P \text{ és regular} \\ 2h_\Gamma(P) & \text{si la punta } P \text{ és irregular} \end{cases}$$

degut a que $f|_k\gamma_P(z) = f|_k\gamma_P\left(\left(\begin{smallmatrix} 1 & \tilde{h}_\Gamma(P) \\ 0 & 1 \end{smallmatrix}\right) z\right) = f|_k\gamma_P(z + \tilde{h}_\Gamma(P))$.

Actuem de forma similar a com vam definir les q-expansions per a formes modulars de $\mathrm{SL}_2(\mathbb{Z})$. Considerem la funció:

$$\begin{array}{rcl} q_P : \mathbb{H} & \longrightarrow & D^* = \{q \in \mathbb{C} \mid 0 < |q| < 1\} \subset \mathbb{C} \\ z & \longmapsto & e^{2\pi i z/\tilde{h}_\Gamma(P)}. \end{array}$$

Convertim la funció $f|_k\gamma_P : \mathbb{H} \to \mathbb{C}$, en $\tilde{f}_P : D^* \to \mathbb{C}$, definint $\tilde{f}_P(q_P) = f|_k\gamma_P(z)$ per a algun $z \in \mathbb{H}$ complint $e^{2\pi i z/\tilde{h}_\Gamma(P)} = q_P$. Aquesta funció està ben definida degut a que si z' també ho compleix, aleshores $z = z' + \tilde{h}_\Gamma(P)n$ per un cert $n \in \mathbb{Z}$. Per tant, $f|_k\gamma_P(z') = f|_k\gamma_P(z + \tilde{h}_\Gamma(P)n) = f|_k\gamma_P(z)$.

El fet que $\lim\limits_{z\to i\infty} f|_k\gamma_P(z) = \lim\limits_{q_P\to 0} \tilde{f}_P(q_P)$ motiva la següent definició.

Definició 4.16. Diem que f és *meromorfa en la punta P* si $\tilde{f}_P$ la podem estendre a una funció meromorfa en el disc unitat. Diem que f és *holomorfa en la punta P* si aquesta continuació meromorfa de $\tilde{f}_P$ és holomorfa en $q = 0$. Diem que f *s'anul·la en la punta P* si $\tilde{f}_P(0) = 0$.

Si f és meromorfa en la punta P, podem expressar $\tilde{f}_P$ localment com una sèrie de Laurent centrada al 0:

$$\tilde{f}_P(q_P) = \sum_{n=M}^{\infty} a_{P,n} q_P^n \text{ amb } a_{P,M} \in \mathbb{C},$$

on $a_{P,n} \neq 0$. Definim *l'ordre de f a la punta P* com $\mathrm{ord}_{\Gamma,P}(f) := M$.

[16] Alguns autors defineixen l'amplada de la punta, com el període $\tilde{h}_\Gamma(P)$.

Definició 4.17. Sigui Γ un subgrup de congruència, i $k \in \mathbb{Z}$. Una *forma modular de pes k per a* Γ és una funció holomorfa $f : \mathbb{H} \to \mathbb{C}$ que és feblement modular de pes k per a Γ i holomorfa en totes les puntes de Γ. Si, a més, f s'anul·la en totes les puntes, aleshores és una *forma cuspidal de pes k per a* Γ.

Intuïtivament, ens podem imaginar que f és holomorfa en totes les puntes com que, per a tot $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, es té,

$$\lim_{z \to i\infty} \frac{1}{(cz+d)^k} f\left(\frac{az+b}{cz+d}\right) \text{ està acotat.}$$

De forma anàloga amb $\mathrm{SL}_2(\mathbb{Z})$ el conjunt de totes les formes modulars de pes k per a Γ també forma un espai vectorial complex.

L'espai de formes modulars de pes k per a un subgrup de congruència Γ el denotem per $M_k(\Gamma)$. *L'espai de formes cuspidals de pes k per a un subgrup de congruència* Γ el denotem per $S_k(\Gamma)$. Més endavant veurem que el $\mathbb{C}$-espai vectorial és de dimensió finita.

Si $\Gamma' \subseteq \Gamma$, el fet que hi hagi una aplicació canónica exhaustiva $\mathrm{Puntes}(\Gamma') \to \mathrm{Puntes}(\Gamma)$, implica que es compleixen les inclusions $M_k(\Gamma) \subseteq M_k(\Gamma')$, així com, $S_k(\Gamma) \subseteq S_k(\Gamma')$. Aquestes inclusions tenen la seva importància en la Teoria d'Atkin-Lehner que veurem més endavant.

A continuació, donem un teorema que ens permet comprovar més ràpidament quan una funció f és una forma modular per a un cert subgrup de congruència.

Teorema 4.18. Sigui $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ un subgrup de congruència i $k \in \mathbb{Z}$. Sigui $f : \mathbb{H} \to \mathbb{C}$ una funció holomorfa, feblement modular de pes k per a Γ. Aleshores són equivalents:

1. $f \in M_k(\Gamma)$.
2. f és holomorfa en l'infinit i existeixen $C > 0$ i $r > 0$, tals que considerant la sèrie de Laurent a l'infinit:
$$\tilde{f}_\infty(q_\infty) = \sum_{n=0}^{\infty} a_{\infty,n} q_\infty^n,$$
es compleix
$$|a_{\infty,n}| < Cn^r \quad \text{per a tot } n > 0.$$

Demostració: Aquest teorema no el demostrem. Per a fer-ho s'utilitzen les sèries d'Eisenstein per a subgrups de congruència. Aquell que estigui interessat pot consultar ([BD16], §6). □

4.4 Fórmula de la València per a Subgrups de Congruència

En aquesta secció donem un resultat anàleg al Teorema 2.25. Ens permet provar que les dimensions dels espais de formes modulars per a subgrups de congruència són de dimensió finita. A més, existeixen fórmules explícites que donen el valor de les respectives dimensions. Calcular aquestes fórmules queda fora de l'objectiu d'aquest treball i no les veurem. Es poden trobar en ([DS05], §3).

Sigui $\overline{\Gamma} := \Gamma/(\Gamma \cap \{\pm I_2\})$. Sigui també

$$\epsilon_{\Gamma,P} = \begin{cases} 1 & \text{si } -I_2 \notin \Gamma \text{ i } P \text{ és regular} \\ 2 & \text{si } -I_2 \in \Gamma \text{ o } P \text{ és irregular} \end{cases}$$

i

$$\bar{\epsilon}_{\Gamma,P} = \begin{cases} 1 & \text{si } P \text{ és regular} \\ 2 & \text{si } P \text{ és irregular} \end{cases}$$

Teorema 4.19. *(Fórmula de la València per a subgrups de congruència)* Sigui Γ un subgrup de congruència. Sigui $f \neq 0$ una funció meromorfa en $\mathbb{H} \cup \infty$, feblement modular de pes k per a Γ. Es compleix:

$$\sum_{z \in \Gamma \backslash \mathbb{H}} \frac{\mathrm{ord}_z f}{\#\mathrm{Stab}_\Gamma(z)} + \sum_{P \in \mathrm{Puntes}(\Gamma)} \frac{\mathrm{ord}_{\Gamma,P} f}{\epsilon_{\Gamma,P}} = \frac{k}{24}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma],$$

així com,

$$\sum_{z \in \Gamma \backslash \mathbb{H}} \frac{\mathrm{ord}_z f}{\#\mathrm{Stab}_{\overline{\Gamma}}(z)} + \sum_{P \in \mathrm{Puntes}(\Gamma)} \frac{\mathrm{ord}_{\Gamma,P} f}{\bar{\epsilon}_{\Gamma,P}} = \frac{k}{12}[\mathrm{PSL}_2(\mathbb{Z}) : \bar{\Gamma}],$$

on $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\}$.
Demostració: S'utilitzen arguments semblants a la de la Fórmula de la València per a $\mathrm{SL}_2(\mathbb{Z})$. En aquest treball no la demostrem. $\square$

Seguidament, abans de concloure la secció, donem tres resultats bàsics que es desprenen de forma immediata del Teorema 4.19.

Corol·lari 4.20. Sigui $k < 0$ i sigui $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ un subgrup de congruència qualsevol, aleshores $M_k(\Gamma) = \{0\}$.

Demostració: És immediat, veient que la part esquerra de la Fórmula de la València per a subgrups de congruència mai pot ser negativa. $\square$

Corol·lari 4.21. Siguin f i $g \in M_k(\Gamma)$, amb q-expansions $\sum_{n \geq 0} a_{P,n} q_P^n$ i $\sum_{n \geq 0} b_{P,n} q_P^n$ en una certa punta P. Suposem que

$$a_j = b_j \quad \text{per a tot } j \in \left\{0, 1, ..., \left\lfloor \frac{k}{24} \epsilon_{\Gamma,P} [\mathrm{SL}_2(\mathbb{Z}) : \Gamma] \right\rfloor \right\}.$$

Aleshores $f = g$.
Demostració: Suposem $f - g \neq 0$. Per hipòtesi, tenim $\mathrm{ord}_{\Gamma,P}(f-g) \geq \left\lfloor \frac{k}{24} \epsilon_{\Gamma,P}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] \right\rfloor + 1 > \frac{k}{24} \epsilon_{\Gamma,P}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$, contradient la Fórmula de la València per a subgrups de congruència. Per tant, $f = g$. $\square$

Corol·lari 4.22. Sigui $k < 0$ i sigui $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ un subgrup de congruència qualsevol, es compleix $\dim(M_k(\Gamma)) < \infty$. En particular, tenim la fita

$$\dim M_k(\Gamma) \leq 1 + \left\lfloor \frac{k}{24} 2[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] \right\rfloor.$$

Demostració: Sigui $n = \left\lfloor \frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] \right\rfloor$.
Pel Corol·lari 4.21, l'aplicació $M_k(\Gamma) \to \mathbb{C}^{n+1}$ que envia f a els seus $(n+1)$-èssims primers coeficients de la q-expansió en una punta P qualsevol, és injectiva. Per tant, $\dim(M_k(\Gamma)) \leq n + 1$. $\square$

4.5 Operadors de Hecke per a $M_k(\Gamma_0(N))$

A partir d'aquest punt ens centrem en subgrups de congruència de la forma $\Gamma_0(N)$.

El concepte d'operador de Hecke per a $M_k(\mathrm{SL}_2(\mathbb{Z}))$ es pot generalitzar per a subgrups de congruència. La construcció dels operadors de Hecke per a $M_k(\Gamma_0(N))$ involucra una construcció semblant a aquella utilitzada per a $\mathrm{SL}_2(\mathbb{Z})$. La principal diferència és que es treballa amb parells (Λ, C), on Λ és un reticle i C és un subgrup cíclic de $\mathbb{C}/\Lambda$ d'ordre N. Donat que la teoria és pràcticament anàloga no detallem el seu contingut i ens limitem a enunciar una sèrie de resultats. Aquell que estigui interessat en un estudi més detallat pot consultar ([Kna92], §IX.6).

Definim,

$$M_2^n(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2^n(\mathbb{Z}) \mid c \equiv 0 \pmod N,\ \mathrm{mcd}(a, N) = 1 \right\},$$

on, recordem, $M_2^n(\mathbb{Z})$ és el conjunt de les matrius amb coeficients enters i determinant n.

Lema 4.23. Les següents matrius:

$$\left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in M_2^n(N) \mid ad = n,\ d > 0,\ 0 \le b < d \right\},$$

formen un conjunt complet de representats de les classes laterals (per la dreta) de l'acció de $\Gamma_0(N)$ en $M_2^n(N)$.

Proposició 4.24. Sigui $\{\gamma_1, ..., \gamma_{s_n}\}$ un conjunt complet de representats de les classes laterals (per la dreta) de l'acció de $\Gamma_0(N)$ en $M_2^n(N)$. Aleshores, donat $f \in M_k(\Gamma_0(N))$, definim *l'operador de Hecke en* $M_k(\Gamma_0(N))$ com:

$$T_n f = \sum_{i=1}^{s_n} f|_k \gamma_i \ ,$$

on $f|_k\gamma_i$ denota l'operador barra de pes k definit a la Proposició 2.6. A més, també tenim $T_n f \in M_k(\Gamma_0(N))$, i la seva restricció a $S_k(\Gamma_0(N))$ també es manté en ella mateixa.

Seguidament, donem el resultat anàleg al Teorema 3.11. Cal destacar, que l'única diferència amb aquest és que diferenciem quan un primer p divideix N.

Teorema 4.25. Sigui $f \in M_k(\Gamma_0(N))$. Aleshores es compleix:

(1) $T_m T_n f = T_{mn} f$	per a m i n enters positius coprimers,
(2) $T_p T_{p^r} f = T_{p^{r+1}} f + p^{k-1} T_{p^{r-1}} f$	per a tot $r > 0$ enter i p primer tal que $p \nmid N$,
(3) $T_{p^r} f = (T_p)^r f$	per a tot $r > 0$ enter i p primer tal que $p \mid N$.

4.6 Producte Escalar de Petersson per a $S_k(\Gamma_0(N))$

Definim el *producte escalar de Petersson per a* $S_k(\Gamma_0(N))$, com:

$$\langle f, g \rangle_{\Gamma_0(N)} = \int_{\mathcal{F}_{\Gamma_0(N)}} f(z) \overline{g(z)} y^k \frac{dx\ dy}{y^2},$$

on $z = x+iy$, $\mathcal{F}_{\Gamma_0(N)}$ és un domini fonamental de $\Gamma_0(N)$ i $\overline{g(z)}$ denota el conjugat complex.

De forma anàloga al que hem vist per a $\mathrm{SL}_2(\mathbb{Z})$ es pot demostrar que està ben definit (convergeix i no depèn del domini fonamental escollit) i que és un producte escalar. En particular, $(S_k(\Gamma_0(N)), \langle\cdot,\cdot\rangle_{\Gamma_0(N)})$ és un espai de Hilbert.

El següent teorema és l'equivalent del Teorema 3.17 i ens dona condicions suficients per garantir que els operadors de Hecke són autoadjunts respecte al producte escalar de Petersson.

Teorema 4.26. Sigui n un enter positiu, complint $\mathrm{mcd}(n, N) = 1$, aleshores els operadors de Hecke T_n per a $S_k(\Gamma_0(N))$ són autoadjunts respecte al producte escalar de Petersson, és a dir,

$$\langle T_n f, g\rangle_{\Gamma_0(N)} = \langle f, T_n g\rangle_{\Gamma_0(N)},$$

per a tot f i g pertanyents a $S_k(\Gamma_0(N))$.

Seguidament, donem un resultat equivalent a la Proposició 3.21.

Proposició 4.27. Sigui $f \in S_k(\Gamma_0(N))$ una forma pròpia, és a dir, un vector propi simultani per a tots els operadors de Hecke T_n. Per tant, compleix $T_n f = \lambda_n f$. Aleshores, si $f(z) = \sum_{n=1}^{\infty} c_n q^n$, és la q-expansió de f en l'infinit, es compleix:

$$c_n = \lambda_n c_1,$$

i, per tant, si $f \neq 0$, es té $c_1 \neq 0$.

Corol·lari 4.28. Sigui $f \in S_k(\Gamma_0(N))$ la mateixa de la Proposició 4.27. Si a més, està normalitzada, és a dir, el coeficient que acompanya a q és 1, podem aplicar la Proposició 4.27 i el Teorema 4.25 per deduir el següent resultat:

$$\begin{array}{ll} c_p c_{p^r} = c_{p^{r+1}} + p^{k-1} c_{p^{r-1}} & \text{per a tot } r > 0 \text{ enter i } p \text{ primer tal que } p \nmid N, \\ c_{p^r} = (c_p)^r & \text{per a tot } r > 0 \text{ enter i } p \text{ primer tal que } p \mid N, \\ c_m c_n = c_{mn} & \text{per a } m \text{ i } n \text{ enters positius coprimers,} \end{array}$$

on $f(z) = \displaystyle\sum_{n=1}^{\infty} c_n q^n$ és la q-expansió de f a l'infinit.

4.7 Teoria d'Atkin-Lehner

Seguidament, donem una sèrie de resultats teòrics que ens ajudaran posteriorment a calcular bases d'espais de formes modulars. Abans però, demostrem un lema previ.

Lema 4.29. Siguin M, N i d nombres naturals positius tals que $M \mid N$ i $d \mid \frac{N}{M}$. Aleshores, per a $\alpha = \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{Q})$, tenim:

$$\Gamma_0(N) \subseteq \Gamma_0(M) \cap \alpha^{-1}\Gamma_0(M)\alpha,$$

i per tant, $\Gamma_0(M) \cap \alpha^{-1}\Gamma_0(M)\alpha$ és un subgrup de congruència.
Demostració: Sigui $\gamma_N = \left(\begin{smallmatrix} a & b \\ cN & e \end{smallmatrix}\right) \in \Gamma_0(N)$. Aleshores,

$$\gamma_N = \left(\begin{smallmatrix} a & b \\ ckdM & e \end{smallmatrix}\right) \text{ per a un cert } k \geq 1 \text{ natural }.$$

Si definim $\gamma_M = \left(\begin{smallmatrix} a & bd \\ ckM & e \end{smallmatrix}\right)$, clarament $\gamma_N = \alpha^{-1}\gamma_M\alpha$. $\square$

Siguin $\Gamma' \subseteq \Gamma$ subgrups de congruència. Per a tot $k \in \mathbb{Z}$, tenim la inclusió natural:

$$\begin{array}{ccc} S_k(\Gamma) & \longrightarrow & S_k(\Gamma') \\ f & \longmapsto & f \end{array}.$$

A més, si definim $\hat{\Gamma} = \Gamma \cap \alpha^{-1}\Gamma\alpha$, per a un cert $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, obtenim la següent inclusió:

$$\begin{array}{ccc} S_k(\Gamma) & \longrightarrow & S_k(\hat{\Gamma}) \\ f & \longmapsto & f|_k\alpha \end{array},$$

sempre que $\hat{\Gamma}$ sigui un subgrup de congruència.

Estem interessats en el cas $\alpha = \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)$, veiem que en aquesta situació $(f|_k\alpha)(z) = d^k f(dz)$ per a tot $f \in M_k(\Gamma)$. Aquest fet ens permet definir l'espai de formes velles.

Definició 4.30. Per a $N \geq 1$ i $k \in \mathbb{Z}$, definim l'*espai de formes velles* i el denotem per $S_k(\Gamma_0(N))^{\mathrm{old}}$ al subespai lineal de $S_k(\Gamma_0(N))$ generat per les imatges de les següents aplicacions:

$$\begin{array}{rcl} \beta_d^{M,N} : S_k(\Gamma_0(M)) & \longrightarrow & S_k(\Gamma_0(N)) \\ f & \longmapsto & (z \mapsto f(dz)) \end{array},$$

per a tot d i $M \neq N$ naturals positius, tals que $M \mid N$ i $d \mid \frac{N}{M}$.

L'*espai de formes noves* és el complement ortogonal respecte el producte escalar de Petersson, el denotem per $S_k(\Gamma_0(N))^{\mathrm{new}}$:

$$S_k(\Gamma_0(N))^{\mathrm{new}} = \{f \in S_k(\Gamma_0(N)) \mid \langle f, g\rangle_{\Gamma_0(N)} = 0 \text{ per a tot } g \in S_k(\Gamma_0(N))^{\mathrm{old}}\}.$$

Notem que en particular:

$$S_k(\Gamma_0(N)) = S_k(\Gamma_0(N))^{\mathrm{new}} \oplus S_k(\Gamma_0(N))^{\mathrm{old}}.$$

A més, tant l'espai de formes velles com l'espai de formes noves són estables sota l'acció dels operadors de Hecke, es a dir, $T_n f \in S_k(\Gamma_0(N))^{\mathrm{new}}$, per a $f \in S_k(\Gamma_0(N))^{\mathrm{new}}$ i respectivament per a $S_k(\Gamma_0(N))^{\mathrm{old}}$. Una demostració més general és pot trobar en ([Mas15], §4).

Finalment, enunciem dos resultats fonamentals de la teoria d'Atkin i Lehner.

Teorema 4.31. Per a $N \geq 1$ natural, i per a $k \in \mathbb{Z}$. Tenim la següent descomposició que ens permet descriure $S_k(\Gamma_0(N))$ a partir de les formes que acabem de definir:

$$S_k(\Gamma_0(N)) = \bigoplus_{M|N,\ d|\frac{N}{M}} \beta_d^{M,N}(S_k(\Gamma_0(M))^{\mathrm{new}}),$$

on només considerem M i d positius.

Teorema 4.32. Sigui $N \geq 1$, aleshores $S_k(\Gamma_0(N))^{\mathrm{new}}$ té una base formada per vectors propis de tot T_p, on $p \nmid N$.

La demostració es pot trobar en ([AL70]).

No aprofundim més en aquest apartat, aquell que estigui interessat en continuar estudiant pot trobar fàcilment dins de la literatura matemàtica la continuació a aquests apunts.

Una bona forma de continuar seria estudiant la teoria d'operadors de Hecke per a subgrups de congruència en general (en aquest treball només hem treballat amb subgrups $\Gamma_0(N)$). Les funcions L definides a partir de la q-expansió de les formes modulars també formen part d'una branca de la teoria molt interessant que podria ser una bona continuació pel lector. A partir d'aquestes es pot enunciar el teorema de modularitat que relaciona corbes el·líptiques amb formes modulars, i que va permetre demostrar l'Últim Teorema de Fermat.

Seguidament, en aquest treball, introduïm uns conceptes que ens ajudaran a estudiar computacionalment tots els coneixements que hem introduït fins ara.

5 Símbols Modulars

Utilitzant la base d'Eisenstein definida al Teorema 2.30 podem calcular els espais M_k d'una forma relativament senzilla. En aquesta secció voldrem calcular els espais $S_k(\Gamma_0(N))$. Per a portar a terme aquest fet, utilitzarem el concepte de símbol modular.

5.1 Símbols Modulars

Recordem que tal com està explicat a la fórmula (4.2) podem estendre la transformació lineal fraccionària a $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. Denotem per $X_0(N)$ al quocient $\Gamma_0(N)\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))$ que té estructura de superfície de Riemann compacta i orientable ([DS05]). Pel Teorema de Classificació de Superfícies Compactes, $X_0(N)$ es una suma connexa de g-tors.

Hi ha diverses definicions de símbols modulars. Es poden definir com funcions a valors complexos $m : \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \to \mathbb{C}$ complint certes propietats. Tot i així, en aquest treball donem una definció essencialment equivalent.

Definició 5.1. Sigui $\mathbb{M}_2$ el grup abelià lliure generat pel conjunt de símbols $\{\alpha, \beta\}$ amb $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, mòdul la relació

$$\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \beta\} = 0,$$

i mòdul qualsevol torsió.
En particular, es compleix $\{\alpha, \alpha\} = 0$ i $\{\alpha, \beta\} = -\{\beta, \alpha\}$ per a tot $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$.

Ens podem imaginar cada símbol $\{\alpha, \beta\}$ com un camí entre α i β en $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, tal com il·lustra la imatge de sota.

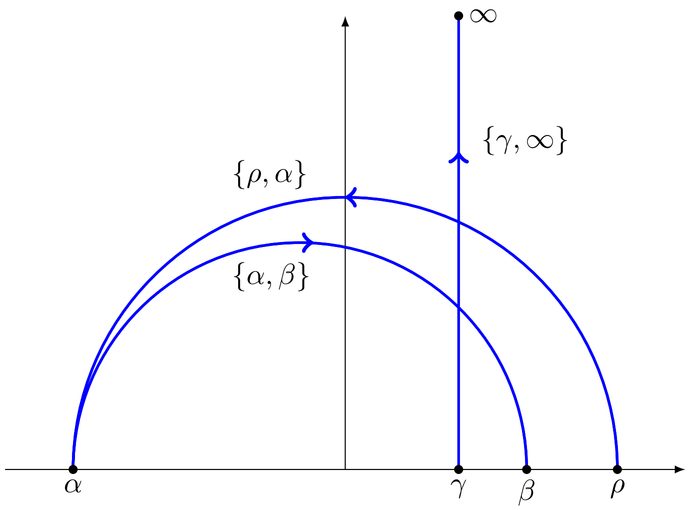


Figura 2

A més, podem definir una acció per l'esquerra de $\mathrm{GL}_2(\mathbb{Q})$ en $\mathbb{M}_2$ simplement per

$$g\{\alpha, \beta\} = \{g\alpha, g\beta\},$$

per a tot $g \in \mathrm{GL}_2(\mathbb{Q})$ i $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, on $g\alpha$ denota la transformació lineal fraccionària de (4.2).

Definició 5.2. L'espai $\mathbb{M}_2(\Gamma_0(N))$ de *símbols modulars per a* $\Gamma_0(N)$ és el quocient de $\mathbb{M}_2$ pel subgrup generat pels elements $\{\alpha,\beta\} - g\{\alpha,\beta\}$ per a tot $g \in \Gamma_0(N)$ i $\alpha,\beta \in \mathbb{P}^1(\mathbb{Q})$ i mòdul qualsevol torsió.

Definició 5.3. L'espai $\mathbb{B}_2(\Gamma_0(N))$ del *conjunt de vores per a* $\Gamma_0(N)$ és el grup abelià lliure generat per les puntes de $\Gamma_0(N)$ tal com es van definir en (4.11). Denotem per $\{\alpha\}$ amb $\alpha \in \mathbb{P}^1(\mathbb{Q})$ a cada generador de $\mathbb{B}_2(\Gamma_0(N))$.

Definició 5.4. La *funció vora* és el següent morfisme:

$$\begin{array}{rcl} \delta : \mathbb{M}_2(\Gamma_0(N)) & \longrightarrow & \mathbb{B}_2(\Gamma_0(N)) \\ \{\alpha,\beta\} & \longmapsto & \{\beta\} - \{\alpha\}\ . \end{array}$$

El nucli de δ el denotem per $\mathbb{S}_2(\Gamma_0(N))$ i l'anomenem *símbols modulars cuspidals.*

Intuïtivament ens podem imaginar cada símbol $\{\alpha,\beta\} \in \mathbb{S}_2(\Gamma_0(N))$ com una combinació lineal de camins en $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ tals que formen camins tancats en $X_0(N)$. Aquest fet motiva el següent teorema que no demostrem ([Man72],§1.9).

Teorema 5.5. (Manin) Es compleix:

$$\mathbb{S}_2(\Gamma_0(N)) \cong \mathrm{H}_1(X_0(N),\mathbb{Z}),$$

on $\mathrm{H}_1(X_0(N),\mathbb{Z})$ denota el grup d'homologia singular de $X_0(N)$.

Proposició 5.6. Tenim:

$$\dim_{\mathbb{C}}(\mathbb{S}_2(\Gamma_0(N)) \otimes_{\mathbb{Z}} \mathbb{C}) = 2\dim_{\mathbb{C}} S_2(\Gamma_0(N)).$$

Demostració: Recordem que $X_0(N) = \Gamma_0(N)\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))$ és una suma connexa de g-tors. Un resultat que no hem vist en el treball ens diu $\dim_{\mathbb{C}} S_2(\Gamma_0(N)) = g$. Aleshores, utilitzant el Teorema anterior i el fet de que $\mathrm{H}_1(X_0(N),\mathbb{Z}) \cong \mathbb{Z}^{2g}$, queda demostrat. □

Una de les principals característiques dels símbols modulars és que són calculables. En la següent secció estudiem aquest fet.

5.2 Càlcul de Símbols Modulars

Aquest apartat està basat en el treball del matemàtic rus Yuri Manin que va desenvolupar les idees que presentem.

Definició 5.7. La *recta projectiva sobre* $\mathbb{Z}/N\mathbb{Z}$ és:

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) = \{(x:y) \in (\mathbb{Z}/N\mathbb{Z})^2 \mid \mathrm{mcd}(x,y,N) = 1\}/\sim\ ,$$

on $(x:y) \sim (x':y')$ si i només si existeix un $u \in (\mathbb{Z}/N\mathbb{Z})^\times$ tal que $x' = ux$ i $y' = uy$.

D'altra banda, usant el Lema 4.5 podem expressar $\mathrm{SL}_2(\mathbb{Z})$ com la següent unió disjunta:

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{i=0}^{m} \Gamma_0(N) r_i\ ,$$

on $\{r_0,\ldots,r_m\}$ són els representants de les classes laterals per la dreta.

Abans de relacionar aquests dos conceptes que acabem de veure, demostrem un lema previ que ens ajudarà més endavant.

Lema 5.8. Per a $i = 1, 2$, sigui $\gamma_i = \left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Són equivalents:

1. γ_1 i γ_2 pertanyen a la mateixa classe lateral per la dreta de $\Gamma_0(N)$.

2. Existeix un u amb $\mathrm{mcd}(u, N) = 1$ tal que $c_1 \equiv uc_2$ i $d_1 \equiv ud_2 \pmod{N}$.

Demostració: Un càlcul ràpid ens dona,

$$\gamma_1\gamma_2^{-1} = \left(\begin{smallmatrix} a_1d_2-b_1c_2 & b_1a_2-a_1b_2 \\ c_1d_2-d_1c_2 & a_2d_1-b_2c_1 \end{smallmatrix}\right),$$

per tant $\gamma_1\gamma_2^{-1} \in \Gamma_0(N)$ si i només si $c_1d_2 - d_1c_2 \equiv 0 \pmod{N}$.
($1 \Rightarrow 2$) Prenent $u = a_2d_1 - b_2c_1$ clarament $\mathrm{mcd}(u, N) = 1$ (ja que $\det(\gamma_1\gamma_2^{-1}) = 1$). Obtenim,

$$uc_2 = a_2d_1c_2 - b_2c_1c_2 \equiv a_2d_2c_1 - b_2c_2c_1 \equiv c_1 \pmod{N},$$

i

$$ud_2 = a_2d_1d_2 - b_2c_1d_2 \equiv a_2d_1d_2 - b_2c_2d_1 \equiv d_1 \pmod{N}.$$

($2 \Rightarrow 1$) Si existeix un u amb $\mathrm{mcd}(u, N) = 1$ tal que $c_1 \equiv uc_2$ i $d_1 \equiv ud_2 \pmod{N}$, clarament $c_1d_2 - d_1c_2 \equiv 0 \pmod{N}$. □

Una vegada vist el Lema ja podem enunciar la següent proposició.

Proposició 5.9. Hi ha una bijecció entre $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ i les classes laterals de $\Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z})$ donada per:

$$\begin{array}{ccc} \Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z}) & \longrightarrow & \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) & \longmapsto & (c : d)\ . \end{array}$$

Demostració: Clarament l'aplicació és bijectiva, ja que donat $(c : d) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ podem construir un element de $\mathrm{SL}_2(\mathbb{Z})$, usant per exemple el Lema 2.1. L'aplicació és injectiva i està ben definida pel Lema anterior. □

Seguidament, donem el resultat clau que permet calcular $\mathbb{M}_2(\Gamma_0(N))$. Aquest ens diu que qualsevol element $\{\alpha, \beta\} \in \mathbb{M}_2(\Gamma_0(N))$ es pot expressar com una combinació lineal amb coeficients a $\mathbb{Z}$ dels símbols $r_i\{0, \infty\}$, on r_i són les classes laterals de $\Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z})$. En particular, $\mathbb{M}_2(\Gamma_0(N))$ està generat per un nombre finit de símbols.

Proposició 5.10. Siguin $r_0, \ldots, r_m$ els representants de les classes laterals per la dreta de $\Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z})$. Sigui $\{\alpha, \beta\} \in \mathbb{M}_2(\Gamma_0(N))$ un element qualsevol, aleshores existeixen $\lambda_0, \ldots, \lambda_m \in \mathbb{Z}$ tals que:

$$\{\alpha, \beta\} = \sum_{i=0}^{m} \lambda_i r_i\{0, \infty\}.$$

Demostració: Donat que

$$\{\alpha, \beta\} = \{\alpha, \infty\} - \{\beta, \infty\},$$

és suficient considerar només el cas $\{\alpha, \infty\}$ on $\alpha = \frac{a}{b} \in \mathbb{P}^1(\mathbb{Q})$.
Trobarem $\alpha' = \frac{a'}{b'} \in \mathbb{P}^1(\mathbb{Q})$ tal que $a'b - ab' = 1$, $b' < b$ i tal que

$$\{\frac{a}{b}, \infty\} = \{\frac{a}{b}, \frac{a'}{b'}\} + \{\frac{a'}{b'}, \infty\}.$$

Ja que en aquest cas,

$$\{\frac{a}{b},\infty\} = \left(\begin{smallmatrix} a' & a \\ b' & b \end{smallmatrix}\right)\{0,\infty\} + \{\frac{a'}{b'},\infty\} = r_i\{0,\infty\} + \{\frac{a'}{b'},\infty\},$$

per a una certa classe lateral r_i. Donat que $b' < b$, per un argument recursiu podem concloure la demostració.
Per a trobar $\alpha' = \frac{a'}{b'} \in \mathbb{P}^1(\mathbb{Q})$ simplement prenem $b' \in \mathbb{Z}$ tal que $|b'| \le \frac{b}{2}$ i tal que

$$b'a \equiv 1 \pmod b.$$

Finalment, prenem $a' \in \mathbb{Z}$ tal que $a'b - ab' = 1$. □

Acabem de veure que el conjunt dels representants de les classes laterals de $\Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z})$ generen $\mathbb{M}_2(\Gamma_0(N))$. Tot i així, encara podem reduir més el nombre de generadors ja que es poden establir algunes relacions lineals entre aquests. Per a poder estudiar en detall aquestes relacions definim els símbols de Manin.

Tal com hem vist a la Proposició 2.4, $\mathrm{SL}_2(\mathbb{Z})$ està generat per $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ i $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Definim

$$\sigma = S, \quad \tau = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right) = TS,$$

que compleixen $\sigma\{0,\infty\} = \{\infty,0\}$, $\tau\{0,\infty\} = \{\infty,1\}$ i $\tau\{\infty,1\} = \{1,0\}$.

Definició 5.11. Siguin $r_0,\dots,r_m$ representants de les classes laterals de $\Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z})$. Anomenem *símbols de Manin* al conjunt formal de símbols $[r_i]$ per a $i = 0,\dots,m$. Equipem aquests símbols amb una acció per la dreta de $\mathrm{SL}_2(\mathbb{Z})$, definint $[r_i]\gamma = [r_j]$ si i només si $\Gamma_0(N)r_j = \Gamma_0(N)r_i\gamma$.

Denotem per M al quocient del grup abelià lliure generat pels símbols de Manin per el subgrup generat per

$$\begin{array}{ll} [r_i] + [r_i]\sigma & \text{per a tot } i \in \{0,\dots,m\}, \\ [r_i] + [r_i]\tau + [r_i]\tau^2 & \text{per a tot } i \in \{0,\dots,m\}. \end{array} \tag{5.1}$$

i mòdul qualsevol torsió.

Teorema 5.12. Hi ha un isomorfisme de grups donat per:

$$\begin{array}{rcl} \psi : M & \longrightarrow & \mathbb{M}_2(\Gamma_0(N)) \\ [r_i] & \longmapsto & r_i\{0,\infty\}\ . \end{array}$$

Demostració: L'aplicació és exhaustiva per la Proposició 5.10. A més, clarament està ben definida donat que

$$\psi([r_i] + [r_i]\sigma) = r_i\{0,\infty\} + r_i\sigma\{0,\infty\} = r_i\{0,\infty\} + r_i\{\infty,0\} = 0,$$

i

$$\psi([r_i]+[r_i]\tau+[r_i]\tau^2) = r_i\{0,\infty\}+r_i\tau\{0,\infty\}+r_i\tau^2\{0,\infty\} = r_i\{0,\infty\}+r_i\{\infty,1\}+r_i\{1,0\} = 0.$$

La injectivitat es pot trobar en ([Man72], §1.7). □

Observem que les relacions de (5.1) són fàcils de calcular i ens permeten establir relacions entre els diferents símbols modulars $r_0\{0,\infty\},\dots,r_m\{0,\infty\}$. Anomenem *base de Manin* a un conjunt de símbols de Manin linealment independents que generi $\mathbb{M}_2(\Gamma_0(N))$. Notem que qualsevol element de $\mathbb{M}_2(\Gamma_0(N))$ es pot posar com a combinació lineal amb coeficients enters dels elements de la base.

5.3 Operadors de Hecke en Símbols Modulars

De la mateixa manera que hem definit els operadors de Hecke en formes modulars, en aquesta secció veurem que també podem definir uns operadors semblants sobre els símbols modulars. A més, tal com observarem, estan molt relacionats, cosa que ens permetrà extreure informació dels operadors de Hecke en formes modulars a partir dels que definirem a continuació.

Definició 5.13. Per a $\{\alpha, \beta\} \in \mathbb{M}_2(\Gamma_0(N))$, definim l'*operador de Hecke en símbols modulars* de la següent manera:

$$T_p(\{\alpha,\beta\}) = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\{\alpha,\beta\} + \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\{\alpha,\beta\} + \left(\begin{smallmatrix} 1 & 1 \\ 0 & p \end{smallmatrix}\right)\{\alpha,\beta\} + \ldots + \begin{pmatrix} 1 & p-1 \\ 0 & p \end{pmatrix}\{\alpha,\beta\} \qquad \text{si } p \nmid N,$$
$$T_p(\{\alpha,\beta\}) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\{\alpha,\beta\} + \left(\begin{smallmatrix} 1 & 1 \\ 0 & p \end{smallmatrix}\right)\{\alpha,\beta\} + \ldots + \begin{pmatrix} 1 & p-1 \\ 0 & p \end{pmatrix}\{\alpha,\beta\} \qquad \text{si } p \mid N.$$

Si veiem els símbols modulars com els camins que hem exemplificat a la Figura 2, ens trobem amb el següent resultat.

Teorema 5.14. El següent aparellament

$$\begin{aligned} \langle \cdot, \cdot \rangle : S_2(\Gamma_0(N)) \times \mathbb{S}_2(\Gamma_0(N)) &\longrightarrow \mathbb{C} \\ (f, \{\alpha,\beta\}) &\longmapsto 2\pi i \int_\alpha^\beta f(z)dz\ , \end{aligned}$$

és nodegenerat i Hecke-equivariant, és a dir, $\langle T_p f, \{\alpha,\beta\}\rangle = \langle f, T_p(\{\alpha,\beta\})\rangle$.
Demostració: Clarament l'aparellament és una forma bilineal. Per a provar que és Hecke-equivariant, notem que usant el Lema 4.23 i la Proposició 4.24, per a $f \in S_2(\Gamma_0(N))$, tenim:

$$T_p f = p\left(f\left(\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)z\right) + f\left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)z\right)\frac{1}{p^2} + f\left(\left(\begin{smallmatrix} 1 & 1 \\ 0 & p \end{smallmatrix}\right)z\right)\frac{1}{p^2} + \ldots + f\left(\begin{pmatrix} 1 & p-1 \\ 0 & p \end{pmatrix}z\right)\frac{1}{p^2}\right) \qquad \text{si } p \nmid N,$$
$$T_p f = p\left(f\left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)z\right)\frac{1}{p^2} + f\left(\left(\begin{smallmatrix} 1 & 1 \\ 0 & p \end{smallmatrix}\right)z\right)\frac{1}{p^2} + \ldots + f\left(\begin{pmatrix} 1 & p-1 \\ 0 & p \end{pmatrix}z\right)\frac{1}{p^2}\right) \qquad \text{si } p \mid N.$$

Aleshores, per a $p \nmid N$, simplement aplicant canvis de variable obtenim:

$$\langle T_p f, \{\alpha,\beta\}\rangle = 2\pi i \int_\alpha^\beta T_p f(z)dz$$

$$= 2\pi i\left(\int_\alpha^\beta pf(pz)dz + \int_\alpha^\beta \frac{1}{p}f\left(\frac{z}{p}\right)dz + \int_\alpha^\beta \frac{1}{p}f\left(\frac{z+1}{p}\right)dz + \ldots + \int_\alpha^\beta \frac{1}{p}f\left(\frac{z+p-1}{p}\right)dz\right)$$
$$= 2\pi i\left(\int_{p\alpha}^{p\beta} f(z)dz + \int_{\frac{\alpha}{p}}^{\frac{\beta}{p}} f(z) + \int_{\frac{\alpha+1}{p}}^{\frac{\beta+1}{p}} f(z)dz + \ldots + \int_{\frac{\alpha+p-1}{p}}^{\frac{\beta+p-1}{p}} f(z)dz\right) = \langle f, T_p(\{\alpha,\beta\})\rangle.$$

Anàlogament per a $p \mid N$.
La demostració de que és nodegenerat és més complexa i no la veurem, és un cas particular dels resultats de ([Ste07], §8.5). □

El Teorema anterior ens permet relacionar els operadors de Hecke en formes modulars amb aquests definits en els símbols modulars. En particular, els valors propis coincideixen. En el següent apartat veurem com és relativament fàcil calcular aquests valors propis.

5.4 Símbols Modulars amb SAGE

En aquesta secció implementem alguns dels resultats que hem demostrat anteriorment. Per a portar-ho a terme, utilitzem un software lliure anomenat *SageMath* força utilitzat entre aquelles persones que investiguen en l'àmbit de la teoria de nombres.

Com hem vist al Teorema 2.30, l'espai M_k de formes modulars per a $\mathrm{SL}_2(\mathbb{Z})$ admet com a base $\{E_4^a E_6^b \mid a \geq 0,\ b \geq 0,\ 4a + 6b = k\}$. Les sèries d'Eisenstein venen donades en SAGE amb la següent comanda:

```
sage: E4=eisenstein_series_qexp(4,7); E4
1/240 + q + 9*q^2 + 28*q^3 + 73*q^4 + 126*q^5 + 252*q^6 + O(q^7)
sage: E6=eisenstein_series_qexp(6,7); E6
-1/504 + q + 33*q^2 + 244*q^3 + 1057*q^4 + 3126*q^5 + 8052*q^6 + O(q^7)
```

SAGE per defecte treballa amb $\mathbb{M}_2(\Gamma_0(N)) \otimes_{\mathbb{Z}} \mathbb{Q}$, que es tracta d'un $\mathbb{Q}$-espai vectorial. A continuació, definim espais de símbols modulars i introduïm comandes de SAGE donant l'exemple per a $N = 17$:

```
sage: G=Gamma0(17); G
Congruence Subgroup Gamma0(17)
sage: M=ModularSymbols(G) ; M
Modular Symbols space of dimension 3 for Gamma_0(17)
of weight 2 with sign 0 over Rational Field
```

Seguidament, veiem com calcular els elements de $\mathbb{P}^1(\mathbb{Z}/17\mathbb{Z})$.

```
sage: M.manin_generators ()
[(0,1), (1,0), (1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (1,7),
 (1,8), (1,9), (1,10), (1,11), (1,12), (1,13), (1,14), (1,15), (1,16)]
```

A continuació, expressem els elements de $\mathbb{P}^1(\mathbb{Z}/17\mathbb{Z})$ com símbols modulars, i viceversa.

```
sage: M((1,14)).modular_symbol_rep()
{-1/14, 0}
sage: ex=sage.modular.modsym.modular_symbols.ModularSymbol(M,0,-1/14,0);ex
{-1/14, 0}
sage: ex.manin_symbol_rep()
-(1,1) - (-14,1)
sage: -M((1,1))-M((-14,1))
(1,14)
```

La següent comanda ens permet expressar cada element de $\mathbb{P}^1(\mathbb{Z}/17\mathbb{Z})$ com una matriu de $\mathrm{SL}_2(\mathbb{Z})$, tal com ho recull la Proposició 5.9.

```
sage: [x.lift_to_sl2z(2) for x in M.manin_generators()]
[[1, 0, 0, 1], [0, -1, 1, 0], [1, 0, 1, 1], [0, -1, 1, 2], [0, -1, 1, 3],
[0, -1, 1, 4], [0, -1, 1, 5], [0, -1, 1, 6], [0, -1, 1, 7], [0, -1, 1, 8],
[0, -1, 1, 9], [0, -1, 1, 10], [0, -1, 1, 11], [0, -1, 1, 12],
[0, -1, 1, 13], [0, -1, 1, 14], [0, -1, 1, 15], [0, -1, 1, 16]]
```

Segons el Teorema 5.12, es poden establir relacions entre els $[r_i]$. SAGE també calcula una base de Manin, així com les relacions entre els r_i.

```
sage: M.basis()
((1,0), (1,14), (1,15))
sage: M.manin_gens_to_basis()
[-1  0  0]
[ 1  0  0]
[ 0  0  0]
[ 0  0  1]
[ 0 -1  1]
[ 0  0  0]
[ 0 -1  1]
[ 0 -1  0]
[ 0 -1  0]
[ 0  0 -1]
[ 0  0 -1]
[ 0  1 -1]
[ 0  1 -1]
[ 0  1  0]
[ 0  0  0]
[ 0  1  0]
[ 0  0  1]
[ 0  0  0]
```

Donat que la nostra base és $(1:0)$, $(1:14)$ i $(1:15)$. Aquesta última taula s'ha d'interpretar com $(0:1) = -(1:0)$ a la primera fila, $(1:1) = 0$ a la tercera, o $(1:3) = -(1:14) + (1:15)$ a la cinquena.

SAGE ens permet escollir si volem treballar amb símbols modulars o amb símbols de Manin (vistos com elements de $\mathbb{P}^1(\mathbb{Z}/17\mathbb{Z})$).

```
sage: set_modsym_print_mode ('modular')
sage: M.basis()
({Infinity, 0}, {-1/14, 0}, {-1/15, 0})
sage: M((8,3))
{-1/14, 0} - {-1/15, 0}
sage: set_modsym_print_mode ('manin')
sage: M.basis()
((1,0), (1,14), (1,15))
sage: M((8,3))
(1,14) - (1,15)
```

Seguidament, veiem com es poden calcular les matrius de Hecke de T_p en $\mathbb{M}_2(\Gamma_0(17))$, per a certs valors de p.

```
sage: M.T(2).matrix()
[ 3  0 -1]
[ 0 -1  0]
```

```
[ 0  0 -1]
sage: M.T(3).matrix()
[ 4  0 -1]
[ 0  0  0]
[ 0  0  0]
sage: M.T(5).matrix()
[ 6  0 -2]
[ 0 -2  0]
[ 0  0 -2]
sage: M.T(7).matrix()
[ 8  0 -1]
[ 0  4  0]
[ 0  0  4]
sage: M.T(11).fcp()
(x - 12) * x^2
```

Notem que per exemple la primera taula ens indica $T_2(\{\infty,0\}) = 3\{\infty,0\} - \{-1/15,0\}$, $T_2(\{-1/14,0\}) = -\{-1/14,0\}$ i $T_2(\{-1/15,0\}) = -\{-1/15,0\}$. A més, M.T(p).fcp() ens escriu el polinomi característic factoritzat.

La funcio M.cusp() ens dona una base de $\mathbb{B}_2(\Gamma_0(17))$. Recordem que hem definit $\mathbb{S}_2(\Gamma_0(N))$ a partir de la funció vora. Aquesta ve donada per:

```
sage: M.cusps()
[Infinity, 0]
sage: M.boundary_map()
Hecke module morphism boundary map defined by the matrix
[ 1 -1]
[ 0  0]
[ 0  0]
Domain: Modular Symbols space of dimension 3 for Gamma_0(17) of weight ...
Codomain: Space of Boundary Modular Symbols
for Congruence Subgroup Gamma0(17) ...
sage: S=M.cuspidal_submodule(); S
Modular Symbols subspace of dimension 2 of Modular Symbols space of
dimension 3 for Gamma_0(17) of weight 2 with sign 0 over Rational Field
```

Observem que a partir de la matriu de la funció vora deduïm que una base de $\mathbb{S}_2(\Gamma_0(17))$ podrien ser el segon i el tercer element de la base de $\mathbb{M}_2(\Gamma_0(17))$. Ho corroborem:

```
sage: S.basis()
((1,14), (1,15))
```

Finalment, per a acabar, donat que per a $\{\alpha,\beta\} \in \mathbb{S}_2(\Gamma_0(N))$, $T_p(\{\alpha,\beta\}) \in \mathbb{S}_2(\Gamma_0(N))$, podem restringir l'acció de Hecke a l'espai dels símbols modulars cuspidals. La matriu ve donada per:

```
sage: S.T(13).matrix()
[-2  0]
[ 0 -2]
```

5.5 Càlcul de $S_2(\Gamma_0(34))$ usant Vectors Propis

En aquesta secció veurem com es pot calcular una base de $S_2(\Gamma_0(N))$ amb SAGE utilitzant la teoria d'Atkin i Lehner. Per a portar-ho a terme estudiem el cas $N = 34$.

Gràcies al Teorema 4.31, per a donar una base de $S_2(\Gamma_0(34))$, és suficient donar una base de $S_2(\Gamma_0(M))^{\text{new}}$, per a tot divisor positiu $M \mid 34$. A més, en virtut del Teorema 4.32, $S_k(\Gamma_0(M))^{\text{new}}$ té una base formada per vectors propis de tot T_p, on $p \nmid N$.

Notem que els únics divisors de 34 són 1, 2, 17 i 34. El següent fet ens permet restingir el nostre estudi als casos $M = 17$ i $M = 34$.

```
sage: dimension_cusp_forms(Gamma0(2),2)
0
sage: dimension_cusp_forms(Gamma0(1),2)
0
```

De la Proposició 4.27 es desprèn que si f és una forma pròpia normalitzada, és a dir, tal que el coeficient que acompanya a q és 1, aleshores:

$$f(z) = \sum_{n=1}^{\infty} \lambda_n q^n, \tag{5.2}$$

on λ_n és el valor propi de f en T_n. A més, el Corol·lari 4.28 ens assegura que

$$\begin{array}{ll} \lambda_p \lambda_{p^r} = \lambda_{p^{r+1}} + p^{k-1}\lambda_{p^{r-1}} & \text{per a tot } r > 0 \text{ enter i } p \text{ primer tal que } p \nmid M, \\ \lambda_{p^r} = (\lambda_p)^r & \text{per a tot } r > 0 \text{ enter i } p \text{ primer tal que } p \mid M, \\ \lambda_m \lambda_n = \lambda_{mn} & \text{per a } m \text{ i } n \text{ enters positius coprimers.} \end{array}$$

Per tant, és suficient calcular λ_p per a p primer, i a través de la fórmula recursiva anterior podem calcular λ_n per a tot $n > 0$. Una vegada calculats, (5.2) ens dona l'element de $S_k(\Gamma_0(M))^{\text{new}}$ desitjat.

Per a $M = 17$, tenim:

```
sage: dimension_new_cusp_forms(Gamma0(17),2)
1
sage: M=ModularSymbols(17,2); S=M.cuspidal_submodule(); S
Modular Symbols subspace of dimension 2 of Modular Symbols space of
dimension 3 for Gamma_0(17) of weight 2 with sign 0 over Rational Field
sage: S.T(2).fcp()
(x + 1)^2
sage: S.T(3).fcp()
x^2
sage: S.T(5).fcp()
(x + 2)^2
sage: S.T(7).fcp()
(x - 4)^2
```

Per tant, concloem que

$$f = q - q^2 - q^4 - 2q^5 + 4q^7 + 3q^8 + \ldots \in S_k(\Gamma_0(17))^{\text{new}} = S_k(\Gamma_0(17)).$$

Usant l'aplicació $\beta_1^{17,34}$ i $\beta_2^{17,34}$ de la Definició 4.30, obtenim

$$f = q - q^2 - q^4 - 2q^5 + 4q^7 + 3q^8 + \ldots \in S_k(\Gamma_0(34)),$$

i

$$f = q^2 - q^4 - q^8 + \ldots \in S_k(\Gamma_0(34)).$$

Finalment, per a calcular $S_k(\Gamma_0(34))^{\text{new}}$, identifiquem el subespai V de $\mathbb{S}_2(\Gamma_0(34))$ que correspon amb $S_k(\Gamma_0(34))^{\text{new}}$. Per a cada divisor positiu propi M de 34, i per a cada divisor positiu d de $\frac{34}{M}$, sigui:

$$\begin{array}{rcl} \phi_{M,d} : \mathbb{S}_2(\Gamma_0(34)) & \longrightarrow & \mathbb{S}_2(\Gamma_0(M)) \\ \{\alpha,\beta\} & \longmapsto & \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)\{\alpha,\beta\}\ , \end{array}$$

aleshores V és la intersecció dels nuclis de totes les aplicacions $\phi_{M,d}$. Utilitzem la següent comanda de SAGE que calcula V:

```
sage: dimension_new_cusp_forms(Gamma0(34),2)
1
sage: M=ModularSymbols(34,2); S=M.cuspidal_submodule(); S
Modular Symbols subspace of dimension 6 of Modular Symbols space of
dimension 9 for Gamma_0(34) of weight 2 with sign 0 over Rational Field
sage: Sn=S.new_submodule(); Sn
Modular Symbols subspace of dimension 2 of Modular Symbols space of
dimension 9 for Gamma_0(34) of weight 2 with sign 0 over Rational Field
sage: Sn.q_expansion_basis()
[
q + q^2 - 2*q^3 + q^4 - 2*q^6 - 4*q^7 + q^8 + O(q^9)
]
```

Comprovem que efectivament es tracta d'una forma nova:

```
sage: dimension_new_cusp_forms(Gamma0(17),2)
1
sage: M=ModularSymbols(17,2); S=M.cuspidal_submodule(); S
Modular Symbols subspace of dimension 2 of Modular Symbols space of
dimension 3 for Gamma_0(17) of weight 2 with sign 0 over Rational Field
sage: Sn.T(2).fcp()
(x - 1)^2
sage: Sn.T(3).fcp()
(x + 2)^2
sage: Sn.T(5).fcp()
x^2
sage: Sn.T(7).fcp()
(x + 4)^2
```

Doncs si, efectivament els valors propis coincideixen amb els coeficients.

Una forma més ràpida de calcular una base en SAGE és de la següent manera:

```
sage: M=ModularSymbols(34,2); S=M.cuspidal_submodule(); S
Modular Symbols subspace of dimension 6 of Modular Symbols space of
dimension 9 for Gamma_0(34) of weight 2 with sign 0 over Rational Field
sage: S.q_expansion_basis(9)
[
q - 2*q^4 - 2*q^5 + 4*q^7 + 2*q^8 + O(q^9),
q^2 - q^4 - q^8 + O(q^9),
q^3 - 2*q^4 - q^5 + q^6 + 4*q^7 + O(q^9)
]
```

Finalment, ens assegurem que tant la base calculada a partir de les formes noves, com la que ha calculat SAGE directament, generen el mateix espai:

```
sage: A=Matrix([[1,0,0,-2,-2,0,4,2],[0,1,0,-1,0,0,0,-1],
[0,0,1,-2,-1,1,4,0],[1,1,-2,1,0,-2,-4,1],
[1,-1,0,-1,-2,0,4,3],[0,1,0,-1,0,0,0,-1]])
sage: A.echelon_form()
[ 1  0  0 -2 -2  0  4  2]
[ 0  1  0 -1  0  0  0 -1]
[ 0  0  1 -2 -1  1  4  0]
[ 0  0  0  0  0  0  0  0]
[ 0  0  0  0  0  0  0  0]
[ 0  0  0  0  0  0  0  0]
```

Referències

[AL70] A. O. L. Atkin, J.Lehner, *Hecke operators on* $\Gamma_0(m)$, Mathematische Annalen 185, 1970, 134-160.

[BD16] Peter Bruin, Sander Dahmen, *Modular Forms*, Notes from a course given at Universiteit Leiden in the spring of 2016.
Disponible a:
`http://www.few.vu.nl/~sdn249/modularforms16/NotesOld.pdf`

[Con16] Keith Conrad, *Modular Forms (Draft, CTNT 2016)*, Notes from several talks given at the Connecticut Summer School in Number Theory (CTNT) in 2016.
Disponible a:
`https://ctnt-summer.math.uconn.edu/....pdf`

[Cre92] J. E. Cremona, *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, 1992.

[DS05] Fred Diamond, Jerry Shurman, *A First Course in Modular Forms*, Volume 228. Graduate Texts in Mathematics. Springer-Verlag, New York, 2005.

[Jer06] Jonas Jermann, *The valence formula and the space of modular forms*, Seminar given at ETH Zürich in November 2006.
Disponible a:
`https://www2.math.ethz.ch/education/bachelor/seminars/....pdf`

[Kna92] Anthony W. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, NJ, 1992.

[Man72] J. I. Manin, *Parabolic points and zeta functions of modular curves*, Mathematics of the USSR-Izvestiya, Volume 6, Number 1, 1972, pages: 19–64.

[Mas15] Marc Masdeu, *Modular Forms (MA4H9)*, Notes from a course given at the University of Warwick during the autumn of 2015.
Disponible a:
`https://mat.uab.cat/....pdf`

[Ser73] Jean-Pierre Serre, *A Course in Arithmetic* Translated from the French, Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg-Berlin, 1973.

[Ste07] William Stein, *Modular forms, a computational approach*, Volume 79. Graduate Studies in Mathematics. With an appendix by Paul E. Gunnells. American Mathematical Society, Providence, RI, 2007.