0.1 Formas Modulares y Series de Eisenstein

Un buen ejemplo de forma modular son las series de Eisenstein. Hay varios estilos de series de Eisenstein, el más sencillo se define como

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

Claro está que no incluimos el sumando asociado a $n = m = 0$; no denotamos esto explícitamente, pero sí lo asumimos implícitamente de ahora en adelante. Ahora, si

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

entonces la función inducida

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

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

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

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

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

otra vez estamos asumiendo implícitamente que el sumando $\lambda = 0$ queda excluido de la suma por razones obvias. Por lo tanto la convergencia absoluta de la serie E_{2k} se reduce a probar la convergencia del lado derecho para cualquier retícula L.

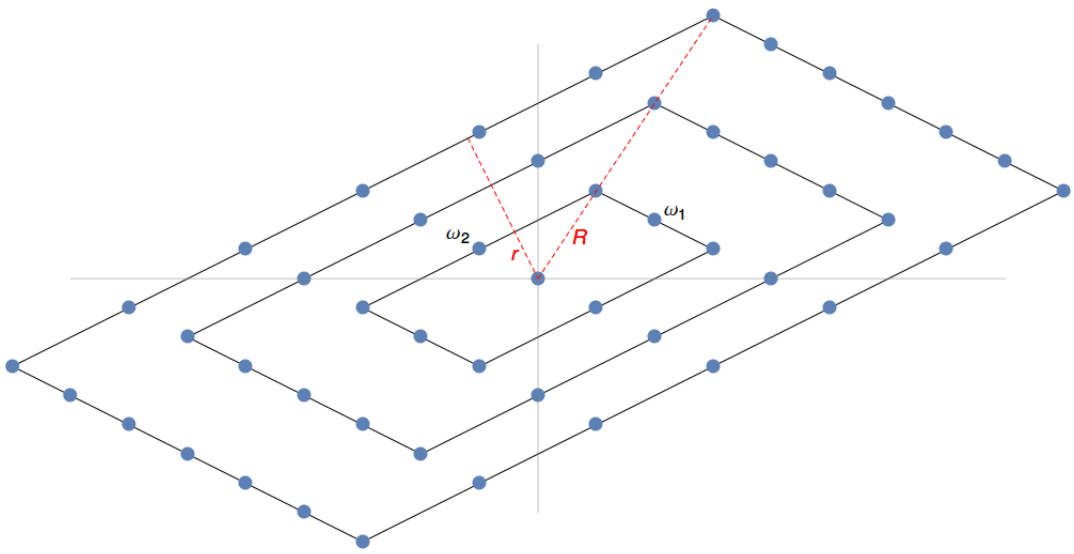
Hay varias maneras de probar que la serie $\sum |\lambda|^{-\sigma}$ converge si y sólo si $\sigma > 2$ (por ejemplo [**?**, §VII.2.2] y [**?**, §III.8]), pero damos una prueba elemental y visual:

Lema 1. *Sea $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subset \mathbb{C}$ una retícula, entonces:*

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

Proof. Todos los elementos de $L - \{0\}$ están sobre un paralelogramo con vértices $\{n\omega_1 + n\omega_2, -n\omega_1 + n\omega_2, -n\omega_1 - n\omega_2, n\omega_1 - n\omega_2\}$ para alguna $n \geq 1$; a estos paralelogramos los denotamos por P_n. Observa que los puntos de la retícula sobre un lado de P_n son $\{n\omega_1 + k\omega_2 \mid -n \leq k \leq n\}$. En particular hay $2n+1$ puntos de la retícula sobre un (y cualquier) lado del paralelogramo. Por lo tanto hay $8n = 4(2n+1) - 4$ puntos en $L \cap P_n$ porque los cuatro vértices se cuentan dos veces. Además, la homotecia $z \mapsto nz$ lleva los vértices $\pm m\omega_1 \pm m\omega_2$ del paralelogramo P_m a los vértices $\pm nm\omega_1 \pm nm\omega_2$ del paralelogramo P_{nm}. Es decir que $nP_m = P_{nm}$.

Ahora tomamos $r > 0$ como la distancia mínima del $0 \in \mathbb{C}$ al primer paralelogramo P_1 y $R > 0$ como la distancia máxima del 0 a P_1, ie. $R = |\omega_1 + \omega_2|$:
De hecho podemos tomar r como el radio de cualquier círculo contenido en P_1 y R como el radio de cualquier círculo que contiene a P_1.



Entonces si $\lambda \in L \cap P_1$, tenemos que $r \leq |\lambda| \leq R$. Más generalmente, si $\lambda \in L \cap P_n = L \cap nP_1$ entonces $\lambda = n\lambda'$ con $\lambda' \in P_1$ y así:

$$r \leq |\lambda'| \leq R \quad \Longrightarrow \quad nr \leq |\lambda| \leq nR$$

Esta desigualdad implica que

$$\frac{1}{n^\sigma R^\sigma} \leq \frac{1}{|\lambda|^\sigma} \leq \frac{1}{n^\sigma r^\sigma} \qquad (\lambda \in P_n \cap L). \tag{2}$$

Ahora sumamos esta desigualdad sobre todos las $\lambda \in P_n \cap L$ y obtenemos:

$$\frac{8}{n^{\sigma-1}R^\sigma} \leq \sum_{\lambda \in P_n \cap L} \frac{1}{|\lambda|^\sigma} \leq \frac{8}{n^{\sigma-1}r^\sigma}$$

porque $\#(L \cap P_n) = 8n$. Por último, si ahora sumamos sobre todos los paralelogramos hasta P_N para alguna $N > 0$, obtenemos:

$$\frac{8}{R^\sigma} \sum_{n=1}^{N} \frac{1}{n^{\sigma-1}} \leq \sum_{\substack{\lambda \in P_i \cap L \\ i \leq N}} \frac{1}{|\lambda|^\sigma} \leq \frac{8}{r^\sigma} \sum_{n=1}^{N} \frac{1}{n^{\sigma-1}}. \tag{3}$$

Ahora estamos en posición de probar el lema: la cota superior de (3) nos garantiza que si $\sigma > 2$, la serie $\sum |\lambda|^{-\sigma}$ converge porque el lado derecho converge a $8r^{-\sigma}\zeta(\sigma-1)$ porque $\sigma - 1 > 1$. Conversamente, si la serie $\sum |\lambda|^{-\sigma}$ converge, entonces el lado izquierdo converge a $8R^{-\sigma}\zeta(\sigma-1)$ lo cual implica que $\sigma - 1 > 1$ y terminamos. □

Con el lema hemos probado que (1) es válido y que E_{2k} se transforma adecuadamente bajo la acción de $\mathrm{SL}_2\mathbb{Z}$. Para terminar de probar que E_{2k} es una forma modular, debemos probar que es holomorfo en ∞.

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

$$E_{2k}(z) = \zeta(2k) + \frac{(-1)^k (2\pi)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \left(\sum_{d|n} d^{2k-1} \right) e^{2\pi i n z} \tag{4}$$

Esta fórmula claramente prueba que $E_{2k}(z)$ es anaítica en ∞ porque no tiene coeficientes negativos de Fourier. No escribimos la prueba de esta identidad porque más adelante probaremos una fórmula más general. Concluimos que las fórmulas (1) y (4) implican que $E_{2k} \in M_{2k}(\mathrm{SL}_2\mathbb{Z})$.

De una vez mencionamos una propiedad importante de los coeficientes de la serie de Fourier anterior. Si usamos los números de Bernoulli y la identidad famosa

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

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

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

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

Lo interesante de la fórmula anterior es que podemos analizar mejor las propiedades de los coeficientes de Fourier porque los números de Bernoulli están bien estudiados. En particular, tenemos el teorema de von Staudt que dice:

Teorema 2. *(von Staudt)Si l es un número primo y $l-1 \mid m$, entonces $lB_m \in \mathbb{Z}_{(l)}$ y*

$$lB_m \equiv -1 \pmod{l}.$$

Nota. Aquí, $\mathbb{Z}_{(l)}$ es la localización de $\mathbb{Z}$ con respecto del ideal primo $(l) \subset \mathbb{Z}$, es decir $\mathbb{Z}_{(l)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$. La prueba del teorema de von Staudt se basa en la relación entre los números de Bernoulli y los valores de las sumas de potencias consecutivas, por ejemplo [**?**, capítulo 5, §8, pg. 384][1].

Con este teorema podemos probar una propiedad importante de las series de Eisenstein normalizadas: su "trivialidad módulo l" cuando $l-1$ divide al peso.

Corolario 3. *Sea l un número primo tal que $l-1 \mid 2k$, y $E'_{2k}(z) := \sum a_n e^{2\pi inz}$ la serie de Fourier de la serie de Eisenstein normalizada de peso $2k$ (con $k > 1$). Entonces todos los coeficientes son elementos de $\mathbb{Z}_{(l)}$ y*

$$a_m \equiv 0 \pmod{l} \qquad \forall m > 0.$$

Proof. Sea $B_{2k} = \frac{a}{b} \in \mathbb{Q}$ con $(a,b) = 1$. Por el teorema de von Staudt tenemos que $lB_{2k} \in \mathbb{Z}_{(l)}$ y que $lB_{2k} \equiv -1 \pmod{l}$, es decir, existe $\frac{a'}{b'} \in \mathbb{Z}_{(l)}$ tal que $lB_{2k} + 1 = l\frac{a'}{b'}$ o en particular $b'(la+b) = la'b$. Como $l \nmid b'$, la igualdad anterior implica que $l | la+b$ y así $l \mid b$. Observa que esto implica que $l \nmid a$ por la elección de a y b. De esta manera tenemos:

$$E'_{2k}(z) = 1 - \frac{4k}{B_{2k}}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)e^{2\pi inz} = 1 - \sum_{n=1}^{\infty}\frac{4bk\sigma_{2k-1}(n)}{a}e^{2\pi inz} \in \mathbb{Z}_{(l)}[[e^{2\pi inz}]]$$

y por último, como $l \mid b$ y $l \nmid a$ entonces $4bk\sigma_{2k-1}(n)/a \in l\mathbb{Z}_{(l)}$, que es otra manera de escribir la congruencia que queríamos probar. □

Este corolario lo usaremos más adelante en la prueba de un resultado debido a Deligne y Serre (Sección 0.4).

En la prueba de la modularidad de $\bar{\rho}_{E,3}$, aparece una generalización de E_{2k} definida por

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

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

[1] Hay que tener cuidado con esta referencia porque en el enuciado del teorema escribe "$lB_m \equiv 1$" en lugar de "$lB_m \equiv -1$"; esto parece ser un error de dedo porque en la prueba sí aparece el signo correcto.

Definición 1. Sea $k \in \mathbb{Z}$ y $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ un caracter de Dirichlet módulo N, entonces la *serie de Eisenstein de peso k y caracter χ y parametro s* se define como

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

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

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

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

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

Sea

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

entonces:

$$\begin{aligned} E_{k,\chi}(\gamma z, s) &= \sum_{n,m\in\mathbb{Z}} \frac{\chi(m)}{\left(m\frac{az+b}{cz+d}+n\right)^k \left|m\frac{az+b}{cz+d}+n\right|^{2s}} \\ &= \sum_{n,m\in\mathbb{Z}} \frac{\chi(m)(cz+d)^k \left|cz+d\right|^{2s}}{((ma+nc)z+(mb+nd))^k \left|(ma+nc)z+(mb+nd)\right|^{2s}} \\ &= (cz+d)^k \left|cz+d\right|^{2s} \sum_{n,n\in\mathbb{Z}} \frac{\chi(m)}{((ma+nc)z+(mb+nd))^k \left|(ma+nc)z+(mb+nd)\right|^{2s}}. \end{aligned} \tag{5}$$

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

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

Sustituimos esta fórmula para $\chi(m)$ en (5) y recordamos que $(m,n) \mapsto (ma+nc, mb+nd)$ permuta los elementos de $\mathbb{Z} \times \mathbb{Z}$ para concluir que:

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

Por lo tanto

$$E_{k,\chi}(\gamma z, s) = (cz+d)^k \left|cz+d\right|^{2s} \chi(d) E_{k,\chi}(z,s). \tag{6}$$

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

En la prueba de la modularidad de $\bar{\rho}_{E,3}$, se usa una serie de Eisenstein particular, entonces a continuación nos enfocaremos solamente en este caso porque la prueba de este caso se generaliza sin muchas complicaciones; referimos a [**?**, §7.2] para el caso general. En lo que sigue vamos a continuar analíticamente $E_{1,\chi}(z,s)$ donde $k=1$, $N=3$ y

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

es el símbolo de Legendre módulo 3 (ie. el único caracter cuadrático módulo 3). Observemos que $\chi(-1) = -1$ implica que

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

Ahora, la serie $E_{1,\chi}(z,s)$ converge absolutamente cuando $\Re(s) > 1/2$, entonces en este caso reordenamos los sumandos:

$$\begin{aligned} E_{1,\chi}(z,s) &= \sum_{n,m\in\mathbb{Z}} \frac{\chi(m)}{(mz+n)\left|mz+n\right|^{2s}} \\ &= \sum_{n=-\infty}^{\infty} \frac{\chi(0)}{n\left|n\right|^{2s}} + \sum_{\substack{m=-\infty \\ m\neq 0}}^{\infty} \sum_{n=-\infty}^{\infty} \frac{\chi(m)}{(mz+n)\left|mz+n\right|^{2s}} \\ &= \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{\chi(m)}{(mz+n)\left|mz+n\right|^{2s}} + \frac{\chi(-m)}{(-mz+n)\left|-mz+n\right|^{2s}} \\ &= \sum_{m=1}^{\infty} \chi(m) \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)\left|mz+n\right|^{2s}} + \frac{1}{(mz-n)\left|mz-n\right|^{2s}} \\ \therefore E_{1,\chi}(z,s) &= 2\sum_{m=1}^{\infty} \chi(m) \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)\left|mz+n\right|^{2s}} \qquad (\Re(s) > \tfrac{1}{2}) \end{aligned} \tag{7}$$

Podemos reescribir la serie $\sum (mz+n)^{-1}\left|mz+n\right|^{-2s}$ en otra serie más sencilla. Primero observemos que:

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

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

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

Por lo tanto:

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

Parece que hemos complicado las cuentas, pero en realidad la segunda serie del lado derecho es un ejemplo de una función cuyas propiedades son conocidas: siguiendo a [**?**, §7.2] definimos

$$S(z;\alpha,\beta) := \sum_{n=-\infty}^{\infty} (z+n)^{-\alpha}(\bar{z}+n)^{-\beta}$$

donde $z \in \mathbb{H}$ y $\alpha, \beta \in \mathbb{C}$. Si sustituimos la notación $S(z;\alpha,\beta)$ en (7) obtenemos

$$E_{1,\chi}(z,s) = 2\sum_{m=1}^{\infty} \chi(m) m^{-1-2s} \sum_{r=0}^{m-1} S\left(z+\tfrac{r}{m}; 1+s, s\right). \tag{8}$$

Observa que si $\Re(\alpha)+\Re(\beta)>1$ entonces la serie $S(z;\alpha,\beta)$ converge absolutamente porque

$$|z+n|=|\overline{z+n}|=|\bar{z}+n|=\sqrt{(\Re(z)+n)^2+\Im(z)^2}=\mathcal{O}(n),$$

y así

$$\left|(z+n)^{-\alpha}(\bar{z}+n)^{-\beta}\right|=|z+n|^{-\Re(\alpha)}\,|\bar{z}+n|^{-\Re(\beta)}=\mathcal{O}\left(n^{-\Re(\alpha+\beta)}\right). \tag{9}$$

La ventaja de usar la serie $S(z;\alpha,\beta)$ es que se puede aplicar la fórmula de sumación de Poisson (FSP) para calcular esta serie. Más precisamente si escribimos $z=x+iy$ con $y>0$ y si denotamos

$$\phi(x,y;\alpha,\beta):=(x+iy)^{-\alpha}(x-iy)^{-\beta},$$

entonces tenemos que

$$S(x+iy;\alpha,\beta)=\sum_{n=-\infty}^{\infty}\phi(x+n,y;\alpha,\beta).$$

Observa que (9) implica que, como función de x tenemos:

$$|\phi(x,y;\alpha,\beta)|=\mathcal{O}(x^{-\Re(\alpha+\beta)})$$

lo cual implica que si $\Re(\alpha+\beta)>1$, entonces ϕ es absolutamente integrable sobre $\mathbb{R}$, ie. $\phi(x,y;\alpha,\beta)\in L^1(\mathbb{R})$ como función de x. Por lo tanto ϕ tiene una transformada de Fourier:

$$\hat{\phi}(u,y;\alpha,\beta)=\int_{-\infty}^{\infty}\phi(x,y;\alpha,\beta)e^{-2\pi iux}dx\qquad(y>0,\Re(\alpha,\beta)>1).$$

Ahora, queremos aplicar la fórmula de sumación de Poisson para concluir que

$$S(x+iy;\alpha,\beta)=\sum_{n=-\infty}^{\infty}\hat{\phi}(n,y;\alpha,\beta)e^{2\pi inx}. \tag{10}$$

Observamos que

$$\left|(x+iy)^{-\alpha}(x-iy)^{-\beta}\right|=|x+iy|^{-\Re(\alpha+\beta)}\leq|y|^{-\Re(\alpha+\beta)}$$

implica que la serie $\sum|\phi(x+n,y;\alpha,\beta)|$ converge uniformemente en la variable x cuando $\Re(\alpha+\beta)>1$. Este hecho es un paso importante en la prueba de la FSP. En efecto, durante la prueba se define una nueva función $F(x):=\sum\phi(x+n,y;\alpha,\beta)$ que resulta ser periódica con periodo 1 y para poder verificar que F coincide con su serie de Fourier (y así deducir la FSP), es suficiente ver que F es continua. La convergencia uniforme de la serie $\sum\phi(x+n,y;\alpha,\beta)$ implica la continuidad de F.

Por último, es necesario probar que el lado derecho de (10) es absolutamente convergente para poder justificar la igualdad en (10). Para esto vamos a tener que calular $\hat{\phi}$.

A nosotros nos interesa el caso $\alpha=s+1$ y $\beta=s$, entonces redefinimos la función:

$$\phi(x,y;s):=\phi(x,y;s+1,s)=(x+iy)^{-(s+1)}(x-iy)^{-s}$$

donde similarmente $|\phi(x,y;s)|=\mathcal{O}(x^{2\Re(s)-1})$ lo cual implica que $\phi(x,y;s)$ es absolutamente integrable como función de x cuando $\Re(s)>\frac{1}{2}$ (que es la misma condición que pedimos para la convergencia absoluta de la serie $E_{1,\chi}(z;s)$). De esta manera ϕ tiene una transformada de Fourier:

$$\hat{\phi}(u,y;s)=\int_{-\infty}^{\infty}\phi(x,y;s)e^{-2\pi iux}dx=\int_{-\infty}^{\infty}\frac{e^{-2\pi iux}dx}{(x+iy)^{s+1}(x-iy)^{s}}. \tag{11}$$

Con esta notación también definimos

$$S(x+iy;s):=S(x+iy;s+1,s)=\sum_{n=-\infty}^{\infty}\phi(x+n,y;s).$$

Queremos probar que la fórmula de sumación de Poisson se puede aplicar a $S(z;s)$. La prueba que damos a continuación contiene todo lo necesario para generalizarse sin muchos problemas al caso general de $S(z;\alpha,\beta)$ (ie. fórmula 10); referimos de nuevo a [**?**, Teorema 7.2.8] para el caso general.

Primero calculamos $\hat{\phi}(u,y;s)$ con:

Teorema 4. *Para $\Re(s) > 1$ tenemos la siguiente fórmula:*

$$\hat{\phi}(u,y;s) = \begin{cases} 2\pi i(2\pi u)^{2s} e^{-2\pi y u}\Gamma(s)^{-1}\Gamma(s+1)^{-1}\sigma(4\pi y u; s, s+1) & (u>0) \\ 2\pi i\Gamma(2s)(2y)^{-2s}\Gamma(s)^{-1}\Gamma(s+1)^{-1} & (u=0) \\ 2\pi i(2\pi u)^{2s} e^{-2\pi y|u|}\Gamma(s)^{-1}\Gamma(s+1)^{-1}\sigma(4\pi y\,|u|\,; s+1, s) & (u<0) \end{cases} \quad (\Re(s)>1) \qquad (12)$$

donde

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

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

Proof. Viene el en apéndice **??**. □

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

Teorema 5. *La función $\sigma(z;\alpha,\beta)$ admite una continuación meromorfa a $\mathbb{H}' \times \mathbb{C} \times \mathbb{C}$ con polos cuando $\beta = 0, -1, -2, \ldots$, ie. $\widetilde{\sigma}(z;\alpha,\beta) := \Gamma(\beta)^{-1}z^\beta\sigma(z;\alpha,\beta)$ es una función holomorfa y para cualquier compacto $Q \subset \mathbb{C}\times\mathbb{C}$ existen constantes $A, B > 0$ tales que*

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

y en particular

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

Este teorema nos dice que el lado derecho de (12) es una función entera de s cuando $u \neq 0$ (observa los factores $\Gamma(s)^{-1}\Gamma(s+1)^{-1}$) y meromorfa con polos en $2s = 0, -1, -2, \ldots$ cuando $u = 0$. Por lo tanto $\hat{\phi}(u,y;s)$ es una función meromorfa de s. Otra consecuencia del teorema 5 (y del teorema 4) es que podemos acotar $|\hat{\phi}(n,y;s)|$ para después probar la convergencia absoluta de la serie (10) y a su vez verificar el uso de la fórmula de sumación de Poisson. Más precisamente:

Teorema 6. *Como función de s, $S(z;s)$ tiene a continuación meromorfa a $\mathbb{C}$ y cumple la fórmula:*

$$S(z;s) = \hat{\phi}(0,y;s) + \sum_{\substack{n=-\infty \\ n\neq 0}}^{\infty} \hat{\phi}(n,y;s)e^{2\pi i n x} \qquad (z = x+iy \in \mathbb{H}). \qquad (13)$$

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

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

Consideramos la serie

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

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

$$\sum_{n=1}^{\infty}\left|\hat{\phi}(n,y;s)e^{2\pi inx}\right| \leq \underbrace{\frac{A}{2}\pi^{C_2}C_3C_1^{-C_2-1}(1+C_1^{-B})}_{C}\sum_{n=1}^{\infty} n^{C_2-1}e^{-2\pi C_1 n}$$

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

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

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

observa que

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

define una función holomorfa sobre $\mathbb{H}\times\mathbb{C}$. Por último, el teorema 4 dice que el sumando $\hat{\phi}(0,y;s)$ es una función meromorfa sobre $\mathbb{H}\times\mathbb{C}$ con polos cuando $2s = 0,-1,-2,\ldots$ o en particular $\Gamma(2s)^{-1}\hat{\phi}(0,y;s)$ es una función entera. Por lo tanto el lado derecho de 13 es una función meromorfa sobre $\mathbb{H}\times\mathbb{C}$ y da la continuación meromorfa de $S(z;s)$ a $\mathbb{H}\times\mathbb{C}$. □

Corolario 7. *La serie de Eisenstein $E_{1,\chi}(z;s)$ admite una continuación analítica a*

Proof. Recordemos (cf. la fórmula 8) que

$$E_{1,\chi}(z,s) = 2\sum_{m=1}^{\infty}\chi(m)m^{-1-2s}\sum_{r=0}^{m-1} S\left(z+\tfrac{r}{m};1+s,s\right).$$

Si sustituimos la fórmula del teorema 6 en lo anterior obtenemos:

$$2\sum_{m=1}^{\infty}\chi(m)m^{-1-2s}\sum_{r=0}^{m-1}\sum_{n=-\infty}^{\infty}\hat{\phi}(n,y;s)e^{2\pi in(x+\frac{r}{m})} \tag{14}$$

Para probar intercambiar las sumas de la serie anterior, hay que proba que es absolutamente convergente.

$$\begin{aligned}
E_{1,\chi}(z,s) &= 2\sum_{m=1}^{\infty}\chi(m)m^{-1-2s}\sum_{r=0}^{m-1} S\left(z+\tfrac{r}{m};1+s,s\right)\text{!!??}intercambiar\text{!!??}\\
&= 2\sum_{m=1}^{\infty}\chi(m)m^{-1-2s}\sum_{r=0}^{m-1}\sum_{n=-\infty}^{\infty}\hat{\phi}(n,y;1+s,s)e^{2\pi in(x+\frac{r}{m})}\\
&= 2\sum_{n=-\infty}^{\infty}\hat{\phi}(n,y;1+s,s)e^{2\pi inx}\sum_{m=1}^{\infty}\chi(m)m^{-1-2s}\underbrace{\sum_{r=0}^{m-1}e^{2\pi inr/m}}_{*}
\end{aligned}$$

Observa que que la suma $(*)$ es simplemente una suma geométrica:

$$\sum_{r=0}^{m-1}e^{2\pi inr/m} = \begin{cases}0 & \text{si } m \not| n\\ m & \text{si } m \mid n\end{cases}$$

Por lo tanto:

$$E_{1,\chi}(z,s) = 2\sum_{n=-\infty}^{\infty} \hat{\phi}(n,y;1+s,s)e^{2\pi inx}\sum_{m|n}\chi(m)m^{-2s}$$

□

0.2 Curvas Elipticas

0.3 Representaciones de Galois

Sea E una curva elíptica sobre $\mathbb{Q}$ y $E[p]$ sus puntos de orden p, un primo. Observa que el grupo de Galois absoluto $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}|\mathbb{Q})$ actúa sobre E y en particular actúa sobre $E[p]$ de la siguiente manera:

$$G_{\mathbb{Q}} \curvearrowright E[p] \qquad \text{con} \qquad \sigma P \mapsto P^{\sigma}.$$

Esta acción está bien definida porque la acción de $G_{\mathbb{Q}}$ conmuta con la suma de E. En efecto, si P y Q son dos puntos de E, entonces las coordenadas de $P+Q$ son funciones racionales en las coordenadas de P y Q [**?**, §III.2, Group Law Algorithm]. Por lo tanto

$$O = O^{\sigma} = ([p]P)^{\sigma} = (P+\cdots+P)^{\sigma} = P^{\sigma}+\cdots+P^{\sigma} = [p]P^{\sigma}$$

y así $P^{\sigma} \in E[p]$ siempre que $P \in E[p]$. De esta manera cada σ induce un automorfismo de $E[p]$, es decir, tenemos una representación $G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$. Por otro lado, sabemos que $E[p] \cong \mathbb{F}_p \times \mathbb{F}_p$ como $\mathbb{F}_p$-espacios vectoriales. Por lo tanto $\mathrm{Aut}(E[p])$ es simplemente $\mathrm{GL}_2(\mathbb{F}_p)$. Así definimos:

Definición 2. La representación de Galois de los puntos de p-torsión de una curva elíptica E se denota por

$$\bar{\rho}_{E,p} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

Nota. El isomorfismo $\mathrm{Aut}(E[p]) \cong \mathbb{F}_p \times \mathbb{F}_p$ no es natural, depende de la $\mathbb{F}_p$-base que elijas para $E[p]$.

Esta representación cumple dos propiedades muy importantes que escribimos como teoremas:

Teorema 8. *Si escribimos $\chi_p : G_{\mathbb{Q}} \to Aut(\mu_p) \cong \mathbb{F}_p^{\times}$ como el caracter ciclotómico, donde $\mu_p \subseteq \mathbb{C}^{\times}$ denota a las raices p-ésimas de la unidad. Entonces*

$$\det \bar{\rho}_{E,p} = \chi_p.$$

Proof. Para ver esto, recuerda que el *Weil pairing* $e_p : E[p] \times E[p] \to \mu_p$ es una forma bilineal, alternante, no-degenerada e invariante bajo la acción de $G_{\mathbb{Q}}$ [**?**, §III.8, proposición 8.1]. □

Teorema 9.

$$\mathrm{tr}\bar{\rho}_{E,p}(\mathrm{Frob}_q)$$

0.4 Un teorema de Deligne y Serre

En esta sección vamos a probar un paso muy importante en la prueba de la modularidad de $\bar{\rho}_{E,3}$ que aparece en un artículo famoso de Pierre Deligne y Jean-Pierre Serre [**?**, Teorema 6.7, §6, pg. 521]. Para esto requerimos los siguientes ingredientes:

Sea $K \subset \mathbb{C}$ un campo numérico, es decir, una extensión finita de $\mathbb{Q}$. Sea λ un lugar finito (o no-arquimediano) de K; éstos son clases de eqivalencias de valores absolutos sobre K. Denotamos por $\mathfrak{O}_{\lambda}$ al anillo de valoración asociado a λ, similarmente denotamos por $\mathfrak{m}_{\lambda}$ y k_{λ} al ideal maximal de $\mathfrak{O}_{\lambda}$ y al campo residual $\mathfrak{O}_{\lambda}/\mathfrak{m}_{\lambda}$ respectivamente. Sea l la característica de k_{λ}.

Sea $f : \mathbb{H} \to \mathbb{C}$ una forma modular de peso k (≥ 1), nebentypus ε sobre $\Gamma_0(N)$. Escribimos su serie de Fourier como $f(z) = \sum_{n=0}^{\infty} a_n q^n$ donde estamos usando la notación tradicional $q = e^{2\pi inz}$. Decimos que f es λ-*entero* si $a_n \in \mathfrak{O}_{\lambda}$ para toda $n \geq 0$ y escribimos $f \equiv 0 \pmod{\lambda}$ si además $a_n \in \mathfrak{m}_{\lambda}$ para toda n. POr último, si denotamos por T_p al p-ésimo operador de Hecke, decimos que f es un *vector propio de T_p módulo λ con valores propios* $a_p + \mathfrak{m}_{\lambda} \in k_{\lambda}$ si $T_p f - a_p f \equiv 0 \pmod{\lambda}$, es decir que f es casi un vector propio de T_p.

Lema 10. *(Deligne-Serre) Sean $\mathfrak{O} = (\mathfrak{O}, \mathfrak{m}, k)$ un anillo de varloración discreta, M un $\mathfrak{O}$-módulo libre de rango finito, $\mathcal{F} \subseteq \mathrm{End}_{\mathfrak{O}}(M)$ una familia de endomorfismos que conmutan dos a dos. Si $f \in M - \{0\}$ es tal que $Tf \equiv a_T f \pmod{\mathfrak{m}}$ para toda $T \in \mathcal{F}$, ie. es un vector propio módulo $\mathfrak{m}$ para todo endomorfismo de $\mathcal{F}$, entonces existe un anillo de valoración discreta $\mathfrak{O}' = (\mathfrak{O}', \mathfrak{m}', k')$ tal que $\mathfrak{O} \subseteq \mathfrak{O}'$, $\mathfrak{m} = \mathfrak{O} \cap \mathfrak{m}'$ y el campo de fracciones de $\mathfrak{O}'$ es una extensión finita del campo de fracciones de $\mathfrak{O}$; además existe un elemento $f' \in \mathfrak{O}' \otimes_{\mathfrak{O}} M$ distinto de cero tal que $Tf' = a'_T f'$ para toda $T \in \mathcal{F}$ y tal que $a_T \equiv a'_T \pmod{\mathfrak{m}'}$.*

Proof. Sea $\mathcal{H}$ la $\mathfrak{O}$-subálgebra de $\mathrm{End}_{\mathfrak{O}}(M)$ generada por $\mathcal{F}$. Como M es libre de rango finito, entonces $\mathrm{End}_{\mathfrak{O}}(M)$ es libre de rango finito, y así $\mathcal{H}$ es un $\mathfrak{O}$-módulo libre de rango finito, en particular es un módulo plano[2]. Observa que el morfismo que convierte a $\mathcal{H}$ en un $\mathfrak{O}$-álgebra es $x \mapsto x\mathrm{Id}_M$.

Ahora, definimos $\chi : \mathcal{H} \to k$ como el morfismo que asigna valores propios, es decir definimos $\chi(T) := a_T + \mathfrak{m}$ para toda $T \in \mathcal{F}$ y extendemos por linealidad a todo $\mathcal{H}$. Observa que por construcción $\chi|_{\mathfrak{O}} = \mathrm{Id}_{\mathfrak{O}}$, entonces χ es sobreyectivo. Por lo tanto $\mathcal{H}/\ker\chi \cong k$ y así $\ker\chi \subset \mathcal{H}$ es un ideal maximal.

Sea $\mathfrak{p} \subseteq \ker\chi$ un ideal primo minimal[3]. Como $\mathfrak{p}$ es minimal, todo sus elementos distintos de cero son divisores de cero. En efecto: si denotamos al conjunto de divisores del cero junto con el mismo 0 por D, entonces

$$\mathfrak{p} \not\subseteq D \quad \Longrightarrow \quad \mathcal{H} - D \not\subseteq \mathcal{H} - \mathfrak{p} \quad \Longrightarrow \quad \mathcal{H} - \mathfrak{p} \subsetneq (\mathcal{H} - D)(\mathcal{H} - \mathfrak{p}) \quad !$$

lo cual es una contradicción porque $(\mathcal{H}-D)(\mathcal{H}-\mathfrak{p})$ es un conjunto multiplicativo que contiene estrictamente al conjunto multiplicativo maximal $\mathcal{H} - \mathfrak{p}$ [**?**, §3]. Por lo tanto $\mathfrak{p} \subseteq D$.

Como $\mathcal{H}$ es un $\mathfrak{O}$-módulo libre, para toda $x \in \mathfrak{O}$ el endomorfismo $f \mapsto xf$ de $\mathcal{H}$ se representa por la matriz diagonal $x\mathrm{Id}_M$ cuyo determinante es una potencia de x que (salvo en el caso $x = 0$) es distinto de cero porque $\mathfrak{O}$ es un dominio entero.

En particular $f \mapsto xf$ es inyectiva para toda $x \in \mathfrak{O} - \{0\}$. Por lo tanto $\mathfrak{O}$ no tiene divisores de cero en $\mathcal{H}$ y así $\mathfrak{p} \cap \mathfrak{O} = 0$. De esta manera la composición $\mathfrak{O} \to \mathcal{H} \twoheadrightarrow \mathcal{H}/\mathfrak{p}$ es inyectiva; por lo tanto podemos considerar a $\mathfrak{O}$ como un subanillo de $\mathcal{H}/\mathfrak{p}$. Además, como $\mathcal{H}$ es un $\mathfrak{O}$-módulo finitamente generado, entonces $\mathcal{H}/\mathfrak{p}$ también es un $\mathfrak{O}$-módulo finitamente generado. Como $\mathfrak{O}$ es un anillo noetheriano (por ser anillo de valoración discreta), entonces $\mathcal{H}/\mathfrak{p}$ es un $\mathfrak{O}$-módulo noetheriano, ie. todos sus submódulos son finitamente generados.

Este comentario sirve para probar que $\mathcal{H}/\mathfrak{p}$ es una extensión entera de $\mathfrak{O}$. En efecto, si tomamos $T + \mathfrak{p} \in \mathcal{H}/\mathfrak{p}$ arbitrario, entonces como $\mathfrak{O}[T + \mathfrak{p}] = \mathfrak{O}[T] + \mathfrak{p} \subseteq \mathcal{H}/\mathfrak{p}$, tenemos que $\mathfrak{O}[T + \mathfrak{p}]$ es un $\mathfrak{O}$-módulo finitamente generado para toda $T + \mathfrak{p} \in \mathcal{H}/\mathfrak{p}$, por lo tanto ([**?**, §5, Proposición 5.1]) $T + \mathfrak{p}$ es entero sobre $\mathfrak{O}$ para toda $T + \mathfrak{p} \in \mathcal{H}/\mathfrak{p}$.

Ahora, sea L el campo de fracciones del dominio entero $\mathcal{H}/\mathfrak{p}$ y $\mathfrak{O}_L$ la cerradura entera de $\mathfrak{O}$ en L. Esto hace que $\mathfrak{O}_L$ sea un anillo de valoración discreta con ideal maximal $\mathfrak{m}_L$ que se contrae a $\mathfrak{m}$ y cuyo campo residual k_L es una extensión de k. Como $\mathfrak{O} \subseteq \mathcal{H}/\mathfrak{p}$ es una extensión entera, tenemos que $\mathcal{H}/\mathfrak{p} \subseteq \mathfrak{O}_L$. Resumiendo, tenemos las siguientes inclusiones:

$$\mathfrak{O} \hookrightarrow \mathcal{H}/\mathfrak{p} \hookrightarrow \mathfrak{O}_L \hookrightarrow L.$$

Definimos $\chi' : \mathcal{H} \to \mathfrak{O}_L$ como la composición de $\mathcal{H} \twoheadrightarrow \mathcal{H}/\mathfrak{p} \hookrightarrow \mathfrak{O}_L$ y denotamos $a'_T := \chi'(T)$ para toda $T \in \mathcal{F}$. En este caso, tenemos que $\chi'(\ker\chi) \subseteq \mathfrak{m}_L$. Para probar esto requerimos del "Going Up Theorem" [**?**, proposición 4.15 y corolario 4.17]. Como $\ker\chi$ es un ideal maximal que contiene a $\mathfrak{p}$, entonces $\ker\chi + \mathfrak{p} \subset \mathcal{H}/\mathfrak{p}$ es un ideal maximal. Por el "Going Up Theorem" existe un ideal primo $I \subset \mathfrak{O}_L$ tal que $I \cap \mathcal{H}/\mathfrak{p} = \ker\chi + \mathfrak{p}$ y además, como $\ker\chi + \mathfrak{p}$ es maximal, I también es maximal. Como $\mathfrak{O}_L$ es local, necesariamente tenemos que $I = \mathfrak{m}_L$. Por lo tanto $\mathfrak{m}_L \cap \mathcal{H}/\mathfrak{p} = \ker\chi + \mathfrak{p}$ y así $\chi'(\ker\chi) \subseteq \mathfrak{m}_L$.

Esto último nos garantiza que $a'_T \equiv a_T \pmod{\mathfrak{m}_L}$, porque $\chi(T - a_T) = \chi(T) - a_T + \mathfrak{m} = 0 + \mathfrak{m}$ para toda $T \in \mathcal{F}$ implica que $T - a_T \in \ker\chi$ y por lo anterior tenemos que:

$$\chi'(T - a_T) = a'_T - a_T \in \mathfrak{m}_L \quad \Longrightarrow \quad a'_T \equiv a_T \pmod{\mathfrak{m}_L} \tag{15}$$

[2]Recuerda que un módulo libre es proyectivo y todo módulo proyectivo es plano; También se puede usar la conmutatividad del producto tensorial y la suma directa para probar de manera elemental que el funtor $N \mapsto N \otimes \mathcal{H}$ es exacto izquierdo.

[3]La existencia de este ideal primo minimal se prueba con el lema de Zorn: como $\ker\chi$ es maximal, el conjunto de ideales primos contenidos en $\ker\chi$ es no vacío, ahora si tomamos una cadena descendiente $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots$ de ideales primos, entonces $\cap\mathfrak{p}_i$ es un ideal primo y una cota de la cadena; por el lema de Zorn el conjunto de ideales primos contenidos en $\ker\chi$ tiene elementos minimales.

Con esto sabemos quienes tienen que ser los valores propios, ahora tenemos que construir un vector propio con esos valores propios. Como $\mathcal{H}$ es un $\mathfrak{O}$-módulo plano, entonces la inclusión $\mathfrak{O} \hookrightarrow L$ se preserva cuando tomamos el producto tensorial con $\mathcal{H}$, es decir tenemos una inclusión $\mathcal{H} \cong \mathfrak{O} \otimes_{\mathfrak{O}} \mathcal{H} \hookrightarrow L \otimes_{\mathfrak{O}} \mathcal{H}$.

Observa que $L \otimes M$ es un $L \otimes \mathcal{H}$-módulo finitamente generado con la acción $(\lambda \otimes T)(\mu \otimes f) = (\lambda\mu \otimes T(f))$.

Sea $\mathfrak{P}$ la extensión del ideal primo $\mathfrak{p}$ en $L \otimes \mathcal{H}$ bajo la inclusión $\mathcal{H} \subset L \otimes \mathcal{H}$. Como $\mathcal{H}$ es un $\mathfrak{O}$-módulo noetheriano, $\mathfrak{p}$ es un ideal finitamente generado por algunas $\{T_1, \ldots, T_n\} \subset \mathfrak{p}$. Por lo tanto $\mathfrak{P}$ es un ideal de $L \otimes \mathcal{H}$ finitamente generado por $\{1 \otimes T_1, \ldots, 1 \otimes T_n\}$. Como $\mathfrak{p}$ consta de puro divisores de cero, existen $T_1, \ldots, T_n' \in \mathcal{H}$ tales que $T_i T_i' = 0$. Para cada $1 \otimes T_i \in \mathfrak{P}$ toma un $f_i \in M$ tal que $T_i'(f_i) \neq 0$. Observa que $(1 \otimes T_i)(1 \otimes T_i'(f_i)) = (1 \otimes T_i(T_i'(f_i))) = 1 \otimes 0 = 0$. Por lo tanto todas las $1 \otimes T_i \in \mathfrak{P}$ son divisores de cero de $L \otimes M$ como $L \otimes \mathcal{H}$-módulo y así $\mathfrak{P} \subseteq D'$ donde D' es el conjunto de divisores de cero de $L \otimes M$.

Es bien conocido que el conjunto de los divisores de cero de un módulo finitamente generado (junto con el cero) es la unión de los ideales primos asociados[4] al módulo [?, teorema 3.1, pg 89]. Por lo tanto si denotamos al conjunto de ideales primos asociados de $L \otimes M$ como $\mathcal{A} = \mathrm{Ass}_{L \otimes \mathbb{H}}(L \otimes M)$ tenemos que

$$\mathfrak{P} \subseteq D' = \bigcup_{\mathfrak{q} \in \mathcal{A}} \mathfrak{q}$$

Por el teorema de "Prime Avoidence" $\mathfrak{P}$ está contenido en algún $\mathfrak{q} \in \mathcal{A}$. Por lo tanto existe un elemento $\lambda \otimes f'' \in L \otimes M$ tal que $\mathfrak{q}$ es el anulador de $\lambda \otimes f'' \neq 0$. Como $T - a_T' \in \mathfrak{p}$ para toda $T \in \mathcal{F}$, entonces $1 \otimes (T - a_T') \in \mathfrak{P} \subseteq \mathfrak{q}$ y así:

$$\big(1 \otimes (T - a_T')\big)(\lambda \otimes f'') = 0 \quad \Longrightarrow \quad (T - a_T')(f'') = 0 \quad \Longrightarrow \quad T f'' = a_T' f''. \tag{16}$$

Por lo tanto, si tomamos $f' \in \mathcal{O}_L \otimes M$ un múltiplo de $\lambda \otimes f''$ (cancela el denominador de λ), entonces f' es el elemento buscado gracias a (15) y a (16). □

[4]Un ideal primo $\mathfrak{p}$ de un anillo A es asociado a un A-módulo M si existe un elemento $f \in M$ tal que $\mathfrak{p} = (f : 0) := \{a \in A \mid af = 0\}$.