Universidad de la República
Facultad de Ciencias

Relación de Eichler-Shimura y Recíproco del Teorema de Modularidad

Monografía presentada a la Facultad de Ciencias de la Universidad de la República por

Santiago Radi

en cumplimiento parcial con los requerimientos para la obtención del título de Licenciado en Matemática.

Tutor

Gonzalo Tornaría ..... Universidad de la República
Gustavo Rama ..... Universidad de la República

Tribunal

Gonzalo Tornaría ..... Universidad de la República
Gustavo Rama ..... Universidad de la República
Juan Alonso ..... Universidad de la República

Montevideo
martes 3 julio, 2018

Relación de Eichler-Shimura y Recíproco del Teorema de Modularidad, Santiago Radi.

Esta tesis fue preparada en LaTeX usando la clase iietesis (v1.1).
Contiene un total de 77 páginas.
Compilada el martes 3 julio, 2018.
http://www.cmat.edu.uy/

Tabla de contenidos

Tabla de contenidos

Prefacio

El objetivo de este documento es familiarizarse con algunos de los objetos y resultados implicados en el Teorema de Modularidad y en la Relación de Eichler-Shimura, demostrando esta última y dando una idea de la prueba del recíproco del Teorema de Modularidad. Introduciremos objetos como las formas modulares, las curvas elípticas, los operadores de Hecke, las curvas modulares, etc. que son objetos que actualmente están en estudio y han dado interesantes resultados de la Teoría de Números, siendo el ejemplo más célebre, el denominado Último Teorema de Fermat.

En el documento utilizaremos libremente conceptos de álgebra lineal (como espacios vectoriales, producto interno, valores y vectores propios, el concepto de operador normal, el Teorema Espectral para Operadores normales y la diagonalización simultánea), álgebra de grupos (acciones, Teoremas de isomorfismo, diagramas conmutativos, orden de un elemento y de un subgrupo, subgrupo de torsión, subgrupos normales), álgebra en anillos (módulos finitamente generados, localización de un anillo, ideales, ideales primos, endomorfismos, dominios, dominios de ideales de principales), y conceptos de extensiones de cuerpos (cuerpo algebraicamente cerrado, clausura algebraica de un cuerpo, polinomio minimal de un número algebraico, enteros algebraicos, polinomio minimal separable, mapa de Frobenius, característica de un cuerpo). Será muy importante la idea de conjunto cociente en distintos contextos, por lo que asumimos, que el lector maneja con claridad esta idea.

Fuera del álgebra, utilizaremos teoremas del análisis complejo, los conceptos de funciones holomorfa y meromorfa, las expansiones de Fourier, las superficies de Riemann y las formas diferenciales. Principalmente en el Capítulo 4, trabajaremos con conceptos de la Geometría Algebraica (curvas algebraicas en general, homogeinización de un polinomio de n variables, valuación) y con espacios proyectivos.

Finalmente, en menor medida utilizaremos resultados de la Teoría de Números clásica, las formas diferenciales, conceptos clásicos de Topología (conjunto compacto, Hausdorff, conexo), conceptos de la Topología Diferencial (atlas, cartas, cambios de carta diferenciales, grado de un mapa entre variedades, conexión simple, homotopías de curvas) y conceptos de la Topología Algebraica (como Teoremas de levantamiento).

Tabla de contenidos

El documento está dividido en 5 capítulos:

El Capítulo 0, mostrará como las curvas elípticas y las formas modulares se pueden utilizar para resolver problemas de la Teoría de Números de dificultad media. Se dará a partir de estos ejemplos, una idea de que son estos objetos sin entrar en una definición matemática formal, resolviendo parcialmente dos problemas interesantes.

En el Capítulo 1, definiremos matemáticamente las formas modulares y cuspidales e introduciremos las Operadores de Hecke para éstas. Separaremos las formas cuspidales en dos subespacios ortogonales y probaremos cuáles son los valores propios para los Operadores de Hecke T_n (Teorema 1.25).

En el Capítulo 2 definiremos las curvas modulares, los Espacios de Moduli, los divisores y el Grupo de Picard. Definiremos morfismos entre divisores y probaremos que pueden definirse en Grupos de Picard (Teorema 2.25). Al final de este capítulo, extenderemos los Operadores de Hecke a Grupos de Picard y Espacios de Moduli.

En el Capítulo 3 definiremos curvas elípticas, formas diferenciales, Jacobiano y Variedades Abelianas. Los conceptos introducidos nos permitirán demostrar al final del capítulo una conexión entre algunas curvas modulares y algunas variedades abelianas de interés, en el Teorema 3.21.

Por último, en el Capítulo 4, desarrollaremos la reducción de curvas elípticas, para luego en las dos últimas secciones demostrar la Relación de Eichler-Shimura (en el Teorema 4.21) y dar una idea de la prueba del recíproco del Teorema de Modularidad (en el Teorema 4.22).

Capítulo 0

Introducción

Durante 358 años, fue un problema abierto muy reconocido en matemática, el llamado "Último Teorema de Fermat". En él se establecía que la ecuación

$$a^n + b^n = c^n$$

no tiene una terna $(a, b, c) \in \mathbb{Z}^3$ que sea solución con $abc \neq 0$ y $n \geq 3$. El esfuerzo de prueba de varios casos particulares se vio reducido cuando en 1984, Gerhard Frey planteó una conexión de este problema con dos objetos de la Teoría de Números muy de moda en esa época (y actualmente), como lo son, las formas modulares y las curvas elípticas. La conexión se hizo a través de una conjetura planteada en 1955, por los matemáticos japoneses Goro Shimura y Yutaka Taniyama, en la cual planteaban que toda curva elíptica E racional se podía corresponder con una forma modular de $\mathcal{S}_2(\Gamma_0(N_E))$ con valores propios racionales, de forma que sus funciones L asociadas sean iguales. A las curvas elípticas que cumplen la conjetura de Taniyama-Shimura las llamaremos curvas modulares y la conjetura es por tanto, que todas las curvas elípticas son modulares.

La relación planteada por Gerhard Frey era que si existe una terna (a, b, c) que sea solución para un cierto n, y construimos la curva elíptica $E_{a,b} : y^2 = x(x - a^n)(x + b^n)$, entonces $E_{a,b}$ no sería una curva elíptica modular. Este hecho fue demostrado en 1986 por Ken Ribet y Jean-Pierre Serre, dando paso a que si la conjetura de Taniyama-Shimura era cierta entonces también lo era el Último Teorema de Fermat. Finalmente, Andrew Wiles, demostró en 1995 la Conjetura de Taniyama-Shimura para una cierta familia de curvas elípticas (las *semiestables*) en la que incluye a todas las curvas $E_{a,b}$. Esto mostraba entonces que como todas las curvas elípticas semiestables eran modulares, las curvas $E_{a,b}$ no podían existir, y por tanto, no podían existir soluciones (a, b, c) al problema de Fermat con $abc \neq 0$ y $n \geq 3$. En 2001, Christophe Breuil, Brian Conrad, Fred Diamond y Richard Taylor extendieron las ideas de Andrew Wiles para demostrar la conjetura de Taniyama-Shimura para todas las curvas elípticas sobre $\mathbb{Q}$.

Esta conexión entre curvas elípticas y formas modulares dada por la Conjetura

de Taniyama-Shimura (actual Teorema de Modularidad) tiene un recíproco, en el sentido de que a cada forma modular de $\mathcal{S}_2(\Gamma_0(N_E))$ con valores propios racionales se le puede hacer corresponder una curva elíptica racional. Este recíproco viene dado por la Relación de Eichler-Shimura, demostrada por los matemáticos Martin Eichler y Goro Shimura.

Para familiarizarnos con las curvas elípticas y con las formas modulares, veremos dos problemas de la Teoría de Números cuya solución se obtiene del uso de estos objetos.

0.1. Curvas elípticas y números congruentes

Definición **0.1.** *Un número natural se dice* ***congruente*** *si es el área de un triángulo rectángulo de lados racionales*

Observemos primero que es simple encontrar números congruentes de triángulos que tienen lados enteros. En efecto, si N es congruente pero utilizando lados enteros, entonces $N = \frac{ab}{2}$ para un triángulo de lados a, b, c que además verifican $a^2+b^2 = c^2$. La terna (a, b, c) de números naturales que forman un triángulo rectángulo se conoce como terna pitagórica, y es sabido que todas las ternas pitagóricas son de la forma $d(2uv, u^2 - v^2, u^2 + v^2)$ con $\text{mcd}(u, v) = 1$ y $d \in \mathbb{N}$. Esto hace que todos los números naturales que son congruentes con lados enteros sean de la forma $N = d^2uv(u^2 - v^2)$. El número de esta forma más pequeño se obtiene con $(d, u, v) = (1, 2, 1)$ y es 6. Sin embargo, este no es el número congruente más pequeño puesto que Fibonacci en 1225 demostró que 5 es un número congruente y se obtiene con la terna racional $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$.

En efecto, 5 es sí, el número congruente más pequeño. Demostrar esto requiere mayor esfuerzo, y el siguiente teorema dará el vínculo de este problema con las curvas elípticas:

Teorema **0.2.** *Si N es un número natural libre de cuadrados, las siguientes afirmaciones son equivalentes:*

1. *N es un número congruente*
2. *Existen tres cuadrados racionales en progresión aritmética de razón N*
3. *La curva $y^2 = x^3 - N^2x$ tiene una solución racional distinta de $(-N, 0)$, $(0, 0)$ y $(N, 0)$.*

La ecuación del tercer punto es precisamente una curva elíptica (la definición de curva elíptica en general se presenta en la definición 3.1). Como veremos en la Sección 3.1, los puntos que son solución de una curva elíptica presentan una suma

que se obtiene de la geometría de la curva elíptica. Esta suma les da estructura de grupo. El neutro de la suma en las curvas elípticas será el punto infinito, que se adjunta a los puntos que verifican la ecuación.

Demostración. Demostraremos 1. $\Leftrightarrow$ 2. $\Leftrightarrow$ 3.

1. $\Rightarrow$ 2.: Si $N = \frac{ab}{2}$ para una terna pitagórica racional (a, b, c) y tomamos $x = (\frac{c}{2})^2 \Rightarrow x - N = (\frac{a-b}{2})^2$ y $x + N = (\frac{a+b}{2})^2$.

2. $\Rightarrow$ 1.: Si x, $x - N$ y $x + N$ son cuadrados perfectos, tomamos $(a, b, c) = (\sqrt{x+N} + \sqrt{x-N}, \sqrt{x+N} - \sqrt{x-N}, 2\sqrt{x})$.

2. $\Rightarrow$ 3.: Si x, $x-N$ y $x+N$ son cuadrados perfectos, también lo es su producto, por lo que $y^2 = x(x-N)(x+N) = x^3 - N^2x$. Luego, $x \notin \{0, \pm N\}$ puesto que la progresión está formada por cuadrados perfectos y N es libre de cuadrados.

3. $\Rightarrow$ 2.: Un punto P se suma a si mismo considerando la recta tangente a la curva elíptica que pasa por P. Si P tiene orden 2, entonces $P+P = \infty$ y por tanto la recta tangente tiene que ser vertical. Esto lleva a que $P = (\tilde{x}, 0)$. Por lo tanto, si tenemos un punto Q distinto a $(-N, 0)$, $(0, 0)$ y $(N, 0)$ según la hipótesis, entonces Q no va a ser de orden 2.

Llamemos $Q = (x_1, y_1)$ y $2Q = (x_2, y_2)$. Dado que la recta tangente r de la curva elíptica por Q no es vertical, la misma es de la forma $y = ax + b$. Por como se realiza la suma de los puntos de una curva elíptica, la recta tangente pasa por Q (dos veces) y por $(x_2, -y_2)$, y por tanto, sustituyendo en la curva elíptica, tenemos el polinomio $P(x) = (x+N)x(x-N) - (ax+b)^2$, tiene como raíces a x_1 (con multiplicidad dos) y a x_2. Como P es mónico, es de la forma $P(x) = (x-x_1)^2(x-x_2)$.

Evaluando P en $-N$ e igualando las dos expresiones de P, obtenemos que $(b - aN)^2 = (x_1 + N)^2(x_2 + N)$.

$x_1 + N \neq 0$ puesto que $b - aN$ lo es y por tanto $x_2 + N$ es un cuadrado perfecto.

De la misma forma, evaluando P en N y 0 obtenemos que x_2 y $x_2 - N$ son cuadrados perfectos. □

Pese a que no entraremos en detalle, se puede demostrar que para las curvas elípticas como la que aparece en el Teorema 0.2, el subgrupo de torsión está formado por las tres soluciones triviales dadas en el Teorema 0.2 y el ∞, y por ende encontrar un nuevo punto Q, implica encontrar infinitos puntos dado que $Q \notin \text{Tor}(E)$. Dado que cada punto Q da un triángulo que hace a N un número congruente, esto implica que si N es congruente para un triángulo, lo es para infinitos triángulos. Este hecho es simple de demostrar solamente utilizando la teoría de las curvas elípticas.

0.2. Formas modulares y el problema de los cuatro cuadrados

Veamos ahora una aplicación de las formas modulares. Utilizaremos las formas modulares para demostrar que todo número natural puede escribirse como suma de cuatro cuadrados. Más aún, la prueba que daremos va a dar una fórmula que dice de cuántas formas distintas puede escribirse n como suma de cuatro cuadrados.

Definimos $r(n,k) = \#\{v \in \mathbb{Z}^k : n = v_1^2 + ... + v_k^2\}$.

Es fácil verificar que si $k_1 + k_2 = k$ para $k_1, k_2 \in \mathbb{N}$, entonces $r(n,k) = \sum_{l+m=n} r(l,k_1)r(m,k_2)$ con $l, m \in \mathbb{N}$.

Definimos

$$\theta(z,k) = \sum_{n=0}^{\infty} r(n,k)q^n$$

con $q = e^{2\pi iz}$ para $z \in \mathcal{H} = \{z \in \mathbb{C} : Im(z) > 0\}$. Es claro que $\theta(z+1,k) = \theta(z,k)$, $\forall k \in \mathbb{N}$.

Veamos que además, $\theta(z,k_1+k_2) = \theta(z,k_1)\theta(z,k_2)$. En efecto:

$$\theta(z,k_1)\theta(z,k_2) = \left(\sum_{l=0}^{\infty} r(l,k_1)q^l\right)\left(\sum_{m=0}^{\infty} r(m,k_2)q^m\right) =$$
$$= \sum_{n=0}^{\infty}\left(\sum_{l+m=n} r(l,i)r(m,j)q^{l+m}\right) = \sum_{n=0}^{\infty} r(n,k_1+k_2)q^n \Rightarrow$$

$$\theta(z,k_1)\theta(z,k_2) = \theta(z,k_1+k_2). \tag{0.1}$$

Consideremos $\theta(z) = \theta(z,1)$, entonces:

$$r(n,1) = \begin{cases} 2 & \text{Si } n \text{ es cuadrado perfecto y } n \neq 0 \\ 1 & \text{Si } n = 0 \\ 0 & \text{Otro caso} \end{cases}$$

y por tanto

$$\theta(z) = \sum_{d\in\mathbb{Z}} e^{2\pi id^2 z} = \sum_{d\in\mathbb{Z}} q^{d^2}.$$

Utilizando la fórmula de adición de Poisson, obtenemos que:

$$\theta\left(\frac{-1}{4z}\right) = \sqrt{-2iz}\theta(z) \tag{0.2}$$

donde la raíz compleja que tomamos es aquella que queda definida en $\mathcal{H}$.

Dado que las transformaciones de Möbius actúan en $\mathbb{C}$, y más aún, las matrices de determinante positivo actúan en $\mathcal{H}$ (ver previo a la definición 1.3), consideremos la acción de $\left(\begin{smallmatrix}1 & 0\\ 4 & 1\end{smallmatrix}\right)$:

$$\theta\left(\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}(z)\right) = \theta\left(\frac{z}{4z+1}\right) = \theta\left(\frac{-1}{4(-1/4z-1)}\right) = \sqrt{2i\frac{1}{4z}+1}\;\theta\left(-\frac{1}{4z}-1\right).$$

Como θ es 1-periódica, $\theta\left(-\frac{1}{4z}-1\right) = \theta\left(-\frac{1}{4z}\right) = \sqrt{-2iz}\;\theta(z)$. Juntando todo nos queda:

$$\theta\left(\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}(z)\right) = \sqrt{4z+1}\;\theta(z). \tag{0.3}$$

Utilizando la ecuación (0.1), obtenemos que $\theta(z,4) = \theta(z)^4$ y la relación de la ecuación (0.3) se transforma en:

$$\theta\left(\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}(z), 4\right) = (4z+1)^2\;\theta(z,4). \tag{0.4}$$

Y si juntamos la ecuación (0.4) con el hecho de que $\theta(z,4)$ es 1-periódica obtenemos que:

$$\theta\left(\begin{pmatrix}a & b\\ c & d\end{pmatrix}(z), 4\right) = (cz+d)^2\;\theta(z,4) \tag{0.5}$$

para $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \{\pm\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right), \pm\left(\begin{smallmatrix}1 & 0\\ 4 & 1\end{smallmatrix}\right)\}$, y por ende para el grupo generado por ellas que es:

$$\Gamma_0(4) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix}* & *\\ 0 & *\end{pmatrix} \pmod 4\right\}.$$

El hecho de que $\theta(z,4)$ satisfaga la ecuación (0.5), indica que $\theta(z,4)$ es una forma modular de peso 2 (por el exponente de $(cz+d)$) para el subgrupo $\Gamma_0(4)$. A este conjunto de formas modulares lo denotaremos $\mathcal{M}_2(\Gamma_0(4))$. Como mencionaremos en el Teorema 1.7, las formas modulares conforman un espacio vectorial de dimensión finita, y en el caso de $\mathcal{M}_2(\Gamma_0(4))$, su dimensión es 2. El conjunto $\{G_{2,2}, G_{2,4}\}$ es una base de $\mathcal{M}_2(\Gamma_0(4))$, por lo que si observamos las primeros dos términos de las tres formas modulares vemos que

$$\theta(z,4) = 1 + 8q + ...$$
$$-\frac{3}{\pi^2}G_{2,2}(z) = 1 + 24q + ...$$
$$-\frac{1}{\pi^2}G_{2,4}(z) = 1 + 8q + ...$$

y por lo tanto $\theta(z,4) = -\frac{1}{\pi^2}G_{2,4}(z)$. Esto da por tanto una fórmula para $r(n,4)$ dado que son conocidos los coeficientes de $G_{2,4}$:

$$r(n,4) = 8 \sum_{\substack{0<d|n \\ 4\nmid d}} d.$$

En particular tenemos que $r(n,4)$ es positivo para todo $n \in \mathbb{N}$. Los problemas de dos, seis y ocho cuadrados, se resuelven de la misma forma, obteniendo fórmulas que indican para cada n, de cuántas formas distintas pueden escribirse.

Capítulo 1

Formas Modulares

1.1. Conceptos básicos

Sea $\mathrm{SL}_2(\mathbb{Z}) = \{\gamma \in \mathcal{M}_{2\times 2}(\mathbb{Z}) : \det(\gamma) = 1\}$.

Es conocido que $\mathrm{SL}_2(\mathbb{Z})$ es un grupo no abeliano con el producto de matrices. Esto se puede ver por el hecho de que el determinante es un morfismo con el producto y que dada una matriz $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, su inverso es $\frac{1}{\det(A)} \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, entonces el inverso de una matriz de $\mathrm{SL}_2(\mathbb{Z})$ es una matriz de $\mathrm{SL}_2(\mathbb{Z})$.

Definición **1.1.** *Llamamos* ***subgrupo de congruencia principal de nivel N*** *al conjunto*

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

donde la congruencia módulo N es en cada entrada de la matriz.

Es fácil ver que $\Gamma(N)$ es un subgrupo de $\mathrm{SL}_2(\mathbb{Z})$ y que $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \simeq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, por tanto $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] \leq N^4 < \infty$.

Definición **1.2.** Γ *es un* ***subgrupo de congruencia*** *si* Γ *es un subgrupo de* $\mathrm{SL}_2(\mathbb{Z})$ *y* $\exists N > 0$ *tal que* $\Gamma(N) \subseteq \Gamma$.

Dado que $\Gamma(N) \subseteq \Gamma \subseteq \mathrm{SL}_2(\mathbb{Z}) \Rightarrow [\mathrm{SL}_2(\mathbb{Z}) : \Gamma] \leq [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] < \infty$.

Nos interesarán principalmente dos subgrupos de congruencia:

$$\Gamma_1(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}.$$

Se cumple que $\Gamma(N) \lhd \Gamma_1(N) \lhd \Gamma_0(N)$.

Sea $\mathcal{H}= \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ el plano superior complejo y $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Definimos una acción de $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\} \curvearrowright \mathcal{H}^*$. Si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, la acción será $\gamma(z) = \frac{az+b}{cz+d}$. La acción queda bien definida porque $\det(\gamma) > 0$. Notar que la acción puede restringirse a $\mathbb{Q} \cup \{\infty\}$ o a $\mathcal{H}$.

Dada $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ y $k \in \mathbb{Z}$, definimos el operador $[\gamma]_k : \mathbb{C}^{\mathcal{H}} \to \mathbb{C}^{\mathcal{H}}$ dado por:

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

donde $j(\gamma, z) = cz + d$ cuando $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Se cumple que $[\gamma\gamma']_k = [\gamma]_k\,[\gamma']_k$ para cualesquiera sean $\gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$.

Definición **1.3.** *Sea $f : \mathcal{H} \to \mathbb{C}$ holomorfa, Γ un subgrupo de congruencia y k un entero. Diremos que f es* ***débilmente modular de peso k con respecto a*** *Γ si $f\,[\gamma]_k = f$, $\forall \gamma \in \Gamma$*

Notar que como Γ es un subgrupo de congruencia, $\exists N > 0$ tal que $\Gamma(N) \subseteq \Gamma$, y por ende $\exists h > 0$ tal que $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$. Tomemos h el mínimo. Si f es débilmente modular de peso k con respecto a Γ, se cumple que:

$$f(z) = f\left[\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)\right]_k (z) = f(z + h)$$

y por tanto f es h-periódica, por lo que admite una expansión de Fourier dada por $f(z) = \sum_{n=-\infty}^{\infty} a_n(f)\, q_h^n$ donde $q_h = e^{\frac{2\pi i z}{h}}$ en $B_1^*(0)$.

Definición **1.4.** *Diremos que f es* ***holomorfa en infinito*** *si la expansión de Fourier anterior admite una extensión holomorfa a $B_1(0)$. En ese caso definimos $f(\infty) = a_0$.*

Notar que la definición anterior es equivalente a que $a_n = 0$, $\forall n < 0$.

Podemos ahora definir:

Definición **1.5.** *Sea Γ un subgrupo de congruencia y $k \in \mathbb{Z}$. Decimos que $f : \mathcal{H} \to \mathbb{C}$ es una* ***forma modular de peso k con respecto a*** *Γ si:*

1. *f es holomorfa en $\mathcal{H}$*
2. *f es débilmente modular de peso k con respecto a Γ*
3. *$f\,[\alpha]_k$ es holomorfa en infinito $\forall \alpha \in \mathrm{SL}_2(\mathbb{Z})$.*

La tercer condición permite asegurar que f va a ser holomorfa en todos los elementos de $\mathcal{H}^* \setminus \mathcal{H}$, puesto que si $s \in \mathcal{H}^* \setminus \mathcal{H}$, existe α en $\mathrm{SL}_2(\mathbb{Z})$ tal que $\alpha(\infty) = s$

Llamaremos $\mathcal{M}_k(\Gamma)$ al espacio de las formas modulares de peso k con respecto a Γ.

Definición **1.6.** *Sea Γ un subgrupo de congruencia, y $k \in \mathbb{Z}$. Diremos que $f : \mathcal{H} \to \mathbb{C}$ es una* ***forma cuspidal de peso k con respecto a*** *Γ si:*

1. *f es una forma modular de peso k con respecto a Γ*
2. *$f\left[\alpha\right]_k(\infty) = 0$, $\forall \alpha \in \mathrm{SL}_2(\mathbb{Z})$.*

La segunda condición implica que f se anula en todas los puntos de $\mathbb{Q} \cup \{\infty\}$.

Llamaremos $\mathcal{S}_k(\Gamma)$ al espacio de las formas cuspidales de peso k con respecto a Γ.

Resumimos en el Teorema 1.7 las propiedades más relevantes de los espacios de las formas modulares y cuspidales.

Teorema **1.7.** *Sean k, l enteros y Γ, Γ_1 y Γ_2 subgrupos de congruencia. Entonces:*

1. *$\mathcal{M}_k(\Gamma)$ es un $\mathbb{C}$-espacio vectorial de dimensión finita.*
2. *$\mathcal{S}_k(\Gamma)$ es un $\mathbb{C}$-subespacio vectorial de $\mathcal{M}_k(\Gamma)$.*
3. *Si $\Gamma_1 \subseteq \Gamma_2 \Rightarrow \mathcal{M}_k(\Gamma_1) \supseteq \mathcal{M}_k(\Gamma_2)$ y $\mathcal{S}_k(\Gamma_1) \supseteq \mathcal{S}_k(\Gamma_2)$.*
4. *Si $f \in \mathcal{M}_k(\Gamma)$, $g \in \mathcal{M}_l(\Gamma) \Rightarrow fg \in \mathcal{M}_{k+l}(\Gamma)$.*
5. *Si $k \neq l \Rightarrow \mathcal{M}_k(\Gamma) \cap \mathcal{M}_l(\Gamma) = \{0\}$.*

Casi todas las propiedades son simples de chequear, salvo, el hecho de que $\dim(\mathcal{M}_k(\Gamma)) < \infty$. La prueba de este hecho se puede encontrar en el Capítulo 3 de [DS00].

A partir del Teorema 1.7, obtenemos que $\mathcal{M}(\Gamma) = \bigoplus_{k \in \mathbb{Z}} \mathcal{M}_k(\Gamma)$ es un anillo y que $\mathcal{S}(\Gamma) = \bigoplus_{k \in \mathbb{Z}} \mathcal{S}_k(\Gamma)$ es un ideal de $\mathcal{M}(\Gamma)$.

1.2. Operadores de Hecke

El objetivo será poder definir transformaciones lineales entre dos espacios de formas modulares del mismo peso.

Sean Γ_1 y Γ_2 dos subgrupos de congruencia y $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ (matrices 2x2 con entradas racionales y determinante positivo).

Consideremos el conjunto $\Gamma_1\alpha\Gamma_2 = \{\gamma_1\alpha\gamma_2 : \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}$. Se puede demostrar que $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$ tiene una cantidad finita de clases. Sea $\{\beta_i\}_{i=1}^r$ un conjunto de representantes de $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$. Dado que cada $\beta_i \in \mathrm{GL}_2^+(\mathbb{Q})$ necesitaremos extender el operador $[\gamma]_k$ de la Sección 1.1. Si $\beta \in \mathrm{GL}_2^+(\mathbb{Q})$ y $f \in \mathbb{C}^{\mathcal{H}}$, definimos:

$$f\,[\beta]_k\,(z) = (\det\beta)^{k-1} j(\beta, z)^{-k} f(\beta(z)).$$

Es claro que esta definición extiende a la anterior puesto que si $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\det\gamma = 1$.

Sea $f \in \mathcal{M}_k(\Gamma_1)$. El **operador** $[\Gamma_1\alpha\Gamma_2]_k$ **de peso k** será:

$$f\,[\Gamma_1\alpha\Gamma_2]_k = \sum_{i=1}^{r} f[\beta_i]_k$$

donde $\{\beta_i\}_{i=1}^r$ es un conjunto de representantes de $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$.

Teorema **1.8.** *Sean Γ_1 y Γ_2 dos subgrupos de congruencia y $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$.*

1. *$[\Gamma_1\alpha\Gamma_2]_k$ no depende del conjunto de representantes $\{\beta_i\}_{i=1}^r$ de $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$.*
2. *$[\Gamma_1\alpha\Gamma_2]_k : \mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2)$.*
3. *$[\Gamma_1\alpha\Gamma_2]_k\,(\mathcal{S}_k(\Gamma_1)) \subseteq \mathcal{S}_k(\Gamma_2)$.*

Demostración. 1. Sea $\beta_i' = \gamma_1\beta_i$ con $\gamma_1 \in \Gamma_1 \Rightarrow f[\beta_i']_k = f[\gamma_1\beta_i]_k = f[\gamma_1]_k[\beta_i]_k = f[\beta_i]_k$ puesto que $f \in \mathcal{M}_k(\Gamma_1)$.

2. Sea $\gamma_2 \in \Gamma_2 \Rightarrow (f[\Gamma_1\alpha\Gamma_2]_k)[\gamma_2]_k = \sum_{i=1}^r f[\beta_i\gamma_2]_k = \sum_{i=1}^r f[\beta_i']_k$ donde $\beta_i' = \beta_i\gamma_2$ para cada i. Dado que $\{\beta_i'\}_{i=1}^r$ es también un conjunto de representantes, $f[\Gamma_1\alpha\Gamma_2]_k$ es débilmente modular de peso k. Además cada $f[\beta_i]$ es holomorfa en $\mathcal{H}^*$ lo que hace a $f[\Gamma_1\alpha\Gamma_2]_k$ holomorfa en $\mathcal{H}^*$.

3. Si $f \in \mathcal{S}_k(\Gamma_1)$, $f[\delta]_k(\infty) = 0$, $\forall\delta \in \mathrm{SL}_2(\mathbb{Z})$. Ahora, $f[\beta_i]_k[\delta]_k = f[\beta_i\delta]_k$, y como $\beta_i\delta$ actúa moviendo todos los elementos de $\mathbb{Q}\cup\{\infty\}$ en todos los elementos de $\mathbb{Q}\cup\{\infty\}$, $f[\beta_i\delta]_k(\infty) = 0$ y esto $\forall\delta \in \mathrm{SL}_2(\mathbb{Z})$, y por tanto $f[\Gamma_1\alpha\Gamma_2]_k \in \mathcal{S}_k(\Gamma_2)$. □

1.2.1. T_n y $\langle n\rangle$

Nos importarán dos operadores de Hecke en particular.

Sean $N, n \in \mathbb{N}$ tal que $\mathrm{mcd}(n, N) = 1$. Por la identidad de Bézout, existen $a, b \in \mathbb{Z}$ tal que $an - bN = 1$, y por tanto, tenemos que $\left(\begin{smallmatrix} a & b \\ N & n \end{smallmatrix}\right) \in \Gamma_0(N)$. Esto nos asegura la existencia de una matriz de la forma $\left(\begin{smallmatrix} a & b \\ rN & n \end{smallmatrix}\right)$ en $\Gamma_0(N)$, lo que nos permite definir el siguiente operador:

Definición **1.9.** *Dados $N, n \in \mathbb{N}$ tal que $\text{mcd}(n, N) = 1$. Definimos el* ***operador diamante*** *como $\langle n \rangle : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$ tal que*

$$\langle n \rangle = \begin{cases} \left[\Gamma_1(N) \left(\begin{smallmatrix} a & b \\ rN & n \end{smallmatrix}\right) \Gamma_1(N)\right]_k & Si \quad \text{mcd}(n, N) = 1 \\ \\ 0 & Si \quad \text{mcd}(n, N) > 1 \end{cases}$$

donde $\left(\begin{smallmatrix} a & b \\ rN & n \end{smallmatrix}\right) \in \Gamma_0(N)$

Veamos que la definición anterior no depende de a, b o r. En efecto, sean $\left(\begin{smallmatrix} a & b \\ rN & n \end{smallmatrix}\right), \left(\begin{smallmatrix} a' & b' \\ r'N & n \end{smallmatrix}\right) \in \Gamma_0(N)$. Dado que $\left(\begin{smallmatrix} a & b \\ rN & n \end{smallmatrix}\right) \left(\begin{smallmatrix} a' & b' \\ r'N & n \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} an - br'N & a'b - b'a \\ nN(r - r') & a'n - b'rN \end{smallmatrix}\right) = \gamma_1 \in \Gamma_1(N) \Rightarrow \left(\begin{smallmatrix} a & b \\ N & n \end{smallmatrix}\right) = \gamma_1 \left(\begin{smallmatrix} a' & b' \\ N & n \end{smallmatrix}\right)$ y por ende no depende de la elección de a, b o r.

Llamemos $\alpha \in \Gamma_0(N)$ a la matriz vinculada al operador $\langle n \rangle$. Observemos que como $\Gamma_1(N) \lhd \Gamma_0(N)$ entonces $\Gamma_1(N) \setminus \Gamma_1(N)\alpha\Gamma_1(N) = \Gamma_1(N) \setminus \Gamma_1(N)\Gamma_1(N)\alpha = \Gamma_1(N) \setminus \Gamma_1(N)\alpha$ por lo que para el operador diamante, $f\left[\Gamma_1(N)\alpha\Gamma_1(N)\right]_k = f\left[\alpha\right]_k$.

Definición **1.10.** *Sea $N \in \mathbb{N}$ y $p \in \mathbb{P}$[1]. Definimos el* ***operador*** *T_p como*

$$T_p : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N)) \ / \ T_p = \left[\Gamma_1(N)\alpha\Gamma_1(N)\right]_k$$

con $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$.

Podemos hallar un conjunto de representantes $\{\beta_i\}_{i=1}^r$ para el operador T_p, de forma de tener una formula más explícita:

Teorema **1.11.** *Sea N un entero positivo y $p \in \mathbb{P} \Rightarrow$*

$$T_p f = \begin{cases} \sum_{i=0}^{p-1} f[\left(\begin{smallmatrix} 1 & i \\ 0 & p \end{smallmatrix}\right)]_k & si \quad p \mid N \\ \\ \sum_{i=0}^{p-1} f[\left(\begin{smallmatrix} 1 & i \\ 0 & p \end{smallmatrix}\right)]_k + f[\left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right) \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)]_k & si \quad p \nmid N \end{cases}$$

donde $mp - nN = 1$

Una prueba del Teorema 1.11 se puede encontrar en la página 170 de [DS00].

Buscamos ahora generalizar el operador T_p a cualquier natural n. Para ello, necesitaremos el siguiente teorema:

Teorema **1.12.** *Sean $p, q \in \mathbb{P}$ distintos y $d \in \mathbb{N}$, entonces:*

1. $T_p\langle d \rangle = \langle d \rangle T_p$
2. *Sea $f \in \mathcal{M}(\Gamma_1(N))$, entonces f es 1-periódica y los coeficientes de la expansión de Fourier de $T_p f$ son:*

$$a_n(T_p f) = a_{np}(f) + \mathbf{1}_N(p) p^{k-1} a_{n/p}(\langle p \rangle f)$$

[1] Denotamos $\mathbb{P}$ al conjunto de los números primos

donde

$$\mathbf{1}_N(p) = \begin{cases} 1 & si \quad p \nmid N \\ 0 & si \quad p \mid N \end{cases}$$

3. $T_p T_q = T_q T_p$

Demostración. 1. Sea $\gamma \in \Gamma_0(N)$ y $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ la matriz vinculada al operador T_p, entonces $\gamma\alpha\gamma^{-1} = \left(\begin{smallmatrix} 1 & * \\ 0 & p \end{smallmatrix}\right)$ (mód N) y por tanto $\Gamma_1(N)\alpha\Gamma_1(N) = \Gamma_1(N)\gamma\alpha\gamma^{-1}\Gamma_1(N)$.

Por otro lado, si $\{\beta_i\}_{i=1}^r$ es un conjunto de representantes para T_p entonces

$$\bigcup_{i=1}^{r} \Gamma_1(N)\beta_i = \Gamma_1(N)\alpha\Gamma_1(N) = \Gamma_1(N)\gamma\alpha\gamma^{-1}\Gamma_1(N).$$

Usando dos veces el hecho de que $\Gamma_1(N) \lhd \Gamma_0(N)$, obtenemos que

$$\bigcup_{i=1}^{r} \Gamma_1(N)\beta_i = \gamma\left(\Gamma_1(N)\alpha\Gamma_1(N)\right)\gamma^{-1} = \gamma\left(\bigcup_{i=1}^{r} \Gamma_1(N)\beta_i\right)\gamma^{-1} = \bigcup_{i=1}^{r} \Gamma_1(N)\gamma\beta_i\gamma^{-1}$$

y multiplicando por γ a derecha nos queda

$$\bigcup_{i=1}^{r} \Gamma_1(N)\beta_i\gamma = \bigcup_{i=1}^{r} \Gamma_1(N)\gamma\beta_i.$$

Si γ es una matriz vinculada al operador diamante $\langle d\rangle$ entonces tenemos que

$$\langle d\rangle T_p f = \sum_{i=1}^{r} f[\beta_i\gamma]_k = \sum_{i=1}^{r} f[\gamma\beta_i]_k = T_p\langle d\rangle f$$

y esto para toda $f \in \mathcal{M}_k(\Gamma_1(N))$.

2. (Esquema de demostración) Dado que $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$, entonces f es 1-periódica. El objetivo es tomar los representantes del operador T_p del Teorema 1.11 y calcular las expansiones de Fourier de cada $f[\beta_i]$.

3. Utilizando la fórmula para los coeficientes de la expansión de Fourier de $T_p f$ dos veces consecutivas (para T_p y para T_q) obtenemos

$$a_n(T_p(T_q f)) = a_{npq}(f) + \mathbf{1}_N(q)q^{k-1}a_{np/q}(\langle q\rangle f) + \mathbf{1}_N(p)p^{k-1}a_{nq/p}(\langle p\rangle f) \\ + \mathbf{1}_N(pq)(pq)^{k-1}a_{n/pq}(\langle pq\rangle f).$$

Como la ecuación es simétrica con p y q, los operadores conmutan. □

Definimos el operador de Hecke para potencias de primos y para $n = 1$ como:

$$\begin{aligned} T_1 &= \mathrm{id} \\ T_{p^r} &= T_p T_{p^{r-1}} - p^{k-1}\langle p\rangle T_{p^{r-2}}. \end{aligned}$$

Luego, si n es un natural tal que su descomposición en factores primos es $n = \prod_{i=1}^{m} p_i^{e_i}$, entonces

$$T_n = \prod_{i=1}^{m} T_{p_i^{e_i}}.$$

Cabe mencionar que para que T_n esté bien definido es necesario verificar que $T_{p^r}T_{q^s} = T_{q^s}T_{p^r}$ para $p, q \in \mathbb{P}$ distintos y $r, s \in \mathbb{N}$. Esto hecho es simple de verificar utilizando el Teorema 1.12.

El Teorema 1.13 resume algunas propiedades de conmutatividad de estos dos operadores de Hecke.

Teorema **1.13.** *Sean m y n dos enteros positivos. Entonces:*

1. $T_m\langle n\rangle = \langle n\rangle T_m$
2. $\langle mn\rangle = \langle m\rangle\langle n\rangle = \langle n\rangle\langle m\rangle$
3. $T_m T_n = T_n T_m$
4. *Si* $\mathrm{mcd}(m, n) = 1 \Rightarrow T_m T_n = T_{mn}$

Demostración. 1. y 4. se obtienen del Teorema 1.12 y de la definición de T_n. Para 3. alcanza con probar por inducción que $T_{p^r}T_{p^s} = T_{p^s}T_{p^r}$, y para 2. alcanza con ver que $\left(\begin{smallmatrix} * & * \\ 0 & m \end{smallmatrix}\right)\left(\begin{smallmatrix} * & * \\ 0 & n \end{smallmatrix}\right) \pmod N = \left(\begin{smallmatrix} * & * \\ 0 & mn \end{smallmatrix}\right) \pmod N$. □

A partir del Teorema 1.12.(2) y de la definición de T_n en función de su descomposición en factores primos, podemos obtener los coeficientes de la expansión de Fourier de $T_n f$.

Teorema **1.14.** *Sea $f \in \mathcal{M}_k(\Gamma_1(N))$ y T_n un operador de Hecke. Los coeficientes de la expansión de Fourier de $T_n f$ son de la forma:*

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

En particular, si $\mathrm{mcd}(m, n) = 1 \Rightarrow a_m(T_n f) = a_{mn}(f)$.

1.2.2. Adjunto de operadores de Hecke

A partir de ahora trabajaremos en $\mathcal{S}_k(\Gamma_1(N))$. El objetivo será ver rápidamente que los operadores del conjunto $T^0(N) = \{T_n, \langle n\rangle : \text{mcd}(n, N) = 1\}$ son normales en $\mathcal{S}_k(\Gamma_1(N))$.

Definición **1.15.** *Sea $T : V \to V$ un operador lineal. Diremos que T es un* ***operador normal*** *si conmuta con su operador adjunto.*

Para poder definir su adjunto será necesario definir un producto interno en $\mathcal{S}_k(\Gamma_1(N))$.

Definición **1.16.** *Dado Γ subgrupo de congruencia, el* ***Producto Interno de Petersson*** *$\langle\ ,\ \rangle_\Gamma : \mathcal{S}_k(\Gamma) \times \mathcal{S}_k(\Gamma) \to \mathbb{C}$ viene dado por*

$$\langle f, g\rangle_\Gamma = \frac{1}{V_\Gamma}\int_{X(\Gamma)} f(z)\overline{g(z)}(\text{Im}(z))^{k-2}dxdy,$$

donde $V_\Gamma = \int_{X(\Gamma)} \frac{1}{y^2}dxdy$.

El conjunto $X(\Gamma)$ será definido en la Sección 2.1. La verificación de que efectivamente es un producto interno se puede encontrar en la Sección 5.4 de [DS00]. El siguiente teorema nos será útil:

Teorema **1.17.** *Sea $\Gamma \subseteq \text{SL}_2(\mathbb{Z})$ un subgrupo de congruencia, $\alpha \in \text{GL}_2^+(\mathbb{Q})$ y definamos $\alpha' = \det(\alpha)\alpha^{-1}$. Entonces $\forall f, g \in \mathcal{S}_k(\Gamma)$,*

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

La prueba de este resultado se puede encontrar en la Proposición 5.5.2 de [DS00].

Teorema **1.18.** *Si $p \nmid N$ entonces T_p y $\langle p\rangle$ son operadores normales.*

Demostración. Sea $\alpha \in \Gamma_0(N)$ una matriz vinculada al operador diamante, entonces $\alpha' = \alpha^{-1}$. Como $\Gamma_1(N) \lhd \Gamma_0(N)$ entonces $\alpha^{-1}\Gamma_1(N)\alpha = \Gamma_1(N)$ y el Teorema 1.17 queda:

$$\langle\langle p\rangle f, g\rangle_\Gamma = \langle f[\Gamma\alpha\Gamma]_k, g\rangle_\Gamma = \langle f, g[\Gamma\alpha'\Gamma]_k\rangle_\Gamma = \left\langle f, \langle p\rangle^{-1} g\right\rangle_\Gamma$$

Por lo tanto $\langle p\rangle^* = \langle p\rangle^{-1}$ y ser su inverso conmuta con $\langle p\rangle$.

Para T_p, al igual que en el caso anterior $\alpha^{-1}\Gamma\alpha = \Gamma$ y usando el Teorema 1.17, obtenemos que $[\Gamma\alpha\Gamma]_k^* = [\Gamma\alpha'\Gamma]_k$.

Sea $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ la matriz vinculada a T_p, entonces $\alpha' = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & n \\ N & mp \end{smallmatrix}\right)^{-1} \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \left(\begin{smallmatrix} p & n \\ N & m \end{smallmatrix}\right)$ donde n y m se eligen para que la primer matriz esté en $\Gamma_1(N)$ y la tercera en $\Gamma_0(N)$.

Por lo tanto $\Gamma_1(N)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma_1(N) = \Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\left(\begin{smallmatrix} p & n \\ N & m \end{smallmatrix}\right)\Gamma_1(N)$.

Sea $\{\beta_i\}_{i=1}^r$ un conjunto de representantes para el operador T_p. Usando que $\Gamma_1(N) \lhd \Gamma_0(N)$ tenemos que

$$\Gamma_1(N)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma_1(N) = \Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_1(N)\left(\begin{smallmatrix} p & n \\ N & m \end{smallmatrix}\right) = \bigcup_{i=1}^{r} \Gamma_1(N)\beta_i\left(\begin{smallmatrix} p & n \\ N & m \end{smallmatrix}\right).$$

Dado que $\left(\begin{smallmatrix} p & n \\ N & m \end{smallmatrix}\right) \in \Gamma_1(N)$, entonces $mp - nN = 1$ y $m = p^{-1}$ (mód N), lo que lleva a que

$$T_p^* = \langle p \rangle^{-1} T_p$$

Finalmente, utilizando el Teorema 1.12, tenemos que T_p es normal. □

Luego, si tenemos $n \in \mathbb{N}$ coprimo con N, el operador $\langle n \rangle$ se puede descomponer en sus factores primos y como cada uno de ellos es normal, su composición es normal. De igual manera ocurre para T_n y sus factores primos, demostrando que los elementos de $T^0(N)$ son normales. Utilizando el Teorema Espectral para operadores normales, tenemos entonces que cada operador de $T^0(N)$ tiene una base ortogonal de vectores propios. Más aún, por el Teorema 1.13, los operadores de $T^0(N)$ conmutan y por lo tanto se diagonalizan simultáneamente, lo que implica que podemos encontrar una base ortogonal de vectores propios para todos los elementos de $T^0(N)$. Utilizaremos la terminología "forma propia" en lugar de vector propio a partir de ahora.

1.2.3. Formas cuspidales nuevas y viejas

Sea M un divisor de N. Es fácil ver que $\Gamma_1(N) \subseteq \Gamma_1(M)$ y por lo visto en el Teorema 1.7.(3), $\mathcal{S}_k(\Gamma_1(M)) \subseteq \mathcal{S}_k(\Gamma_1(N))$. Otra forma de encajar $\mathcal{S}_k(\Gamma_1(M)) \hookrightarrow \mathcal{S}_k(\Gamma_1(N))$ es utilizando el mapa inyectivo $[\alpha_d]_k$ con $\alpha_d = \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)$ y d un divisor de N/M.

Nos interesa distinguir las formas cuspidales que provienen de niveles que son divisores de N con las formas cuspidales que corresponden solo al nivel N. Para ello hacemos la siguiente definición, combinando las dos formas de encajar $\mathcal{S}_k(\Gamma_1(M))$ mencionadas al comienzo de la sección:

Definición **1.19.** *Sea d divisor de N e $i_d : \left(\mathcal{S}_k\left(\Gamma_1\left(\frac{N}{d}\right)\right)\right)^2 \to \mathcal{S}_k(\Gamma_1(N))$ dado por $i_d(f,g) = f + g[\alpha_d]_k$. Definimos el* ***subespacio de formas viejas de nivel N*** *como:*

$$\mathcal{S}_k(\Gamma_1(N))^{old} = \sum_{d|N} \mathrm{Im}(i_d).$$

La definición de $\mathcal{S}_k(\Gamma_1(N))^{old}$ es la formalización de lo que se mencionaba al principio. El término f es debido a la observación de que $\mathcal{S}_k(\Gamma_1(M)) \subseteq \mathcal{S}_k(\Gamma_1(N))$ y el término asociado a g es debido a que $\mathcal{S}_k(\Gamma_1(M)) \hookrightarrow \mathcal{S}_k(\Gamma_1(N))$ por $[\alpha_d]_k$.

Definición **1.20.** *El* ***subespacio de formas nuevas de nivel N*** *será el complemento ortogonal del subespacio anterior con respecto al producto interno de Petersson:*

$$\mathcal{S}_k(\Gamma_1(N))^{new} = (\mathcal{S}_k(\Gamma_1(N))^{old})^{\perp}.$$

Teorema **1.21.** *Para cualquier $N, n \in \mathbb{N}$, $\mathcal{S}_k(\Gamma_1(N))^{new}$ y $\mathcal{S}_k(\Gamma_1(N))^{old}$ son invariantes por T_n y $\langle n \rangle$.*

Una demostración del Teorema 1.21 se puede encontrar en la Proposición 5.6.2 de [DS00]. Es fácil deducir del Teorema 1.21 y de la Sección 1.2.2 que los subespacios "old" y "new" tienen una base ortogonal de formas propias de $T^0(N)$. De hecho, en $\mathcal{S}_k(\Gamma_1(N))^{new}$ se puede quitar la condición de $\text{mcd}(n, N) = 1$. En efecto, para el caso de $\langle n \rangle$ es sencillo, porque si $\text{mcd}(n, N) \neq 1$, $\langle n \rangle = 0$ y todos las formas son formas propias. Para el caso de T_n, será una consecuencia del Teorema 1.25.

1.2.4. Valores propios

Estudiamos los valores propios de T_n para las formas propias en $\mathcal{S}_k(\Gamma_1(N))^{new}$. Para ello precisaremos primero el siguiente lema:

Teorema **1.22** (Lema principal)**.** *Si $f \in \mathcal{S}_k(\Gamma_1(N))$, tiene una expansión de Fourier $f(z) = \sum_{n=0}^{\infty} a_n(f) q^n$ donde $a_n(f) = 0$ cuando $\text{mcd}(n, N) = 1$, entonces $f \in \mathcal{S}_k(\Gamma_1(N))^{old}$.*

Una prueba del Teorema 1.22 se puede encontrar en la Sección 5.7 de [DS00].

Teorema **1.23.** *Sea $f \in \mathcal{S}_k(\Gamma_1(N))$ una forma propia de todos los operadores de $T^0(N)$ tal que $a_1(f) = 0$. Entonces $f \in \mathcal{S}_k(\Gamma_1(N))^{old}$.*

Demostración. Usando la fórmula del Teorema 1.14 tenemos que $a_1(T_n f) = a_n(f)$ y además como f es forma propia, $T_n f = c_n f \Rightarrow a_1(T_n f) = c_n a_1(f)$ para $\text{mcd}(n, N) = 1$. Como $a_1(f) = 0 \Rightarrow a_n(f) = 0$ cuando $\text{mcd}(n, N) = 1$ y por el Teorema 1.22, $f \in \mathcal{S}_k(\Gamma_1(N))^{old}$. □

El contrarrecíproco del Teorema 1.23 nos muestra entonces que si f es una forma propia nueva para todos los operadores de $T^0(N)$, entonces $a_1(f) \neq 0$.

Definición **1.24.** *Sea $f \in \mathcal{S}_k(\Gamma)^{new}$ una forma propia para todos los operadores de $T^0(N)$ con Γ un subgrupo de congruencia. Diremos que f es* ***normalizada*** *si $a_1(f) = 1$.*

Teorema **1.25.** *Si $f \in \mathcal{S}_k(\Gamma_1(N))^{new}$ es una forma propia normalizada de todos los operadores de $T^0(N) \Rightarrow T_n f = a_n(f) f$, $\forall n \in \mathbb{Z}^+$.*

Demostración. Consideremos $g_m = T_m f - a_m(f)f$. Como $f \in \mathcal{S}_k(\Gamma_1(N))^{new} \Rightarrow T_m f \in \mathcal{S}_k(\Gamma_1(N))^{new}$ por el Teorema 1.21 y por lo tanto $g_m \in \mathcal{S}_k(\Gamma_1(N))^{new}$.

Veamos que g_m es forma propia de todos los operadores de $T^0(N)$. En efecto, como f es forma propia de los operadores de $T^0(N)$, $Tf = \alpha f \Rightarrow$
$Tg_m = TT_m f - a_m(f))Tf = T_m Tf - a_m(f))Tf = \alpha(T_m f - a_m(f)f) = \alpha g_m$. Observar que en uno de los pasos utilizamos el Teorema 1.13 para cambiar TT_m por $T_m T$.

Por último, $a_1(g_m) = a_1(T_m f) - a_m(f)a_1(f)$. Una vez más, usando la fórmula del Teorema 1.14 tenemos que $a_1(T_m f) = a_m(f)$ y como $a_1(f) = 1 \Rightarrow a_1(g_m) = 0$ y por el Teorema 1.23, $g_m \in \mathcal{S}_k(\Gamma_1(N))^{old}$ y como ya vimos que $g_m \in \mathcal{S}_k(\Gamma_1(N))^{new} \Rightarrow g_m = 0 \Rightarrow T_m f = a_m(f)f$ y esto $\forall m \in \mathbb{Z}^+$. □

Esta página ha sido intencionalmente dejada en blanco.

Capítulo 2

Curvas Modulares y espacios de Moduli

2.1. Curvas modulares

En la Sección 1.1 definimos una acción $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\} \curvearrowright \mathcal{H}^*$.

Definición **2.1.** *Dado* Γ *subgrupo de congruencia, definimos la* ***curva modular con respecto a*** Γ *al conjunto*

$$X(\Gamma) = \{\Gamma z : z \in \mathcal{H}^*\} = \Gamma \setminus \mathcal{H}^*.$$

En el Capítulo 2 de [DS00] se prueba que $X(\Gamma)$ es una superficie de Riemann Hausdorff, conexa y compacta y en el Capítulo 7 de [DS00] que es una curva algebraica sobre $\mathbb{Q}$.

En particular nos van a interesar $X_1(N) = X(\Gamma_1(N))$ y $X_0(N) = X(\Gamma_0(N))$.

Definición **2.2.** *De manera análoga, definimos*

$$Y(\Gamma) = \{\Gamma z : z \in \mathcal{H}\} = \Gamma \setminus \mathcal{H}.$$

En particular nos van a interesar $Y_1(N) = Y(\Gamma_1(N))$ e $Y_0(N) = Y(\Gamma_0(N))$.

Es claro que $Y(\Gamma) \subseteq X(\Gamma)$.

Definición **2.3.** *Una* ***cúspide*** *es un elemento* Γq *de* $X(\Gamma)$ *con* $q \in \mathbb{Q} \cup \{\infty\}$.

Se puede ver que para cualquier subgrupo de congruencia, la cantidad de cúspides es finita. En efecto, como $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\} \curvearrowright \mathbb{Q} \cup \{\infty\}$ es una acción transitiva, la cantidad de cúspides va a ser menor o igual a $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$, y como vimos luego de la definición 1.2, $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] < \infty$.

Dado que los precisaremos en la Sección 3.3, daremos una idea de las cartas de $X(\Gamma)$, sobre todo en las cúspides. En efecto, dado $x \in \mathcal{H}^*$, existe una función holomorfa $\psi_j : T_j \to V_j$ con T_j entorno de x y V_j entorno de 0 tal que $\psi_j(x_1) = \psi_j(x_2) \Leftrightarrow \pi(x_1) = \pi(x_2)$, siendo $\pi : \mathcal{H}^* \to X(\Gamma)$ la proyección cociente. Por lo

tanto, ψ_j pasa al cociente $X(\Gamma)$, y permite definir una carta φ_j que hace conmutar el siguiente diagrama:

$$\begin{array}{ccc} & & T_j \\ & \overset{\psi_j}{\swarrow} & \downarrow \pi \\ V_j & \xleftarrow[\varphi_j]{} & U_j. \end{array} \tag{2.1}$$

Si $s \in \mathbb{Q} \cup \{\infty\}$, existe $\delta \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\delta(s) = \infty$. Sin dar detalles de prueba, tenemos que el $\mathrm{Stab}_{\delta\Gamma\delta^{-1}}(\infty) = \left[\pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)\right]$ para algún $h > 0$ (la existencia de este h está asociada a lo visto posterior a la definición 1.3) y si definimos $\rho(\tau) = e^{\frac{2\pi i \tau}{h}}$ entonces $\rho \circ \delta = \psi_j$ como en el diagrama (2.1) que lleva s en 0. El conjunto U será un entorno de s con la topología dada en el capítulo 2 de [DS00]. En la figura 2.1 se ilustra como son los entornos U en los elementos de $\mathbb{Q} \cup \{\infty\}$.

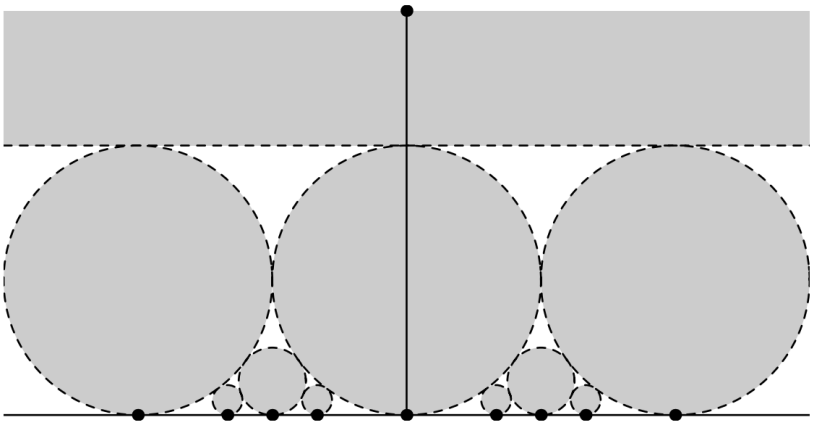


Figura 2.1: En gris, los entornos de los puntos racionales y el ∞. Se observa que son circunferencias tangentes a la recta real que dos a dos no se intersectan. (Imagen extraída de [DS00]).

2.2. Retículos e isogenias

Definición **2.4.** *Un* ***retículo*** *en* $\mathbb{C}$ *es un conjunto* $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ *con* $\omega_1, \omega_2 \in \mathbb{C}$ *tal que* $\omega_1/\omega_2 \in \mathcal{H}$. *Un* ***toro complejo*** *es el cociente* $\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}$.

Es simple chequear que los toros complejos son un grupo con la suma.

Teorema **2.5.** *Sean* $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ *y* $\Lambda' = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$ *dos retículos. Entonces* $\Lambda = \Lambda'$ *sí y solo sí* $\exists \gamma \in SL_2(\mathbb{Z})$ *tal que*

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

.

Demostración. ($\Rightarrow$) Si $\Lambda = \Lambda'$ entonces

$$\begin{cases} \omega_1' = a\omega_1 + b\omega_2 \\ \omega_2' = c\omega_1 + d\omega_2 \end{cases}$$

Tomemos $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Como $\{\omega_1, \omega_2\}$ es también base del retículo Λ' como $\mathbb{Z}$-módulo, entonces $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ y como $\gamma^{-1} = \frac{1}{\det(\gamma)} \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, entonces $\det(\gamma) = \pm 1$. Luego como ω_1/ω_2 y $\omega_1'/\omega_2' \in \mathcal{H}$, entonces $\det(\gamma) > 0$.

($\Leftarrow$) Sea $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ tal que

$$\begin{cases} \omega_1' = a\omega_1 + b\omega_2 \\ \omega_2' = c\omega_1 + d\omega_2 \end{cases}$$

Tomemos $n\omega_1' + m\omega_2' \in \Lambda'$ entonces $n\omega_1' + m\omega_2' = (na+mc)\omega_1 + (nb+md)\omega_2 \in \Lambda$ por lo que $\Lambda' \subseteq \Lambda$. Como γ es invertible, usando γ^{-1} se prueba que $\Lambda \subseteq \Lambda'$. $\square$

Definición **2.6.** *Dado $z \in \mathcal{H}$ definimos el retículo $\Lambda_z = z\mathbb{Z} \oplus \mathbb{Z}$.*

Definición **2.7.** *Una **isogenia** es un morfismo de grupos holomorfo entre dos toros complejos.*

Teorema **2.8.** *Si $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ es una isogenia $\Rightarrow \exists m \in \mathbb{C}$ $/ m\Lambda \subseteq \Lambda'$ y $\varphi(z + \Lambda) = mz + \Lambda'$. Además, φ es invertible $\Leftrightarrow m\Lambda = \Lambda'$.*

Demostración. Lo primero es utilizar algún teorema de levantamiento de Topología Algebraica para pasar φ a una función $\tilde{\varphi} : \mathbb{C} \to \mathbb{C}$ holomorfa, de manera de que el siguiente diagrama conmute:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{\varphi}} & \mathbb{C} \\ \downarrow{\scriptstyle \pi_\Lambda} & & \downarrow{\scriptstyle \pi_{\Lambda'}} \\ \mathbb{C}/\Lambda & \xrightarrow{\varphi} & \mathbb{C}/\Lambda'. \end{array}$$

La proposición 1.33 de [Hat01] nos asegura la existencia de una $\tilde{\varphi}$. A continuación damos una idea de la construcción de $\tilde{\varphi}$:

Sea $x_0 \in \mathbb{C}$ un punto base en $\mathbb{C}$ y $x \in \mathbb{C}$ un punto arbitrario. Sea $\gamma : [0,1] \to \mathbb{C}$ una curva tal que $\gamma(0) = x_0$ y $\gamma(1) = x$ (existe porque $\mathbb{C}$ es conexo por caminos) y consideremos $\varphi \circ \pi_\Lambda \circ \gamma$ la imagen de γ por $\varphi \circ \pi_\Lambda$.

Sea $y_0 = \varphi \circ \pi_\Lambda(x_0)$. Como $\pi_{\Lambda'}$ tiene infinitas preimágenes para y_0, elijamos una que denotaremos $\widetilde{y_0}$. Una vez elegido $\widetilde{y_0}$, existe una única curva $\widetilde{\gamma}$ en $\mathbb{C}$ tal que $\widetilde{\gamma}(0) = \widetilde{y_0}$ y $\pi_{\Lambda'}(\widetilde{\gamma}) = \varphi \circ \pi_\Lambda \circ \gamma$. Definimos $\widetilde{\varphi}(x) = \widetilde{\gamma}(1)$.

Para ver que está bien definida consideremos $\gamma' : [0,1] \to \mathbb{C}$ otra curva tal que $\gamma'(0) = x_0$ y $\gamma'(1) = x$. Como $\mathbb{C}$ es simplemente conexo, existe una homotopía γ_s tal que $\gamma_0 = \gamma$ y $\gamma_1 = \gamma'$. Como φ y π_Λ son continuas, γ_s pasa a una homotopía $\varphi \circ \pi_\Lambda \circ \gamma_s$ en $\mathbb{C}/\Lambda'$ y por tanto, como el punto base $\widetilde{y_0}$ es el mismo, entonces $\widetilde{\gamma}(1) = \widetilde{\gamma'}(1)$. Finalmente $\widetilde{\varphi}$ es holomorfa porque $\pi_{\Lambda'}$ tiene inversa local holomorfa.

Si tomamos $\lambda \in \Lambda$ y consideramos $\psi_\lambda(z) = \tilde{\varphi}(z+\lambda) - \tilde{\varphi}(z)$, entonces ψ_λ es holomorfa y solo toma valores en Λ', y por lo tanto ψ_λ es constante dado que Λ' es un conjunto discreto. Esto lleva a que dado $\lambda \in \Lambda$, $\exists \lambda' \in \Lambda'$ tal que $\tilde{\varphi}(z+\lambda) = \tilde{\varphi}(z)+\lambda'$.

Si derivamos, $\tilde{\varphi}'(z+\lambda) = \tilde{\varphi}'(z)$ lo que muestra que $\tilde{\varphi}'$ es Λ-periódica y holomorfa, y por tanto acotada, y por Liouville, $\tilde{\varphi}'$ es constante $\Rightarrow \tilde{\varphi}(z) = mz + b$. Dado que se que tiene que cumplir que $\tilde{\varphi}(z+\lambda) = \tilde{\varphi}(z) + \lambda' \Rightarrow mz + m\lambda + b = mz + b + \lambda' \Rightarrow m\lambda = \lambda'$ y esto para $\forall \lambda \in \Lambda \Rightarrow m\Lambda \subseteq \Lambda'$. Finalmente, como queremos que sea un morfismo, $b \in \Lambda'$.

Para la segunda parte, el directo, veamos que si $m\Lambda \subset \Lambda' \Rightarrow \exists z \in \Lambda'$ tal que $z/m \notin \Lambda \Rightarrow \varphi(z/m + \Lambda) = z + \Lambda' = \Lambda'$ puesto que $z \in \Lambda'$. Dado que $\varphi(\Lambda) = \Lambda'$, tenemos entonces que φ no es inyectiva, lo que es absurdo. Para el recíproco, veamos que $\psi : \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$ dado por $\psi(w+\Lambda') = m^{-1}w + \Lambda$ es el inverso de φ. En efecto, $\psi \circ \varphi(z+\Lambda) = \psi(mz+\Lambda') = z + m^{-1}\Lambda' + \Lambda = z + \Lambda$ puesto que $m^{-1}\Lambda' = \Lambda$. Del otro lado, $\varphi \circ \psi(w+\Lambda') = \varphi(m^{-1}z + \Lambda) = w + m\Lambda + \Lambda' = w + \Lambda'$ usando de vuelta que $m\Lambda = \Lambda'$. □

Si la isogenia es no nula, el núcleo debe ser finito, puesto que como el toro complejo es compacto, si el núcleo es infinito debe ser la isogenia nula.

Definición **2.9.** *Sea φ un morfismo no nulo. Definimos el* ***grado*** *de φ como* $\deg(\varphi) = \left|\varphi^{-1}(y)\right|$ *con $y \in Im(\varphi)$.*

Dado que φ es un morfismo, el grado queda bien definido y de hecho $\deg(\varphi) = |\ker(\varphi)|$ (en característica 0).

Definición **2.10.** *Sea $N \in \mathbb{N}$. Definimos el morfismo $[N] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ dado por $[N](z+\Lambda) = Nz + \Lambda$.*

Definición **2.11.** *Dada $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ una isogenia tal que $\varphi(z+\Lambda) = mz + \Lambda'$, definimos la* ***isogenia dual*** *como $\hat{\varphi} : \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$ /$\hat{\varphi}(z+\Lambda') = \frac{deg(\varphi)}{m} z + \Lambda$.*

Teorema **2.12.** *Sea φ una isogenia y $\hat{\varphi}$ su isogenia dual, y $N \in \mathbb{N}$. Entonces:*

1. $\deg([N]) = N^2$.
2. $\hat{\varphi}\varphi = [deg(\varphi)]$.
3. $\deg(\hat{\varphi}) = \deg(\varphi)$.
4. $\hat{\hat{\varphi}} = \varphi$.

Demostración. Trivial. □

2.3. Espacios de Moduli

Consideremos ahora un par (E, C) donde E es un toro complejo en $\mathbb{C}$ y C es un subgrupo cíclico en E de orden N. Definimos la equivalencia $\sim_0$ donde $(E, C) \sim_0 (E', C') \Leftrightarrow \exists \varphi : E \to E'$ isomorfismo holomorfo tal que $\varphi(C) = C'$.

Definición **2.13.** *El* ***espacio de Moduli para*** $\Gamma_0(N)$ *es el conjunto* $S_0(N) = \{(E, C) : E \text{ toro complejo, } C \text{ cíclico de orden } N \text{ de } E\}/\sim_0$.

De manera análoga, consideremos un par (E, Q) donde E es un toro complejo en $\mathbb{C}$ y Q punto en E de orden N. Definimos la equivalencia $\sim_1$ donde $(E, Q) \sim_1 (E', Q') \Leftrightarrow \exists \varphi : E \to E'$ isomorfismo holomorfo tal que $\varphi(Q) = Q'$.

Definición **2.14.** *El* ***espacio de Moduli para*** $\Gamma_1(N)$ *es el conjunto* $S_1(N) = \{(E, Q) : E \text{ toro complejo, } Q \text{ punto de orden } N \text{ en } E\}/\sim_1$.

Teorema **2.15.** *Sea N entero positivo.*

1. $S_0(N) = \{[\mathbb{C}/\Lambda_z, \langle 1/N + \Lambda_z\rangle]_{\sim_0} : z \in \mathcal{H}\}$ *donde dos clases son equivalentes si y solo sí* $\Gamma_0(N)z = \Gamma_0(N)z'$.

   $\psi_0 : S_0(N) \to Y_0(N)$ *dado por* $\psi_0([\mathbb{C}/\Lambda_z, \langle 1/N + \Lambda_z\rangle]_{\sim_0}) = \Gamma_0(N)z$ *es una biyección.*

2. $S_1(N) = \{[\mathbb{C}/\Lambda_z, 1/N + \Lambda_z]_{\sim_1} : z \in \mathcal{H}\}$ *donde dos clases son equivalentes si y solo sí* $\Gamma_1(N)z = \Gamma_1(N)z'$

   $\psi_1 : S_1(N) \to Y_1(N)$ *dado por* $\psi_1([\mathbb{C}/\Lambda_z, \langle 1/N + \Lambda_z\rangle]_{\sim_0}) = \Gamma_1(N)z$ *es una biyección.*

El Teorema 2.15 nos dice entonces que los puntos de las curvas modulares los podemos entender como un par "toro complejo-subgrupo cíclico".

2.4. Divisores

Definición **2.16.** *Sea X una superficie de Riemann compacta. Un* ***divisor*** *es una suma formal de múltiplos enteros de puntos de X:*

$$D = \sum_{x \in X} n_x x$$

donde $n_x \in \mathbb{Z}$, $\forall x \in X$ *y* $\#\{x \in X : n_x \neq 0\} < \infty$

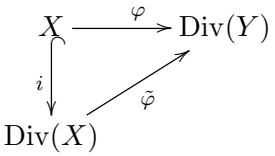
Llamaremos $\mathrm{Div}(X)$ *al conjunto de los divisores de X.*

Observaciones:

- $\mathrm{Div}(X)$ es un grupo abeliano libre con la suma $\sum_{x \in X} n_x x + \sum_{x \in X} n'_x x = \sum_{x \in X} (n_x + n'_x)x$

- $\mathrm{Div}(X)$ se puede ver como $\mathbb{Z}$-módulo con el producto $n.\left(\sum_{x\in X} n_x x\right) = \sum_{x\in X}(nn_x)x$
- $\mathrm{Div}(X)$ tiene un orden parcial dado por $\sum_{x\in X} n'_x x \geq \sum_{x\in X} n_x x \Leftrightarrow n'_x \geq n_x$, $\forall x \in X$.

Teorema **2.17.** *Sean X, Y dos superficies de Riemann compactas. Si $\varphi : X \to \mathrm{Div}(Y) \Rightarrow \exists!\ \widetilde{\varphi} : \mathrm{Div}(X) \to \mathrm{Div}(Y)$ morfismo tal que el siguiente diagrama conmuta:*



Demostración. Basta con definir $\widetilde{\varphi}(\sum_{x\in X} n_x x) = \sum_{x\in X} n_x \varphi(x)$.

□

2.4.1. Pullback y Pushforward entre divisores

Sea $h : X \to Y$ una función holomorfa no constante entre superficies de Riemann compactas. Sean (U, φ) una carta de x y $(\widetilde{U}, \widetilde{\varphi})$ una carta de $h(x)$. Nos será útil el siguiente teorema:

Teorema **2.18** (Teorema del comportamiento local)**.** *Sea $g : \Omega \subseteq \mathbb{C} \to \mathbb{C}$ holomorfa no contante, $z_0 \in \Omega$ y $m = \min\left\{k \geq 1 : g^{(k)}(z_0) \neq 0\right\}$. Entonces, existen un entorno abierto U de z_0 y $\psi : U \to \mathbb{C}$ biholomorfa tal que $g(z) = g(z_0) + (\psi(z))^m$*

El Teorema 2.18 nos dice que localmente g es m a 1. Si tomamos $g = \widetilde{\varphi} \circ h \circ \varphi^{-1}$ podemos definir el **grado de ramificación** (e_x) de h en x como el m del Teorema 2.18. El natural e_x queda bien definido ya que como las cartas son biholomorfas, no depende de ellas.

Diremos que un punto x es **ramificado** si $e_x > 1$. El Teorema 2.18 nos muestra también que los puntos ramificados son aislados. En efecto, esto es porque g es localmente z^{e_x} y el único punto ramificado de z^{e_x} es el 0. Otra forma es observar que los puntos ramificados son ceros de g', y como g es no constante, g' no es cero y por lo tanto tiene ceros aislados.

Por otro lado es importante mencionar que la cantidad de preimágenes de cualquier $y \in Y$ es finita. En efecto, como h es holomorfa no constante $h^{-1}(y)$ no acumula en X y como X es compacto, $h^{-1}(y)$ es un conjunto finito.

Teorema **2.19.** *Sea $h : X \to Y$ holomorfa no constante entre superficies de Riemann Hausdorff, compactas y conexas. Entonces $\sum_{x\in h^{-1}(y)} e_x$ es constante $\forall y \in Y$.*

Demostración. Sea $\mathcal{E} = \{x \in X : e_x > 1\}$, $X' = X \setminus \mathcal{E}$, $Y' = Y \setminus h(\mathcal{E})$. Dado que $\#\mathcal{E} < \infty$ pues $\mathcal{E}$ es aislado en X que es un conjunto compacto y que X, Y son conexas, entonces X', Y' son conexas, y si tomamos $y \in Y'$, como X es Hausdorff y $\#h^{-1}(y) < \infty$, encontramos entornos disjuntos dos a dos para las preimágenes de y en donde h es invertible. Como $e_x = 1, \forall x \in h^{-1}(y)$ obtenemos que la función $g : Y' \to \mathbb{N}$ / $g(y) = \#h^{-1}(y)$ es localmente constante en el conexo Y' y por tanto g es constante y se extiende a todo Y de forma continua. Por tanto, si ahora tomamos $y \in Y$, tenemos $y' \in Y'$ en un entorno de y, y por el Teorema 2.18, dado $x \in h^{-1}(y)$, y' es la imagen de e_x puntos x' en un entorno de x, donde para cada uno de esos x', $e_{x'} = 1$, lo que prueba lo buscado. □

Definición **2.20.** *Dada $h : X \to Y$ holomorfa no constante entre superficies de Riemann Hausdorff compactas y conexas, definimos* $\deg(h)$ *como la constante del Teorema 2.19.*

Definición **2.21.** *Dados X, Y superficies de Riemann compactas y $h : X \to Y$ holomorfa no constante, definimos el* ***pullback*** *entre divisores como:*

$$h^* : \mathrm{Div}(Y) \to \mathrm{Div}(X) \ / \ h^*(y) = \sum_{x \in h^{-1}(y)} e_x x.$$

La función h^* queda bien definida puesto que la cantidad de preimágenes de cualquier punto de Y es finita. Usando el Teorema 2.17, se extiende luego para $\mathrm{Div}(Y)$.

Definición **2.22.** *Dados X, Y superficies de Riemann compactas y $h : X \to Y$ holomorfa no constante, definimos el* ***pushforward*** *entre divisores como:*

$$h_* : \mathrm{Div}(X) \to \mathrm{Div}(Y) \ / \ h_*(x) = h(x).$$

Usando el Teorema 2.17, h_* se extiende a $\mathrm{Div}(X)$.

2.4.2. Grupo de Picard

Definimos el morfismo $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ dado por $\deg(\sum_{x \in X} n_x x) = \sum_{x \in X} n_x$, y llamamos $\mathrm{Div}^0(X) = \ker(\deg)$.

Definición **2.23.** *Sea $f : X \to \widehat{\mathbb{C}}$ meromorfa. Definimos el* ***divisor de*** *f como:*

$$\mathrm{div}(f) = \sum_{x \in X} \nu_x(f) x,$$

donde $\nu_x(f)$ es el orden de cero o de polo de f (Si $\nu_x(f) > 0$, f tiene un cero en x y si $\nu_x(f) < 0$, f tiene un polo en x).

Denotaremos $\mathrm{Div}^\ell(X)$ *al conjunto de los divisores de* $\mathrm{Div}^0(X)$ *que provienen de una función meromorfa f. A estos divisores los llamaremos* ***principales****.*

Dado que si $f, g : X \to \widehat{\mathbb{C}}$ son funciones meromorfas, se tiene que $\operatorname{div}(f/g) = \operatorname{div}(f) - \operatorname{div}(g)$ y que $\operatorname{div}(f) \in \operatorname{Div}^0(X) \Rightarrow \operatorname{Div}^\ell(X)$ es un subgrupo de $\operatorname{Div}^0(X)$.

Definición **2.24.** *El* ***grupo de Picard*** *es el conjunto* $\operatorname{Pic}^0(X) = \operatorname{Div}^0(X)/\operatorname{Div}^\ell(X)$.

Observemos que si el género de X es positivo ($g_X > 0$), entonces fijado $x_0 \in X$, tenemos una inclusión i tal que $X \overset{i}{\hookrightarrow} \operatorname{Pic}^0(X)$, dada por $i(x) = [x - x_0]$. Para demostrarlo utilicemos la fórmula de Riemann-Hurwitz, que enuncia que si $h : X \to Y$ es una función holomorfa no constante entre superficies de Riemann compactas, g_X es el género de X y g_Y es el género de Y entonces:

$$2g_X - 2 = \deg(h)(2g_Y - 2) + \sum_{x \in X} (e_x - 1)$$

Para ver que i es un encaje, alcanza con ver que dados dos puntos $x, x' \in X$, no existe una función meromorfa $f : X \to \mathbb{C}$ tal que $x' - x_0 = x - x_0 + \operatorname{div}(f)$, o lo que es lo mismo, no existe f una función meromorfa tal que $\operatorname{div}(f) = x' - x$.

Si existiese tal f, entonces $\deg(f) = 1$, y por lo tanto $e_x = 1$ para todo $x \in X$. Utilizando la fórmula de Riemann-Hurtwitz nos queda que $2g_x - 2 = 0$, pero esto no puede ser si $g_x > 0$.

Veamos ahora que los mapas h_* y h^* descienden a Grupos de Picard:

Teorema **2.25.** *Sea X, Y superficies de Riemann compactas y $h : X \to Y$ una función holomorfa no constante. Entonces:*

1. $h_*(\operatorname{Div}^0(X)) \subseteq \operatorname{Div}^0(Y)$ *y* $h^*(\operatorname{Div}^0(Y)) \subseteq \operatorname{Div}^0(X)$.
2. $h_*(\operatorname{Div}^\ell(X)) \subseteq \operatorname{Div}^\ell(Y)$ *y* $h^*(\operatorname{Div}^\ell(Y)) \subseteq \operatorname{Div}^\ell(X)$.

Demostración. 1. Sea $D = \sum_{x \in X} n_x x \in \operatorname{Div}^0(X) \Rightarrow \deg(h_*(D)) = \sum_{x \in X} n_x = \deg(D) = 0$.
Si ahora $D = \sum_{y \in Y} n_y y \in \operatorname{Div}^0(Y) \Rightarrow \deg(h^*(D)) = \sum_{y \in Y} n_y \sum_{x \in h^{-1}(y)} e_x = \deg(h) \sum_{y \in Y} n_y = \deg(h)\deg(D) = 0$.

2. Sea $f : X \to \widehat{\mathbb{C}}$ meromorfa. $h_*(\operatorname{div}(f)) = \sum_{x \in X} \nu_x(f) h(x) =$
$= \sum_{y \in Y} \left[\sum_{x \in h^{-1}(y)} \nu_x(f)\right] y$. Defino $\operatorname{norm}_h f(y) = \prod_{x \in h^{-1}(y)} f(x)^{e_x}$. Entonces, $\operatorname{norm}_h f$ es meromorfa y $\nu_y(\operatorname{norm}_h f) = \sum_{x \in h^{-1}(y)} \nu_x(f)$ y entonces $h_*(\operatorname{div}(f)) = \operatorname{div}(\operatorname{norm}_h f)$.
Si ahora $f : Y \to \widehat{\mathbb{C}}$ meromorfa, $h^*(\operatorname{div}(f)) = \sum_{y \in Y} \nu_y(f) \sum_{x \in h^{-1}(y)} e_x x$. Ahora, si tomamos $f \circ h : X \to \widehat{\mathbb{C}}$, $f \circ h$ meromorfa y $\nu_x(f \circ h) = e_x \nu_{h(x)}(f) \Rightarrow \operatorname{div}(f \circ h) = \sum_{x \in X} e_x \nu_{h(x)}(f) x = \sum_{y \in Y} \nu_y(f) \sum_{x \in h^{-1}(y)} e_x x = h^*(\operatorname{div}(f))$. □

Los divisores y el Grupo de Picard pueden extenderse a curvas algebraicas proyectivas no singulares sobre cuerpos arbitrarios y tendremos nociones equivalentes

para las definiciones 2.20, 2.21 y 2.22. El siguiente resultado muestra que en curvas algebraicas proyectivas podemos obtener un representante para una clase del Grupo de Picard, evitando un conjunto finito de puntos. Este resultado nos será útil en la Sección 4.3.

Teorema **2.26.** *Sea C una curva algebraica proyectiva no singular sobre un cuerpo k y $S \subseteq C$ un subconjunto finito. Entonces, dado $[D] \in \mathrm{Pic}^0(C)$, existe un representante $\sum_{P\in C} n_P P \in [D]$ tal que $n_P = 0\ \forall P \in S$.*

Demostración. Sin dar detalles de la contrucción, utilizando herramientas de Geometría Algebraica se pueden construir funciones $\{F_P\}_{P\in S}$ tal que $\nu_P(F_P) = 1$ y $\nu_Q(F_P) = 0$ para todo $Q \in S \setminus \{P\}$. Luego, dado $D = \sum_{P\in S} n_P P + \sum_{P\in C\setminus S} n_P P$, definamos $F = \prod_{P\in S}(F_P)^{n_P} \Rightarrow \mathrm{div}(F) = \sum_{P\in S} n_P P + D'$, donde $D'|_S = 0$. La existencia de D' viene dada del hecho de que $\deg(\mathrm{div}(F)) = 0$. Tomando clases, $[D] = [D - \mathrm{div}(F)] = \sum_{P\in C\setminus S} n_P P - D'$, y por tanto, $D - \mathrm{div}(F)|_S = 0$. □

2.5. Operadores de Hecke

El objetivo de esta sección es mostrar que los Operadores de Hecke se pueden definir en divisores de curvas modulares, Grupos de Picard y Espacios de Moduli, de una forma análoga a la hecha en el Capítulo 1 para formas modulares.

Sean Γ_1, Γ_2 dos subgrupos de congruencia, $\alpha \in GL_2^+(\mathbb{Q})$ y $\{\beta_i\}_{i=1}^r$ un conjunto de representantes de $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$. Definimos $[\Gamma_1\alpha\Gamma_2]$ para divisores de curvas modulares como:

$$[\Gamma_1\alpha\Gamma_2] : X(\Gamma_2) \to \mathrm{Div}(X(\Gamma_1)) \text{ dado por } \Gamma_2 z \mapsto \sum_{i=0}^{r} \Gamma_1\beta_i(z).$$

Luego, $[\Gamma_1\alpha\Gamma_2]$ se extiende rápidamente a un morfismo de $\mathrm{Div}(X(\Gamma_2))$ usando el Teorema 2.17, donde queda:

$$\sum_z n_z \Gamma_2 z \mapsto \sum_z n_z \sum_{i=0}^{r} \Gamma_1\beta_i(z).$$

2.5.1. Operadores de Hecke en Grupos de Picard

Veamos que $[\Gamma_1\alpha\Gamma_2]$ se puede ver como composición de pushforwards y pullbacks. Para ello, definimos $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$ y $\Gamma_3' = \alpha\Gamma_3\alpha^{-1} = \Gamma_1 \cap \alpha\Gamma_2\alpha^{-1}$. Sea $\{\beta_i\}_{i=1}^r$ un conjunto de representantes de $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$, se puede probar que si definimos $\delta_i = \alpha^{-1}\beta_i$, entonces $\{\delta_i\}_{i=1}^r$ es un conjunto de representantes de $\Gamma_3 \setminus \Gamma_2$.

Como $\Gamma_3 \leq \Gamma_2$ y $\Gamma_3' \leq \Gamma_1$, tenemos definidas las proyecciones $\pi_1 : X(\Gamma_3') \to X(\Gamma_1)$, $\pi_2 : X(\Gamma_3) \to X(\Gamma_2)$. Definiendo $\hat{\alpha} : X(\Gamma_3) \mapsto X(\Gamma_3')$ / $\hat{\alpha}(\Gamma_3 z) = \Gamma_3'\alpha(z)$ obtenemos el siguiente diagrama:

$$\begin{array}{ccc} X(\Gamma_3) & \xrightarrow{\hat{\alpha}} & X(\Gamma_3') \\ {\scriptstyle \pi_2}\downarrow & & \downarrow{\scriptstyle \pi_1} \\ X(\Gamma_2) & \overset{[\Gamma_1\alpha\Gamma_2]}{\dashrightarrow} & X(\Gamma_1). \end{array}$$

Veamos que $[\Gamma_1\alpha\Gamma_2] = \pi_{1,*} \circ \hat{\alpha}_* \circ \pi_2^*$. En efecto

$$\Gamma_2 z \overset{\pi_2^*}{\mapsto} \sum_{i=0}^{r} \Gamma_3\delta_i(z) \overset{\hat{\alpha}_*}{\mapsto} \sum_{i=0}^{r} \Gamma_3'\alpha\delta_i(z) = \sum_{i=0}^{r} \Gamma_3'\beta_i(z) \overset{\pi_{1,*}}{\mapsto} \sum_{i=0}^{r} \Gamma_1\beta_i(z).$$

Cabe destacar que e_x no aparece en el primer término porque al sumar en todas las coclases, ya se está contando e_x veces en caso que un elemento tenga multiplicidad.

Usando el Teorema 2.25, vemos que $\pi_{1,*}$, $\hat{\alpha}_*$ y π_2^* descienden a grupos de Picard, y por ende $[\Gamma_1\alpha\Gamma_2]$ desciende a grupos de Picard. En particular, quedan definidos $T_p : \mathrm{Pic}^0(X_1(N)) \to \mathrm{Pic}^0(X_1(N))$ cuando $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$ y $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ y $\langle n \rangle$ cuando $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$ y $\alpha = \left(\begin{smallmatrix} a & b \\ rN & n \end{smallmatrix}\right)$.

2.5.2. Operadores de Hecke en Espacios de Moduli

Por otro lado, y a raíz de la Sección 2.5, podemos ver a $[\Gamma_1(N)\alpha\Gamma_1(N)] : \mathrm{Div}(S_1(N)) \to \mathrm{Div}(S_1(N))$. Sea $[E, Q] \in S_1(N)$. Si usamos el Teorema 2.15 tenemos que:

$$[E,Q] \simeq [\mathbb{C}/\Lambda_z, 1/N + \Lambda_z] \overset{\psi_1}{\longmapsto} \Gamma_1(N)z \overset{[\Gamma_1\alpha\Gamma_2]}{\longmapsto} \sum_{i=0}^{r} \Gamma_1(N)\beta_i(z) \overset{\psi_1^{-1}}{\longmapsto} \sum_{i=0}^{r} \left[\mathbb{C}/\Lambda_{\beta_i(z)}, 1/N + \Lambda_{\beta_i(z)}\right].$$

Si pensamos en T_p, el Teorema 1.11 muestra que tenemos dos casos. Analicemos el caso cuando $p \nmid N$ (que es el caso que nos interesa en la Sección 4.3).

Si $\beta_j = \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)$, entonces $\beta_j(z) = \frac{z+j}{p}$. Si $\beta_\infty = \left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$, entonces $\beta_\infty(z) = \frac{mpz+n}{Npz+p}$. Se puede verificar que $\Lambda_z \subseteq \Lambda_{\beta_i(z)}$ y entonces $\Lambda_{\beta_i(z)}/\Lambda_z = C_i$ es un subgrupo de $\mathbb{C}/\Lambda_z$. Utilizando el Tercer Teorema de Isomorfismo tenemos que $E/C = (\mathbb{C}/\Lambda_z)/(\Lambda_{\beta_i(z)}/\Lambda_z) = \mathbb{C}/\Lambda_{\beta_i(z)}$.

Tenemos entonces los subgrupos $C_0, ..., C_{p-1}, C_\infty$, uno por cada matriz β_j en el conjunto de representantes. Para $j \neq \infty$, $\beta_j(z) + \Lambda_z$ es generador del subgrupo C_j. Para C_∞, tenemos que $C_\infty = (Nz+1)\Lambda_{\beta_\infty(z)}$ y entonces

$$C_\infty = \frac{1}{p}\left((mpz+n)\mathbb{Z} \oplus (Npz+p)\mathbb{Z}\right).$$

Usando el Teorema 2.5, con la matriz $\left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)$ tenemos que

$$C_\infty = \frac{1}{p}\left(pz\mathbb{Z} \oplus \mathbb{Z}\right) = z\mathbb{Z} \oplus \frac{1}{p}\mathbb{Z}.$$

Por lo tanto C_∞ es generado por $\frac{1}{p} + \Lambda_z$.

Dado que cada generador tiene orden p, entonces los C_j son subgrupos de orden p. Por otro lado, dado que $p \nmid N$ y que $Q = 1/N + \Lambda_z$, entonces $C_j \cap \langle Q \rangle = \{0\}$ para todo j, y además, los C_j son disjuntos dos a dos.

Juntando todo, podemos contar la cantidad de elementos que implican estos subgrupos de la siguiente manera: tenemos $p+1$ subgrupos con intersección trivial dos a dos, por lo que hay $p-1$ elementos diferentes por cada uno, y todos comparten al 0, de forma que el total de elementos es $1 + (p+1)(p-1) = p^2$ que es la cantidad de elementos de orden p en el toro complejo $\mathbb{C}/\Lambda_z$. Esto implica que $C_0, ..., C_{p-1}, C_\infty$ son todos los subgrupos de orden p en el toro complejo.

Por lo tanto, si $p \nmid N$ tenemos que:

$$T_p[E, Q] = \sum_{\substack{C \leq E \\ |C| = p}} [E/C, Q + C]. \tag{2.2}$$

En la figura 2.2, se muestra un ejemplo de los subgrupos de orden 5 para un retículo $\mathbb{C}/\Lambda_z$.

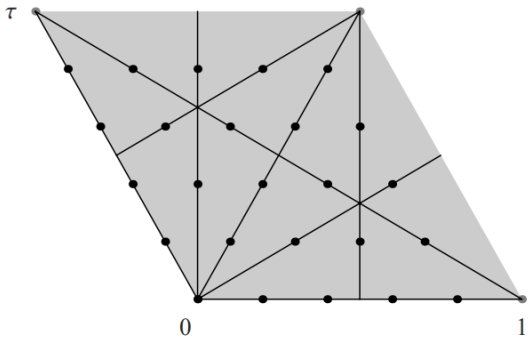


Figura 2.2: En la figura se muestra en $\mathbb{C}/\Lambda_z$ los seis 5-subgrupos cíclicos unidos con rectas (Imagen extraída de [DS00]).

Si trabajamos con el operador diamante $\langle n \rangle$, y tenemos $\alpha = \left(\begin{smallmatrix} a & b \\ rN & n \end{smallmatrix}\right) \in \Gamma_0(N)$ una matriz asociada al operador diamante entonces

$$[E, Q] \simeq [\mathbb{C}/\Lambda_z, 1/N + \Lambda_z] \overset{\psi_1}{\longmapsto} \Gamma_1(N)z \overset{\langle n \rangle}{\longmapsto} \Gamma_1(N)\alpha(z) \overset{\psi_1^{-1}}{\longmapsto} \left[\mathbb{C}/\Lambda_{\alpha(z)}, 1/N + \Lambda_{\alpha(z)}\right].$$

Consideremos el retículo $\Lambda = (az+b)\mathbb{Z} \oplus (rNz+n)\mathbb{Z}$. Dado que

$$\begin{pmatrix} az+b \\ rNz+n \end{pmatrix} = \alpha \begin{pmatrix} z \\ 1 \end{pmatrix},$$

por el Teorema 2.5, $\Lambda = \Lambda_z$.

Observemos que $\Lambda_{\alpha(z)} = \alpha(z)\mathbb{Z} \oplus \mathbb{Z} = \frac{az+b}{rNz+n}\mathbb{Z} \oplus \mathbb{Z}$ y que si definimos $\varphi : \mathbb{C}/\Lambda_{\alpha(z)} \to \mathbb{C}/\Lambda$ una isogenia entre toros complejos dada por $\varphi(\omega + \Lambda_{\alpha(z)}) = (rNz+n)\omega + \Lambda$, entonces por el Teorema 2.8, φ es un isomorfismo de toros complejos que manda $\frac{1}{N} + \Lambda_{\alpha(z)} \mapsto \frac{rNz+n}{N} + \Lambda = rz + \frac{n}{N} + \Lambda_z = \frac{n}{N} + \Lambda_z$. Por lo tanto, en término de elementos del espacio de Moduli, $[\mathbb{C}/\Lambda_{\alpha(z)}, 1/N + \Lambda_{\alpha(z)}] = [\mathbb{C}/\Lambda_z, n/N + \Lambda_z]$ lo que prueba que:

$$\langle n \rangle [E, Q] = [E, [n]Q]. \tag{2.3}$$

Capítulo 3

Curvas Elípticas y Variedades Abelianas

3.1. Curvas Elípticas

Definición **3.1.** *Una* ***curva elíptica*** *sobre un cuerpo k es una ecuación*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

no singular con $a_1, ..., a_6 \in k$.

Llamaremos $E(\overline{k}) = \left\{(x, y) \in \overline{k}^2 : E(x, y) = 0\right\} \cup \{\infty\}$.

Se define el **discriminante** $\Delta(E)$ como un polinomio en los coeficientes de la curva elíptica, que cumple que E es no singular sí y solo sí $\Delta(E) \neq 0$.

Si la característica del cuerpo no es ni 2 ni 3, mediante cambios de variable, puede llevarse E a la forma

$$y^2 = x^3 + ax + b \tag{3.1}$$

con $a, b \in k$. Esta reducción se conoce como la **forma normal de Weierstrass**. Para las curvas de esta forma, $\Delta = 4a^3 + 27b^2$.

Definición **3.2.** *Sea E una curva elíptica en su forma normal de Weiertrass. Definimos el* ***invariante*** $j(E) = -1728\frac{a^3}{\Delta} = 1728\frac{a^3}{4a^3+27b^2}$.

El término "1728" está asociado a una relación del invariante $j(E)$ con la forma automorfa j, que es una división entre dos formas modulares de peso 12 que utiliza también el término "1728" para remover factores comunes.

Realizaremos cambios de variables para identificar curvas elípticas con el mismo invariante j. Un cambio de variable será **admisible** si es de la forma:

$$x = u^2x' \ , \ y = u^3y' \text{ con } u \in k^*.$$

Este cambio de variable lleva ecuaciones de Weierstrass en ecuaciones de Weierstrass, puesto que hecho el cambio de variable, obtenemos la curva elíptica

$$y'^2 = x'^3 + au^{-4}x' + u^{-6}b. \tag{3.2}$$

Si llamamos Δ al discriminante de la ecuación de (3.1) y Δ' al de la ecuación (3.2) $\Rightarrow \Delta' = \Delta/u^{12}$, y si utilizando la misma notación para los invariantes, tenemos que $j' = j$.

Si en particular, k es algebraicamente cerrado, $ab \neq 0$ y tomamos $u = (\frac{b}{a})^{1/2}$, obtenemos la curva elíptica

$$y^2 = x^3 + \frac{a^3}{b^2}x + \frac{a^3}{b^2}.$$

Escribiendo $\frac{a^3}{b^2}$ en función de su invariante j, nos queda

$$y^2 = x^3 - \frac{1}{4}\left(\frac{27j}{j-1728}\right)x - \frac{1}{4}\left(\frac{27j}{j-1728}\right). \tag{3.3}$$

Las curvas elípticas no singulares presentan una ley de grupo que se ejemplifica en la figura 3.1 para un cuerpo $k \subseteq \mathbb{C}$.

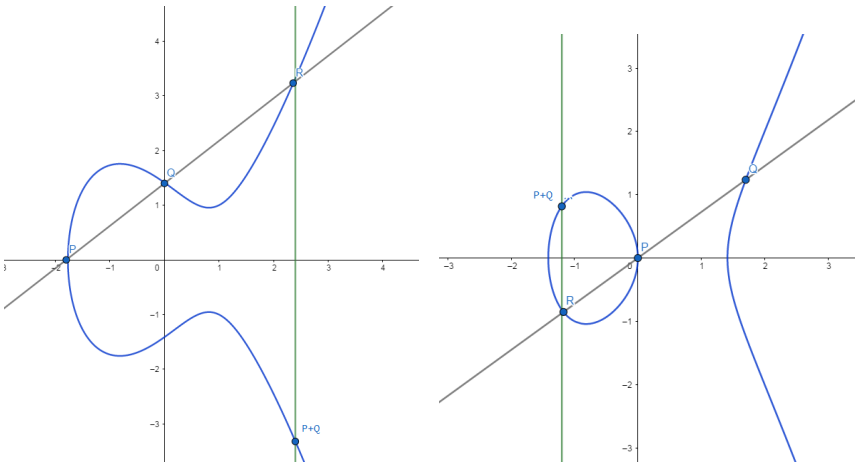


Figura 3.1: Ley de grupo en una curva elíptica

Para obtener la suma de dos puntos P y Q, tomemos la recta que pasa por ellos. Como la curva elíptica es un polinomio de grado 3 en x, tiene un tercer punto R que está en la recta y en la curva elíptica. Simetrizando R con el eje real, obtenemos el punto $P+Q$. Cabe considerar que ∞ es el nulo del grupo y cuando se suma $P+P$, la recta que se toma es la tangente por P (que está bien definida porque la curva elíptica es no singular). Con esta operación, las curvas elípticas se transforman en un grupo abeliano. En particular, podremos considerar isomorfismos de grupos entre dos curvas no singulares, y de hecho se puede demostrar que dos curvas E y

E' son isomorfas $\Leftrightarrow j(E) = j(E')$, lo que lleva a que todas las curvas elípticas se pueden llevar a alguna curva elíptica isomorfa de la forma de la ecuación (3.3).

Dado $N \in \mathbb{N}$, definimos $[N] : E(\overline{k}) \to E(\overline{k})$ como

$$[N](P) = \underbrace{P + ... + P}_{N veces}.$$

El subgrupo $\ker([N])$ serán los puntos de N-torsión. Escribiremos $E[N] = \ker([N]) \leq E(\overline{k})$.

Teorema **3.3.** *Sea E una curva elíptica sobre k y $N \in \mathbb{N}$ tal que $N = \prod_{i=1}^{r} p_i^{e_i}$ con $p_i \in \mathbb{P}, \forall i = 1, ..., r$. Entonces:*

1. $E[N] \simeq \prod_{i=1}^{r} E[p_i^{e_i}]$.
2. *Si* $p \neq char(k) \Rightarrow E[p^e] \simeq (\mathbb{Z}/p^e\mathbb{Z})^2$.
3. *Si* $char(k) \nmid N \Rightarrow E[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$.
4. *Si* $p = char(k) \Rightarrow E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z}$ *ó* $E[p^e] = \{0\}$.

En particular, si $p = char(k)$ y $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$, diremos que E es **ordinaria** y si $E[p] = \{0\}$ diremos que E es **supersingular**.

Los toros complejos están conectados con las curvas elípticas sobre $\mathbb{C}$. Dado Λ un retículo sobre $\mathbb{C}$, llamaremos función $\wp_\Lambda$ **de Weierstrass** a la función $\wp_\Lambda : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ dada por:

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right),$$

donde $\Lambda^* = \Lambda \setminus \{0\}$.

Teorema **3.4.** *La función $\wp_\Lambda$ es meromorfa en $\mathbb{C}$, Λ-periódica y el par $(\wp_\Lambda, \wp'_\Lambda)$ satisface la curva elíptica $E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ sobre $\mathbb{C}$, donde $g_2(\Lambda) = 60G_4(\Lambda)$ y $g_3(\Lambda) = 140G_6(\Lambda)$, siendo $G_k(\Lambda) = \sum_{z \in \Lambda \setminus \{0\}} \frac{1}{z^k}$.*

El Teorema 3.5 resume una importante conexión entre la estructura de las curvas elípticas y los toros complejos:

Teorema **3.5.**
1. *Sea Λ un retículo y $E_\Lambda(\mathbb{C})$ las soluciones complejas de la curva elíptica $E_\Lambda \Rightarrow E_\Lambda(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ como grupos y como superficies de Riemann.*
2. *La función $\{\Lambda : \Lambda$ retículo$\} \to \left\{E : y^2 = 4x^3 - ax - b\right\}$ dada por $\Lambda \mapsto E_\Lambda$ es una biyección.*

El Teorema 3.5 nos dice entonces que toda curva elíptica sobre $\mathbb{C}$ se puede ver como un toro complejo y viceversa. Más aún, esta relación entre toros complejos y curvas elípticas nos permitirá generalizar los conceptos de isogenia, isogenia dual y operadores de Hecke a curvas elípticas sobre cualquier cuerpo k. En efecto, las isogenias serán morfismos entre curvas elípticas que verifican el Teorema 2.12, y los operadores de Hecke se generalizan a partir de las ecuaciones (2.2) y (2.3).

Por último, mencionamos sin dar una prueba, el siguiente teorema a utilizar en el Capítulo 4.

Teorema **3.6.** *Sea E una curva elíptica sobre un cuerpo k. Entonces el mapa*

$$\begin{aligned} \mathrm{Pic}^0(E) &\mapsto E, \\ \sum_{P\in E(\overline{\mathbb{F}}_p)} n_P P &\mapsto \sum_{P\in E(\overline{\mathbb{F}}_p)} [n_P]P \end{aligned}$$

es un isomorfismo de grupos, considerando en E la suma presentada en la Sección 3.1.

La prueba de este hecho se puede encontrar en el Teorema 7.3.3 de [DS00].

3.2. Jacobiano

Definición **3.7.** *Sea V un abierto de $\mathbb{C}$. Definimos el conjunto de formas diferenciales holomorfas en V a*

$$\Omega^1_{hol}(V) = \{f dz \ / \ f : V \to \mathbb{C} \text{ es holomorfa}\}.$$

Definición **3.8.** *Sean V_1, V_2 dos abiertos de $\mathbb{C}$ y $\varphi : V_1 \to V_2$ holomorfa. Definimos el* ***pullback*** *asociado a φ como*

$$\varphi^* : \Omega^1_{hol}(V_2) \to \Omega^1_{hol}(V_1) \ / \ \varphi^*(f(z_2)dz_2) = f(\varphi(z_1))\varphi'(z_1)dz_1.$$

Es simple ver que $\Omega^1_{hol}(V)$ es un $\mathbb{C}$-espacio vectorial y φ^* es una transformación lineal.

Sea X una superficie de Riemann con un atlas $\mathcal{A} = \{(\varphi_j, U_j)\}_{j\in J}$ donde $\varphi_j : U_j \to V_j \subseteq \mathbb{C}$ para cada j. Por ser una variedad, el cambio de carta es holomorfo. Llamemos $V_{j,k} = \varphi_j(U_j \cap U_k)$ y $\varphi_{k,j} = \varphi_k \circ \varphi_j^{-1} : V_{j,k} \to V_{k,j}$. El diagrama (3.4) ilustra la situación.

$$\begin{array}{ccc} & U_j \cap U_k & \\ {\scriptstyle \varphi_j}\swarrow & & \searrow{\scriptstyle \varphi_k} \\ V_{j,k}, V_j & \xrightarrow{\quad\varphi_{k,j}\quad} & V_{k,j}, V_k \end{array} \tag{3.4}$$

Definición **3.9.** *Sea X una superficie de Riemann con un atlas $\mathcal{A} = \{(\varphi_j, U_j)\}_{j\in J}$. Una* ***forma diferencial holomorfa en*** *X es una colección de formas diferenciales locales*

$$(\omega_j)_{j\in J} \in \prod_{j\in J} \Omega^1_{hol}(V_j)$$

que verifica que $\varphi^*_{k,j}(\omega_k|_{V_{k,j}}) = \omega_j|_{V_{j,k}}$.

A esta última condición que debe cumplir $(\omega_j)_{j\in J}$, que está asociada al cambio de carta la llamaremos condición de **compatibilldad**. Denotaremos $\Omega^1_{hol}(X)$ al conjunto de las formas diferenciales holomorfas en X.

Sea X una superficie de Riemann compacta de género g, y consideremos $A_1, ..., A_g$ curvas cerradas longitudinales alrededor de cada asa y $B_1, ..., B_g$ curvas cerradas latitudinales alrededor de cada asa como muestra la figura 3.2.

Denotemos $\Omega^1_{hol}(X)^\wedge$ el espacio dual de $\Omega^1_{hol}(X)$ y sea $\mathcal{B} = \left\{\int_{A_i}, \int_{B_i} : i = 1, ..., g\right\} \subseteq \Omega^1_{hol}(X)^\wedge$. Entonces $\mathcal{B}$ es linealmente independiente en $\Omega^1_{hol}(X)^\wedge$ como $\mathbb{R}$-espacio vectorial y se cumple que

$$\Omega^1_{hol}(X)^\wedge \simeq \mathbb{R}\int_{A_1} \oplus ... \oplus \mathbb{R}\int_{A_g} \oplus \mathbb{R}\int_{B_1} \oplus ... \oplus \mathbb{R}\int_{B_g}.$$

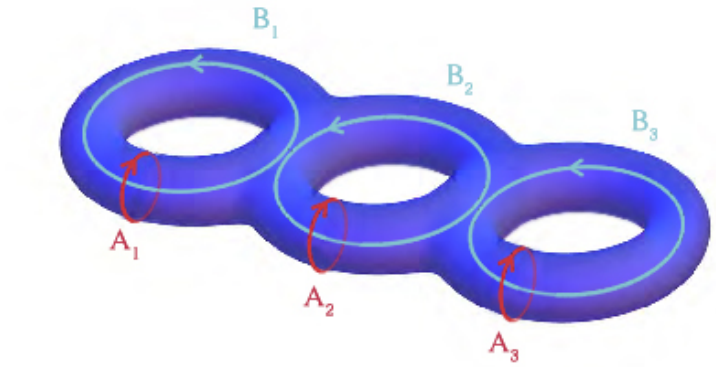


Figura 3.2: Ejemplo de una superficie de Riemann de género 3 en el que se ilustran las curvas longitudinales y latitudinales alrededor de cada asa.

Definición **3.10.** *Definimos el* ***grupo de homología*** *de X al conjunto*

$$H_1(X, \mathbb{Z}) = \mathbb{Z}\int_{A_1} \oplus ... \oplus \mathbb{Z}\int_{A_g} \oplus \mathbb{Z}\int_{B_1} \oplus ... \oplus \mathbb{Z}\int_{B_g}.$$

El conjunto $H_1(X,\mathbb{Z})$ será un retículo en $\Omega^1_{hol}(X)^\wedge$. Pese a que no lo demostraremos cabe mencionar que si α es una curva cerrada en X, entonces existen únicos $m_1, ..., m_g$ y $n_1, ..., n_g \in \mathbb{Z}$ tales que

$$\int_\alpha = \sum_{i=1}^{g} m_i \int_{A_i} + \sum_{i=1}^{g} n_i \int_{B_i}$$

y por tanto, para cualquier curva cerrada α, $\int_\alpha \in H_1(X, \mathbb{Z})$.

Definición **3.11.** *El* ***Jacobiano*** *de X es el conjunto*

$$\mathrm{Jac}(X) = \Omega^1_{hol}(X)^\wedge / H_1(X, \mathbb{Z}).$$

Nos interesarán principalmente $J_1(N) = \mathrm{Jac}(X_1(N))$ y $J_0(N) = \mathrm{Jac}(X_0(N))$.

Sean $x, x_0 \in X$. En principio, $\int_{x_0}^{x}$ no está bien definido puesto que depende de la curva que los una. Sin embargo, si γ, γ' son dos curvas que llevan x_0 a x, tenemos que $\int_{\gamma'} = \int_\gamma + \int_\alpha$ con α una curva cerrada y como $\int_\alpha \in H_1(X, \mathbb{Z})$, $\int_{x_0}^{x}$ queda bien definida a menos de elementos de $H_1(X, \mathbb{Z})$, es decir que $\int_{x_0}^{x} \in \mathrm{Jac}(X)$.

Dado que $H_1(X, \mathbb{Z})$ es un retículo, el Jacobiano será un toro complejo g-dimensional.

Teorema **3.12** (Teorema de Abel)**.** *El mapa*

$$\mathrm{Pic}^0(X) \to \mathrm{Jac}(X) \text{ dado por } \left[\sum_{x \in X} n_x x\right] \mapsto \sum_{x \in X} n_x \int_{x_0}^{x}$$

es un isomorfismo de grupos.

Este isomorfismo permite pasar todos los mapas entre grupos de Picard definidos en la Sección 2.4.2 a Jacobianos, como lo son h^*, h_* y $[\Gamma_1 \alpha \Gamma_2]$ por lo visto en la Sección 2.5.1. En particular, T_p y $\langle n \rangle$ actúan en $J_1(X)$.

3.3. Formas diferenciales en $X(\Gamma)$

Sea Γ un subgrupo de congruencia y $\omega = (\omega_j)_{j \in J} \in \Omega^1_{hol}(X(\Gamma))$. Por lo visto en la Sección 2.1, dado $x \in \mathcal{H}^*$, tenemos una función $\psi_j : T_j \to V_j$ con T_j entorno de x y V_j entorno de 0 que define una carta en el cociente. Escribamos $T'_j = T_j \cap \mathcal{H}$, $V'_j = \psi_j(T'_j)$ y $w'_j = w_j|_{V'_j}$.

Llamemos $\pi : \mathcal{H}^* \to X(\Gamma)$ a la proyección cociente y definamos $\pi^*(\omega)|_{U'_j} = \psi_j^*(\omega'_j)$. Utilizando la compatibilidad de ω y el hecho de que $\mathcal{H}$ es simplemente conexo, se puede ver que $\pi^*(\omega) = f(z)dz$ para una función f holomorfa definida en $\mathcal{H}$.

Como ω es un objeto de $X(\Gamma)$, es Γ-invariante, y por lo tanto, dada $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, $f(z)dz = \gamma^*(f(z)dz) = f(\gamma(z))\gamma'(z)dz$. Un simple cálculo muestra que $\gamma'(z) = (cz + d)^{-2} = j(\gamma, z)^{-2}$ y por tanto $f(z)dz = f[\gamma]_2 dz$, lo que implica que f es una forma débilmente modular de peso 2 para Γ.

Observemos que ocurre con las cúspides. Por lo visto en la Sección 2.1, para una cúspide $s \in \mathbb{Q} \cup \{\infty\}$, la carta ψ_j es $\psi_j = \rho \circ \delta$ donde $\rho(\tau) = e^{\frac{2\pi i \tau}{h}}$ y $\delta(s) = \infty$ con $\delta \in \mathrm{SL}_2(\mathbb{Z})$.

Consideremos el dibujo de la figura 3.3 que muestra la acción de los mapas δ y ρ. Definimos como z a la variable en el entorno U de s, como τ a la variable en el entorno W de ∞ y q a la variable en el entorno V de 0. Se cumple que $\delta(z) = \tau$ y que $\rho(\tau) = q$.

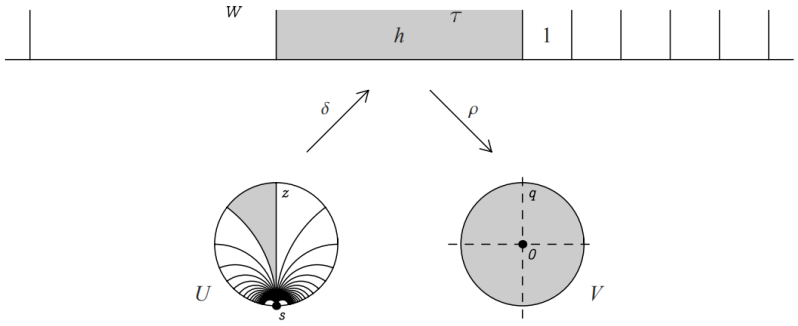


Figura 3.3: Acción de los mapas δ y ρ en los entornos de s, ∞ y 0 respectivamente (Imagen extraída de [DS00]).

Por la definición de forma diferencial holomorfa en $X(\Gamma)$, existe una función holomorfa $g : V \to \mathbb{C}$ tal que $\omega|_V = g(q)dq$. Calculando el pullback, nos queda que $(\rho \circ \delta)^*(\omega|_V) = (\rho \circ \delta)^*(g(q)dq) = g(q)(\rho \circ \delta)'(z)dz$.

Al igual que como mostrábamos antes, $\delta'(z) = j(\delta, z)^{-2}$ y calculando también ρ' y utilizando la regla de la cadena obtenemos:

$$(\rho \circ \delta)^*(\omega|_V) = g(q)q\frac{2\pi i}{h}j(\delta, z)^{-2}.$$

Como $\rho \circ \delta$ es carta de $X(\Gamma)$, $(\rho \circ \delta)^*(\omega|_V) = f(z)dz$ en $U \setminus \{s\}$ y por lo tanto $f(z) = g(q)q\frac{2\pi i}{h}j(\delta, z)^{-2}$ en $U \setminus \{s\}$.

Sea $\tilde{f} = f[\alpha]_2 \Rightarrow \tilde{f}[\delta]_2 = f \Rightarrow \tilde{f}(\delta(z)) = \tilde{f}(\tau) = g(q)q\frac{2\pi i}{h}$. Dado que g está definida en V y es holomorfa, $\tilde{f}$ tiene una extensión holomorfa a ∞ y su valor en ∞ se obtiene de sustituir q por 0 según la Definición 1.4, lo que prueba que $\tilde{f}(\infty) = 0$. Realizando esto con todos los elementos de $\mathbb{Q} \cup \{\infty\}$, obtenemos que $f \in \mathcal{S}_2(\Gamma)$.

El camino inverso toma ideas de las presentadas anteriormente. Si $f \in \mathcal{S}_2(\Gamma)$ y tomamos s una cúspide con δ y α como antes, entonces $\tilde{f}(\tau) = f[\alpha]_2(\tau) = g(q)q\frac{2\pi i}{h}$ con g holomorfa en un entorno de 0. Luego, se puede encontrar una forma diferencial $\omega_f \in \Omega^1_{hol}(X(\Gamma))$ tal que $\pi^*(\omega_f) = f(z)dz$, lo que da lugar al siguiente resultado:

Teorema **3.13.** *Sea Γ un subgrupo de congruencia, entonces $\psi : \Omega^1_{hol}(X(\Gamma)) \to \mathcal{S}_2(\Gamma)$ dada por $\psi(\omega_f) = f$ es un isomorfismo de $\mathbb{C}$-espacios vectoriales en donde f y ω_f cumplen que $\pi^*(\omega_f) = f(z)dz$.*

3.4. Variedades Abelianas

El Teorema 3.13 nos permite ver que $\Omega^1_{hol}(X(\Gamma))^\wedge \simeq \mathcal{S}_2(\Gamma)^\wedge$ es un isomorfismo de $\mathbb{C}$-espacios vectoriales, por lo que existe un subgrupo de $\mathcal{S}_2(\Gamma)^\wedge$ que se identifica con $H_1(X(\Gamma), \mathbb{Z})$.

Los operadores de Hecke actúan sobre $\mathcal{S}_2(\Gamma)^\wedge$ de la siguiente forma:

$$T : \mathcal{S}_2(\Gamma)^\wedge \to \mathcal{S}_2(\Gamma)^\wedge \ / \ \varphi \mapsto \varphi \circ T.$$

De hecho, como T desciende a $J_1(N)$, la acción de T queda definida en $H_1(X(\Gamma), \mathbb{Z}) \simeq \mathbb{Z}^{2g}$.

Teorema **3.14.** *Sea $f \in \mathcal{S}_2(\Gamma_1(N))^{new}$ una forma propia normalizada para todos los operadores de Hecke del conjunto $T^0(N)$. Entonces los valores propios del conjunto $\{a_n(f) : n \in \mathbb{Z}^+\}$ son enteros algebraicos.*

Demostración. Sea T un operador de Hecke de $T^0(N)$. Por lo mencionado anteriormente, la acción de T queda definida en $H_1(X_1(N), \mathbb{Z}) \simeq \mathbb{Z}^{2g}$, y por tanto su polinomio característico $\widehat{\chi_T}$ es mónico y tiene coeficientes enteros. Por el Teorema de Cayley-Hamilton, $\widehat{\chi_T}(T) = 0$ en $\mathcal{S}_2(\Gamma)^\wedge$ y por tanto $\widehat{\chi_T}(T) = 0$ en $\mathcal{S}_2(\Gamma)$. Si χ_T es el polinomio característico de T en $\mathcal{S}_2(\Gamma) \Rightarrow \chi_T \mid \widehat{\chi_T}$ y como $\chi_T(\lambda) = 0$ para cualquier valor propio de $T \Rightarrow \widehat{\chi_T}(\lambda) = 0$ para todos los valores propios de T. Si tomamos $T = T_n$, por lo visto en el Teorema 1.25, obtenemos que $\widehat{\chi_{T_n}}(a_n(f)) = 0$ y por lo tanto los $a_n(f)$ son enteros algebraicos. □

Definición **3.15.** *Definimos el* ***álgebra de Hecke*** *como*

$$\mathbb{T}_\mathbb{Z} = \mathbb{Z}\left[\left\{T_n, \langle n\rangle : n \in \mathbb{Z}^+\right\}\right] \ \text{ y } \mathbb{T}_\mathbb{C} = \mathbb{C}\left[\left\{T_n, \langle n\rangle : n \in \mathbb{Z}^+\right\}\right].$$

Es decir que $\mathbb{T}_\mathbb{Z}$ es el $\mathbb{Z}$-módulo generado por los operadores de Hecke y $\mathbb{T}_\mathbb{C}$ es el $\mathbb{C}$-espacio vectorial generado por los operadores de Hecke. Dado que $\mathbb{T}_\mathbb{Z}$ es un submódulo de $\mathrm{End}_\mathbb{Z}(H_1(X_1(N), \mathbb{Z}))$ donde $H_1(X_1(N), \mathbb{Z})$ es finitamente generado, entonces $\mathbb{T}_\mathbb{Z}$ es finitamente generado por ser $\mathbb{Z}$ un DIP.

Sea $f(z) = \sum_{n=1}^\infty a_n(f) q^n$ una forma propia normalizada de todos los operadores de Hecke de $\mathbb{T}_\mathbb{Z}$. Definimos el siguiente morfismo:

$$\lambda_f : \mathbb{T}_\mathbb{Z} \to \mathbb{C} \ / \ Tf = \lambda_f(T) f.$$

Dado que $\mathbb{T}_\mathbb{Z}$ es finitamente generado, su imagen por λ_f también lo es, y usando además el Primer Teorema de Isomorfismo obtenemos que $\mathbb{T}_\mathbb{Z}/\ker(\lambda_f) \simeq \mathbb{Z}[\{a_n(f) : n \in \mathbb{Z}^+\}]$ es finitamente generado como $\mathbb{Z}$-módulo. Esto último da otra prueba del Teorema 3.14.

Definición **3.16.** *Sea $f \in \mathcal{S}_2(\Gamma_1(M_f))$ una forma propia normalizada, nueva para el nivel M_f, tal que $f(z) = \sum_{n=1}^{\infty} a_n(f)q^n$. Definimos el* ***cuerpo de coeficientes de*** *f como el cuerpo $\mathbb{K}_f = \mathbb{Q}(\{a_n(f)\})$.*

Como $\mathbb{Z}[\{a_n(f) : n \in \mathbb{Z}^+\}]$ es finitamente generado, $[\mathbb{K}_f : \mathbb{Q}] < \infty$.

Dado que $\mathbb{T}_{\mathbb{Z}}$ actúa sobre $J_1(M_f)$, tiene sentido el subgrupo $\ker(\lambda_f)J_1(M_f)$ y por ende podemos definir:

Definición **3.17.** *Dada $f \in \mathcal{S}_2(\Gamma_1(M_f))$. Definimos la* ***variedad abeliana asociada a*** *f como el cociente*

$$A_f = J_1(M_f)/\ker(\lambda_f)J_1(M_f).$$

Se cumple que A_f es un toro complejo de dimensión $[\mathbb{K}_f : \mathbb{Q}]$. La prueba puede encontrarse en la proposición 6.6.4 de [DS00].

Observemos que $\mathbb{T}_{\mathbb{Z}}/\ker(\lambda_f)$ actúa sobre A_f. En efecto si tenemos $T + I$ con $I \in \ker(\lambda_f)$ y $j \in J_1(M_f) \Rightarrow (T + I)(j) = T(j) + I(j)$ y dado que $I(j) \in \ker(\lambda_f)J_1(M_f)$, $[T]$ actúa sobre A_f, y por lo tanto también lo hace su imagen isomorfa, que es $\mathbb{Z}[\{a_n(f) : n \in \mathbb{Z}^+\}]$. Dado que $\lambda_f(T_p) = a_p(f)$ (ver Teorema 1.25), el siguiente diagrama conmuta:

$$\begin{array}{ccc} J_1(M_f) & \xrightarrow{T_p} & J_1(M_f) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ A_f & \xrightarrow{a_p(f)} & A_f \end{array} \tag{3.5}$$

Para entender la acción del mapa $a_p(f)$ nos será útil el siguiente resultado:

Teorema **3.18.** *Sea $f \in \mathcal{S}_2(\Gamma_0(M_f))$ una forma propia nueva normalizada de todos los operadores de Hecke tal que $f(z) = \sum_{n=0}^{\infty} a_n(f)q^n$, $\sigma : \mathbb{K}_f \hookrightarrow \mathbb{C}$ un encaje y $f^\sigma(z) = \sum_{n=0}^{\infty} a_n^\sigma(f)q^n$. Entonces f^σ es también una forma propia nueva normalizada de todos los operadores de Hecke.*

Entonces, sea $\varphi \in \mathcal{S}_2(\Gamma_1(M_f))^\wedge$. Como observamos al comienzo de la sección, podemos identificar a $J_1(M_f)$ con un cociente de $\mathcal{S}_2(\Gamma_1(M_f))^\wedge$ y aunque no entraremos en detalles, a A_f lo podemos identificar con un cociente del dual del subespacio vectorial generado por $\{f^\sigma : \sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})\}$. Para simplificar la notación llamemos H a $H_1(X_1(N), \mathbb{Z})$ y A al mapa $a_p(f)$. Utilizando el diagrama (3.5), tenemos que:

$$A([\varphi + H]) = [\varphi \circ T_p + H].$$

Sea f una forma propia normalizada de todos los operadores de Hecke y sea $\sigma : \mathbb{K}_f \hookrightarrow \mathbb{C}$ un encaje, entonces $T_p f^\sigma = a_p(f^\sigma)f^\sigma = (a_p(f))^\sigma f^\sigma$ lo que lleva a que:

$$A([\varphi + H])(f^\sigma) = (a_p(f))^\sigma [\varphi + H](f^\sigma). \tag{3.6}$$

Vemos en particular que cuando $a_p(f) \in \mathbb{Z}$, $(a_p(f))^\sigma = a_p(f)$ y la fila de abajo del diagrama (3.5) es multiplicar por $a_p(f)$. Además, si $\delta_1, \delta_2 \in \mathbb{C}$ y consideramos los mapas que ellos generan según la ecuación (3.6), entonces es fácil ver que $\delta_1 \circ \delta_2 = \delta_1\delta_2$.

Buscamos ver como se puede descomponer el Jacobiano en variedades abelianas. Para ello, observemos primero que la definición 2.7 puede extenderse a toros de dimensión superior a 1 y de hecho, tenemos una generalización para el Teorema 2.8:

Teorema **3.19.** *Si* $\varphi : \mathbb{C}^g/\Lambda_g \to \mathbb{C}^h/\Lambda_h$ *es una isogenia entre toros complejos* $\Rightarrow g = h$, $\varphi(z + \Lambda_g) = Mz + \Lambda_h$ *con* $M \in GL_g(\mathbb{C})$ *y* $M\Lambda_g \subseteq \Lambda_h$.

La prueba de 3.19 es idéntica a la presentada en el Teorema 2.8.

Por otro lado, definimos una relación de equivalencia entre las formas propias nuevas normalizadas:

$$\overline{f} \sim f \iff \overline{f} = f^\sigma \text{ para algún } \sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}).$$

Teorema **3.20.** *Existe una isogenia*

$$J_1(N) \longrightarrow \bigoplus_{f,n} A_f$$

donde f *se mueve en los distintos representantes de las clases de equivalencia anterior en* $\mathcal{S}_2(\Gamma_1(M_f))$ *con* M_f *divisor de* N *y* n *se mueve en los distintos divisores de* N/M_f.

El Teorema 3.20 junto con el diagrama (3.5), nos permite crear el siguiente diagrama:

$$\begin{array}{ccc} J_1(N) & \xrightarrow{T_p} & J_1(N) \\ \downarrow & & \downarrow \\ \bigoplus_{f,n} A_f & \xrightarrow{\prod_{f,n} a_p(f)} & \bigoplus_{f,n} A_f. \end{array} \tag{3.7}$$

Utilizando la existencia de una isogenia dual, podemos pasar el diagrama (3.7) a:

$$\begin{array}{ccc} \bigoplus_{f,n} A_f & \xrightarrow{\prod_{f,n} a_p(f)} & \bigoplus_{f,n} A_f \\ \downarrow & & \downarrow \\ J_1(N) & \xrightarrow{T_p} & J_1(N). \end{array} \tag{3.8}$$

De manera análoga podemos definir $A'_f = J_0(M_f)/\ker(\lambda_f)J_0(M_f)$ y todos los teoremas y resultados dados para A_f se cumplen en A'_f.

El siguiente resultado será clave en la Sección 4.4:

Teorema **3.21.** *Sea $f \in \mathcal{S}_2(\Gamma_0(M_f))$ una forma nueva tal que $a_n(f) \in \mathbb{Q}\ \forall n \in \mathbb{N} \Rightarrow$ A'_f es una curva elíptica sobre $\mathbb{C}$ y $\exists \alpha : X_0(N) \to A'_f$ un morfismo sobreyectivo sobre $\mathbb{C}$ de curvas algebraicas.*

Demostración. Dado que $a_n(f) \in \mathbb{Q}$ entonces $\mathbb{K}_f = \mathbb{Q}$ y por tanto, $\dim(A'_f) = 1$. Como A'_f tiene dimensión 1 y es un toro complejo, por el Teorema 3.5, A_f es una curva elíptica sobre $\mathbb{C}$.

A partir de lo dado a lo largo del documento, tenemos morfismos que nos dan el siguiente camino que nos definen el morfismo α que buscamos:

$$X_0(N) \overset{i}{\hookrightarrow} \mathrm{Div}^0(X_0(N)) \overset{\pi}{\mapsto} \mathrm{Pic}^0(X_0(N)) \mapsto J_0(N) \mapsto A'_f.$$

Dado que $\dim(A'_f) = 1$ y α es no trivial, entonces es sobreyectivo. □

Pese a que la demostración del Teorema 3.21 se hizo sobre $\mathbb{C}$, se puede probar que $X_0(N)$, A_f y A'_f están definidas sobre $\mathbb{Q}$ y que hay un morfismo α como en el Teorema 3.21 sobre $\mathbb{Q}$. Los Operadores de Hecke pueden también definirse de igual manera a lo hecho hasta ahora pero sobre $\mathbb{Q}$. Estas ideas son presentadas en el Capítulo 7 de [DS00].

Esta página ha sido intencionalmente dejada en blanco.

Capítulo 4

Relación de Eichler-Shimura

4.1. Reducción de curvas elípticas sobre $\overline{\mathbb{Q}}$

Sea $p \in \mathbb{P}$ y sea $\overline{\mathbb{Z}}$ el anillo de enteros algebraicos (el conjunto de los números complejos que satisfacen un polinomio mónico con coeficientes enteros). Consideremos en $\overline{\mathbb{Z}}$ el ideal $p\overline{\mathbb{Z}}$. Por Zorn, podemos encontrar un ideal maximal $\mathfrak{p}$ tal que $p\overline{\mathbb{Z}} \subseteq \mathfrak{p}$. Fijemos $\mathfrak{p}$ a partir de ahora y consideremos la localización

$$\overline{\mathbb{Z}}_{(\mathfrak{p})} = \left\{ \frac{x}{y} : x, y \in \overline{\mathbb{Z}}, y \notin \mathfrak{p} \right\}.$$

El conjunto $\overline{\mathbb{Z}}_{(\mathfrak{p})}$ es un subanillo de $\overline{\mathbb{Q}}$ que contiene a $\overline{\mathbb{Z}}$ y su único ideal maximal es $\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$. Tenemos por tanto que $\overline{\mathbb{Z}}_{(\mathfrak{p})}/\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$ es un cuerpo.

Teorema **4.1.** *1. El mapa $\phi : \overline{\mathbb{Z}}/\mathfrak{p} \to \overline{\mathbb{Z}}_{(\mathfrak{p})}/\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$ dado por $\alpha + \mathfrak{p} \mapsto \alpha + \mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$, es un isomorfismo de cuerpos.*

2. $\overline{\mathbb{Z}}/\mathfrak{p}$ es una clausura algebraica de $\mathbb{F}_p$.

A partir del Teorema 4.1, identificamos $\overline{\mathbb{F}}_p = \overline{\mathbb{Z}}_{(\mathfrak{p})}/\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$ y entonces el mapa $\sim: \overline{\mathbb{Z}}_{(\mathfrak{p})} \to \overline{\mathbb{F}}_p$ dado por $\widetilde{\alpha} = \alpha + \mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$ es un mapa sobreyectivo con $\ker(\sim) = \mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$.

Notemos también que $\sim$ induce un morfismo de anillos entre $\overline{\mathbb{Z}}_{(\mathfrak{p})}[x_1, ..., x_n]$ y $\overline{\mathbb{F}}_p[x_1, ..., x_n]$ que se obtiene de transformar los coeficientes de los polinomios de $\overline{\mathbb{Z}}_{(\mathfrak{p})}[x_1, ..., x_n]$ por $\sim$. Si $\varphi \in \overline{\mathbb{Z}}_{(\mathfrak{p})}[x_1, ..., x_n]$, $\widetilde{\varphi}$ será su transformado por $\sim$.

Definición **4.2.** *Sea C una curva algebraica sobre $\overline{\mathbb{Q}}$ definida por los polinomios $\varphi_1, ..., \varphi_m \in \mathbb{Z}_{(p)}[x_1, ..., x_n]$. Diremos que C tiene* ***buena reducción módulo p*** *si $\widetilde{\varphi_1}, ..., \widetilde{\varphi_m}$ define una curva algebraica sobre $\overline{\mathbb{F}}_p$. En ese caso llamaremos $\widetilde{C}$ a la* ***reducción de C módulo p****.*

Buscamos extender la función $\sim$ a $\sim: \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{P}^n(\overline{\mathbb{F}}_p)$. Para ello precisaremos el siguiente resultado:

Teorema **4.3.** *Sea $\alpha \in \overline{\mathbb{Q}} \setminus \{0\} \Rightarrow \alpha$ o $1/\alpha \in \overline{\mathbb{Z}}_{(\mathfrak{p})}$*

De esta manera, si $P = [x_0 : ... : x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$, tenemos que algunas de sus coordenadas es no nula; supongamos que $x_0 \neq 0$, por lo tanto $P = [1 : \frac{x_1}{x_0} : ... : \frac{x_n}{x_0}]$ y su primer coordenada está en $\overline{\mathbb{Z}}_{(\mathfrak{p})}$. Ahora, si $\frac{x_1}{x_0} \in \overline{\mathbb{Z}}_{(\mathfrak{p})}$ pasamos a la siguiente coordenada, si no, por el Teorema 4.3, $\frac{x_0}{x_1} \in \overline{\mathbb{Z}}_{(\mathfrak{p})}$ y entonces al multiplicar por $\frac{x_0}{x_1}$, no alteramos la primer coordenada porque estamos multiplicando dos elementos del anillo y la segunda coordenada pasa a ser 1. De esta manera, haciendo este proceso en todas las coordenadas, se obtiene una representación $P = [y_0 : ... : y_n]$ donde $y_i \in \overline{\mathbb{Z}}_{(\mathfrak{p})} \forall i = 0, ..., n$ y alguno de los $y_i = 1$. Luego, se puede aplicar la función $\sim$, obteniendo un punto reducido $\widetilde{P} = [\widetilde{y_0}, ..., \widetilde{y_n}]$ que efectivamente se encuentra en el proyectivo, dado que alguna de sus coordenadas es no nula. Llamaremos $\widetilde{P}$ a la reducción de P.

Tenemos entonces dos maneras de aplicar $\sim$: a los coeficientes de la ecuación que la determina, o a los puntos de la curva proyectiva. Por lo hecho anteriormente, aplicársela a los puntos de la curva proyectiva no tiene inconveniente. Sin embargo, consideremos el caso de la siguiente curva elíptica con coeficientes en $\mathbb{Q}$. Aclarar que si los coeficientes son de $\mathbb{Z}_{(p)} = \left\{ \frac{x}{y} : x, y \in \mathbb{Z}, y \notin p\mathbb{Z} \right\} \subseteq \mathbb{Q}$, la función $\sim$ se puede definir de $\mathbb{Z}_{(p)}$ a $\mathbb{F}_p$ y lleva $\frac{x}{y} \mapsto xy^{-1} \pmod p$.

$$E : y^2 = x^3 + \frac{1}{p^2}x + \frac{1}{p}.$$

En la forma que se presenta, los coeficientes de E no se pueden reducir puesto que hay denominadores cuyo inverso no está bien definido en $\mathbb{F}_p$. Sin embargo, podemos realizar algún cambio de variable admisible que quite estos denominadores, como por ejemplo, tomar $u = p^{-1}$, obteniendo:

$$E' : y'^2 = x'^3 + p^2x' + p^5.$$

Ahora los coeficientes se pueden reducir, y su reducción es:

$$\widetilde{E} : y'^2 = x'^3.$$

Ocurre que el discriminante de $\widetilde{E}$ es nulo y por tanto $\widetilde{E}$ no es una curva elíptica.

Si bien esto parece tener que ver con la curva elíptica anterior, nuestra definición de curva reducida va a tener un problema si permitimos cualquier cambio de variable admisible. En efecto, si $E : y^2 = x^3 + ax + b$ es una curva elíptica cualquiera con $a, b \in \mathbb{Q}$ tal que $r^l a, r^l b \in \mathbb{Z}$ para algún $l \in \mathbb{N}$, entonces el cambio de variable admisible $u = r^{-l}$ deja a la curva elíptica E' como:

$$E' : y'^2 = x'^3 + r^{4l}ax' + r^{6l}b$$

que al reducirla para un primo $p \mid r$ nos queda:

$$\widetilde{E} : y'^2 = x'^3$$

y será singular como la anterior.

Se hace necesario afinar que cambio de variable admisible tomaremos para representar la curva elíptica que queremos reducir.

Definición **4.4.** *Dado $q \in \mathbb{Q}$ y $p \in \mathbb{P}$, podemos expresar q como $q = p^e m/n$ con $m, n \in \mathbb{Z}$ de forma que $p \nmid m$ y que $p \nmid n$. Definimos la* ***valuación*** *de q con respecto a p como:*

$$\nu_p(q) = e.$$

Definición **4.5.** *Sea E una curva elíptica con coeficientes en $\mathbb{Q}$ y $\mathcal{E}$ el conjunto de las curvas elípticas con coeficientes en $\mathbb{Z}$ y que se obtienen de E a partir de un cambio de variable admisible. Definimos la* ***valuación*** *de E como:*

$$\nu_p(E) = \min\left\{\nu_p(\Delta(E')) : E' \in \mathcal{E}\right\}.$$

Definición **4.6.** *Dada E una curva elíptica con coeficientes en $\mathbb{Q}$, definimos el* ***discriminante mínimo global*** *de E como:*

$$\Delta_{mn}(E) = \prod_{p \in \mathbb{P}} p^{\nu_p(E)}.$$

Este producto es finito puesto que $\nu_p(E) = 0$ para todo $p \nmid \Delta(E)$. Se puede demostrar, que existe un cambio de variable admisible que da una curva elíptica $E' \in \mathcal{E}$ tal que $\Delta(E') = \Delta_{mn}(E)$. Llamaremos a E' la **ecuación de Weierstrass minimal global** de E, puesto que esta ecuación permite una reducción no ambigua para todos los primos simultáneamente.

Cabe mencionar, que las definiciones 4.4, 4.5 y 4.6 pueden extenderse a $\overline{\mathbb{Q}}$, cambiando $\mathbb{Z}$ por $\overline{\mathbb{Z}}$ y $p\mathbb{Z}$ por $\mathfrak{p}$, con la diferencia de que no necesariamente encontraremos una ecuación de Weierstrass minimal global, sino que tendremos una E' para cada $\mathfrak{p}$.

A partir de ahora, trabajaremos con la versión E de la curva elíptica que tenga discriminante mínimo.

Definición **4.7.** *Diremos que $\widetilde{E}$ tiene* ***buena reducción en*** *$\mathfrak{p} \Leftrightarrow \widetilde{E}$ es una curva elíptica sobre $\overline{\mathbb{F}}_p$.*

Por como fue definido Δ_{min} y $\nu_p(E)$, es claro que E va a tener buena reducción módulo $p \Leftrightarrow p \nmid \Delta_{min}$.

Sea E una curva elíptica y $\tilde{E}$ su reducción módulo p. La reducción será:

1. *Buena*: Si $\widetilde{E}$ es una curva elíptica.

   a) *Ordinaria*: Si $\widetilde{E}[p] = \mathbb{Z}/p\mathbb{Z}$.

   b) *Supersingular*: Si $\widetilde{E}[p] = \{0\}$.

2. *Mala*: Si $\widetilde{E}$ no es una curva elíptica.

   a) *Semiestable o multiplicativa*: Si $\widetilde{E}$ tiene un nodo.

   b) *Inestable o aditiva*: Si $\widetilde{E}$ tiene una cúspide.

El caso de mala reducción semiestable fue el caso demostrado de la Conjetura de Taniyama-Shimura que dio paso al Último Teorema de Fermat (ver Capítulo 0). El hecho de que sólo tengamos esos dos casos para curvas elípticas con buena reducción fue enunciado en el Teorema 3.3.(4).

Definición **4.8.** *Sea E una curva elíptica sobre $\mathbb{Q}$. Definimos el* ***conductor*** *de la curva elíptica $N_E = \prod_{p\in\mathbb{P}} p^{f_p}$ donde:*

$$f_p = \begin{cases} 0 & \text{Si } E \text{ tiene buena reducción módulo } p \\ 1 & \text{Si } E \text{ tiene reducción semiestable módulo } p \\ 2 & \text{Si } E \text{ tiene reducción inestable módulo } p \text{ y } p \notin \{2,3\} \\ 2+\delta_p & \text{Si } E \text{ tiene reducción inestable módulo } p \text{ y } p \in \{2,3\} \end{cases}$$

Sin entrar demasiado en detalle en δ_p (porque trabajaremos en curvas con buena reducción) diremos que $\delta_2 \leq 6$ y que $\delta_3 \leq 3$.

Es claro que $p \mid \Delta_{min}(E) \Leftrightarrow p \mid N_E$.

El siguiente teorema nos será útil en la Sección 4.3:

Teorema **4.9.** *Sea E una curva elíptica sobre $\overline{\mathbb{Q}}$ con buena reducción en $\mathfrak{p}$ y $N \in \mathbb{N}$. Entonces:*

1. *El mapa $E[N] \to \widetilde{E}[N]$ es sobreyectivo.*

2. *Si C es un subgrupo cíclico de orden p en E. Entonces E/C tiene buena reducción a $\mathfrak{p}$. Más aún, E/C preserva el tipo de reducción que tenga E.*

Por último, si $Q \in E(\overline{k})$, $\widetilde{Q}$ es su reducción y $\widetilde{E}$ es la reducción de la curva elíptica, entonces $\widetilde{Q} \in \widetilde{E}(\overline{k})$. Sin embargo, no todos los puntos de $\widetilde{E}(\overline{k})$ son puntos reducidos de E.

4.2. Mapa de Frobenius y reducción de isogenias

Dado $p \in \mathbb{P}$, definimos el mapa de Frobenius como $\sigma_p : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ dado por $x \mapsto x^p$.

La función $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, y más aún, si definimos $\sigma_{p^e} = \sigma_p^e$, la función σ_{p^e} tiene como puntos fijos a los puntos de $\mathbb{F}_{p^e}$. Si bien σ_p es una función biyectiva, su inversa no es un polinomio, por lo que no es un isomorfismo.

El mapa de Frobenius se extiende a $\mathbb{P}^n(\overline{\mathbb{F}}_p)$ de forma biyectiva, dado por:

$$\sigma_p([x_0 : ... : x_n]) = [x_0^p : ... : x_n^p] \tag{4.1}$$

lo que nos permite considerar la acción de σ_p en curvas proyectivas sobre un cuerpo de característica p y en puntos de curvas algebraicas proyectivas.

Sea $\varphi \in \overline{\mathbb{F}}_p[x_0, ..., x_n]$ un polinomio homogéneo, es decir que todo sus términos tienen el mismo grado, dado por $\varphi(x) = \sum_e a_e x^e$ (x^e es una forma corta de escribir $x_0^{e_0}...x_n^{e_n}$) y consideremos $\varphi^{\sigma_p}(x) = \sum_e a_e^{\sigma_p} x^e$. Tenemos entonces que:

$$\varphi^{\sigma_p}(x^{\sigma_p}) = \sum_e a_e^{\sigma_p}(x^{\sigma_p})^e = \sum_e (a_e x^e)^{\sigma_p} = \left(\sum_e a_e x^e\right)^{\sigma_p} = (\varphi(x))^{\sigma_p}. \tag{4.2}$$

Definición **4.10.** *Sea C una curva algebraica proyectiva en $\overline{\mathbb{F}}_p$ determinada por los polinomios $\varphi_1, ..., \varphi_m \in \overline{\mathbb{F}}_p[x_1, ..., x_n]$. Definimos C^{σ_p} como la curva proyectiva en $\overline{\mathbb{F}}_p$ determinada por los polinomios $\varphi_1^{\sigma_p}, ..., \varphi_m^{\sigma_p}$.*

Definición **4.11.** *Sea C una curva algebraica proyectiva en $\overline{\mathbb{F}}_p$ y Q un punto de C. Definimos $Q^{\sigma_p} = \sigma_p(Q)$ dado por la ecuación* (4.1).

Por lo observado en la ecuación (4.2), si Q es un punto de una curva algebraica proyectiva C, entonces Q^{σ_p} es un punto de C^{σ_p}.

Buscaremos también pasar el mapa de Frobenius a divisores a través de las definiciones 2.21 y 2.22 para obtener σ_p^* y $\sigma_{p,*}$. Sea C una curva algebraica proyectiva sobre $\mathbb{F}_p$ y P un punto de C sobre $\overline{\mathbb{F}}_p$. Es claro que $\sigma_{p,*}(P) = \sigma_p(P)$, y para el pullback, dado que σ_p es biyectiva y el grado de ramificación es p, tenemos que $\sigma_p^*(\sum_{P \in C} n_P P) = p \sum_{P \in C} n_P \sigma_p^{-1}(P)$.

Teorema **4.12.** *Sea $h : C \to C'$ un mapa sobre $\mathbb{F}_p$ de curvas proyectivas. Denotamos $\sigma_{p,C}$ al mapa de Frobenius sobre C y $\sigma_{p,C'}$ al mapa de Frobenius sobre C'. Entonces:*

1. $h \circ \sigma_{p,C} = \sigma_{p,C'} \circ h$.
2. $h \circ \sigma_{p,C}^{-1} = \sigma_{p,C'}^{-1} \circ h$.
3. $h_* \circ (\sigma_{p,C})_* = (\sigma_{p,C'})_* \circ h_*$.

4. $h_* \circ \sigma^*_{p,C} = \sigma^*_{p,C'} \circ h_*$.

Demostración. 1. $h : C \to C'$ es un mapa sobre $\mathbb{F}_p$ de curvas proyectivas, entonces, podemos homogeneizar h para obtener un polinomio con coeficientes en $\mathbb{F}_p$ y como $\sigma_p \in Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p) \Rightarrow h^{\sigma_p} = h$. Luego, a partir de la ecuación (4.2), obtenemos:

$$h \circ \sigma_{p,C} = \sigma_{p,C'} \circ h.$$

2 $h \circ \sigma^{-1}_{p,C} = \sigma^{-1}_{p,C'} \circ \sigma_{p,C'} \circ h \circ \sigma^{-1}_{p,C} = \sigma^{-1}_{p,C'} \circ h \circ \sigma_{p,C} \circ \sigma^{-1}_{p,C} = \sigma^{-1}_{p,C'} \circ h$.

3. Es inmediato de la propiedad para la composición de los pushforwards.

4. Sea $P \in C(\overline{\mathbb{F}}_p) \Rightarrow (h_* \circ \sigma^*_{p,C})(P) = ph_*(\sigma^{-1}_{p,C}(P)) = p(h \circ \sigma^{-1}_{p,C})(P) =$
$= p(\sigma^{-1}_{p,C'} \circ h)(P)$.
Por otro lado, $(\sigma^*_{p,C'} \circ h_*)(P) = \sigma^*_{p,C'}(h(P)) = p(\sigma^{-1}_{p,C'} \circ h)(P)$.

Luego, alcanza con observar que P es genérico y los puntos de C sobre $\overline{\mathbb{F}}_p$) generan el grupo de divisores. □

Definición **4.13.** *Sea k un cuerpo y K una extensión de k. K/k es* ***separable*** *si para $u \in K$, su polinomo minimal en $k[x]$ es separable en $\overline{k}$. En caso contrario, diremos que es* ***inseparable****. Si para todo $u \in K$, u es la única raíz de su polinomio minimal, K/k será una extensión* ***puramente inseparable****.*

Por ejemplo, las raíces que se adjunten del polinomio $x^p - s$ harán una extensión puramente inseparable, puesto que si $s = t^p$, se tiene que $x^p - s = (x - t)^p$. La extensión adjunta solo una raíz, pero que se repite p veces.

Para hacer las siguientes definiciones, tendremos que mencionar algunos conceptos de Geometría Algebraica. Si C es una curva algebraica irreducible sobre $\overline{k}$ entonces $C = \left\{ P \in \overline{k}^n : \varphi(P) = 0, \forall \varphi \in I \right\}$ con I un ideal primo de $\overline{k}[x_1, ..., x_n]$.
Llamaremos $\overline{k}[C] = \overline{k}[x_1, ..., x_n]/I$. $\overline{k}[C]$ es un dominio y llamaremos $\overline{k}(C)$ a su cuerpo de fracciones.

Sea $h : C \to C'$ un morfismo sobreyectivo entre curvas algebraicas sobre $\overline{\mathbb{F}}_p$. Llamemos $k_1 = \overline{\mathbb{F}}_p(C')$ y $K_1 = \overline{\mathbb{F}}_p(C)$, entonces $h^* : k_1 \to K_1$ dada por $h^*\left(\frac{f}{g}\right) = \frac{f \circ h}{g \circ h}$ es un mapa inyectivo, por ser un morfismo de cuerpos.

Dado que la composición de dos extensiones de cuerpos separables es separable, podemos definir k_{sep} como la extensión separable maximal de $h^*(k_1)$ dentro de K_1. Por ser maximal, la extension K_1/k_{sep} es puramente inseparable. Aunque no entraremos en detalles, asociado a k_{sep} tenemos una curva algebraica C_{sep} de manera de tener el siguiente diagrama:

$$C \xrightarrow{h_{ins}} C_{sep} \xrightarrow{h_{sep}} C',$$

y por lo tanto, h se descompone en dos morfismos de curvas algebraicas: uno separable y otro puramente inseparable. Como h_{ins} es puramente inseparable, entonces $h_{ins} = \sigma_p^e$ siendo $p^e = [K_1 : k_{sep}]$. En conclusión, $h = h_{sep} \circ \sigma_p^e$ donde e es el grado de inseparabilidad de la extensión (si $e = 0$ será separable, $e > 0$ inseparable y $h_{sep} = 1$ puramente inseparable).

Definimos $\deg_{sep}(h) = \deg(h_{sep})$ y $\deg_{ins}(h) = \deg(\sigma_p^e) = p^e$.

Teorema **4.14.** *Sean h, h' morfismos sobreyectivos entre curvas algebraicas, entonces:*

1. $\deg(h) = \deg_{sep}(h) \deg_{ins}(h)$.
2. $\deg_{sep}(h' \circ h) = \deg_{sep}(h') \deg_{sep}(h)$.
3. $\deg_{ins}(h' \circ h) = \deg_{ins}(h') \deg_{ins}(h)$.
4. *Si φ es un morfismo sobreyectivo de curvas elípticas $\Rightarrow$ $deg_{sep}(\varphi) = |\ker(\varphi)|$.*

Definición **4.15.** *Sea E una curva elíptica sobre $\mathbb{Q}$, $p \in \mathbb{P}$, $e \geq 1$ y $\widetilde{E}$ su reducción módulo p. Definimos*

$$a_{p^e}(E) = p^e + 1 - \left|\widetilde{E}(\mathbb{F}_{p^e})\right|.$$

Teorema **4.16.** *Sea E una curva elíptica sobre $\mathbb{Q}$ con buena reducción en $p \in \mathbb{P}$ y $\widetilde{E}$ su reducción $\Rightarrow$ $[a_{p^e}(E)] = \sigma_{p^e,*} + \sigma_{p^e}^*$ como endomorfismo de $\mathrm{Pic}^0(\widetilde{E})$, siendo $\sigma_{p^e,*}$ y $\sigma_{p^e}^*$ el pushforward y el pullback respectivamente.*

Demostración. Pensemos a la función $\mathrm{id} : E \to E$ como multiplicar por 1 y consideremos el mapa $\sigma_{p^e} - 1$. La función $\sigma_{p^e} - 1$ es un morfismo de E. Para ver esto, veamos que $\sigma_{p,*} - 1_*$ está bien definido en $\mathrm{Pic}^0(E)$ y como por el Teorema 3.6, $\mathrm{Pic}^0(E)$ y E son isomorfos, entonces $\sigma_{p^e} - 1$ está bien definido en E.

Veamos ahora que $\sigma_{p^e} - 1$ es separable. En efecto, supongamos que $\sigma_{p^e} - 1 = f \circ \sigma_p$ con $f : E \to E$ un morfismo. Despejando, nos queda que $1 = (\sigma_{p^{e-1}} - f) \circ \sigma_p$, y esto es absurdo, puesto que σ_p no es un isomorfismo.

Ahora, dado que $\sigma_{p^e} \in Gal(\overline{\mathbb{F}}_p/\mathbb{F}_{p^e})$, entonces

$$\widetilde{E}(\mathbb{F}_{p^e}) = \left\{P \in \widetilde{E} : P^{\sigma_{p^e}} = P\right\} = \ker(\sigma_{p^e} - 1).$$

A su vez, como $\sigma_{p^e} - 1$ es separable, entonces $\left|\widetilde{E}(\mathbb{F}_{p^e})\right| = |\ker(\sigma_{p^e} - 1)| = \deg(\sigma_{p^e} - 1)$.

Se puede demostrar (aunque no lo haremos) que $h_* \circ h^* = [\deg(h)]$ al igual que con isogenias pero en caracterítica p. Usándolo con $h = \sigma_{p^e} - 1$ tenemos que

$$\left[\left|\widetilde{E}(\mathbb{F}_{p^e})\right|\right] = [\deg(\sigma_{p^e} - 1)] = (\sigma_{p^e} - 1)_* \circ (\sigma_{p^e} - 1)^* = (\sigma_{p^e,*} - 1_*) \circ (\sigma_{p^e}^* - 1^*) = [\deg(\sigma_{p^e})] + 1 - \sigma_{p^e,*} - \sigma_{p^e}^* = [p^e] + 1 - \sigma_{p^e,*} - \sigma_{p^e}^*.$$

□

Mediante $\sim$ podremos reducir también los mapas entre curvas proyectivas. Encontramos los siguientes resultados:

Teorema **4.17.** *Si $h : C \to C'$ es un morfismo entre curvas algebraicas, donde C' tiene género positivo, entonces existe $\widetilde{h} : \widetilde{C} \to \widetilde{C'}$ tal que:*

1. *El siguiente diagrama conmuta:*

$$\begin{array}{ccc} C & \xrightarrow{h} & C' \\ {\scriptstyle\sim}\downarrow & & \downarrow{\scriptstyle\sim} \\ \widetilde{C} & \xrightarrow{\widetilde{h}} & \widetilde{C'}. \end{array}$$

2. $\deg(\widetilde{h}) = \deg(h)$.

3. *Si $k : C' \to C''$ es otro morfismo entre curvas proyectivas y $\widetilde{k}$ es su reducción $\Rightarrow \widetilde{k \circ h} = \widetilde{k} \circ \widetilde{h}$.*

4. *El siguiente diagrama conmuta:*

$$\begin{array}{ccc} \mathrm{Pic}^0(C) & \xrightarrow{h_*} & \mathrm{Pic}^0(C') \\ {\scriptstyle\sim}\downarrow & & \downarrow{\scriptstyle\sim} \\ \mathrm{Pic}^0(\widetilde{C}) & \xrightarrow{\widetilde{h}_*} & \mathrm{Pic}^0(\widetilde{C'}). \end{array}$$

Un caso particular del Teorema 4.17, es cuando C y C' son curvas elípticas y h es una isogenia sobre $\overline{\mathbb{Q}}$. Si φ es una isogenia, también lo será $\widetilde{\varphi}$.

4.3. Relación de Eichler-Shimura

Sea $N \in \mathbb{N}$, $p \in \mathbb{P}$ y $\mathfrak{p}$ un ideal maximal de $\overline{\mathbb{Z}}$ que contiene al ideal $p\overline{\mathbb{Z}}$ como en la Sección 4.1.

Dada la relación entre toros complejos y curvas elípticas complejas presentada en el Teorema 3.5.(1), podemos extender la idea de Espacio de Moduli para pares curva elíptica-subgrupo cíclico, tanto en característica 0 como en característica p. En particular, consideremos la siguiente restricción de $S_1(N)$:

$$S_1(N)'_{gd} = \left\{[E, Q] \in S_1(N) : \widetilde{j(E)} \notin \{0, 1728\}\right\}$$

donde E es una curva elíptica racional con buena reducción módulo p y $Q \in E(\overline{\mathbb{Q}})$ es un punto de orden N. El hecho de que $\widetilde{j(E)}$ evite el conjunto $\{0, 1728\}$ está asociado a los problemas que implican estos valores en la curva elíptica de la ecuación (3.3).

Para curvas elípticas en $\overline{\mathbb{F}}_p$ definimos el Espacio de Moduli

$$\widetilde{S}_1(N) = \big\{(E,Q) : E \text{ curva elíptica en } \overline{\mathbb{F}}_p \ , \ Q \in E(\overline{\mathbb{F}}_p) \text{ punto de orden } N\big\}/\sim_1$$

donde $\sim_1$ es la equivalencia dada por $(E,Q) \sim_1 (E',Q') \iff \exists \varphi : E \to E'$ isomorfismo de grupos tal que $\varphi(Q) = Q'$ y la restricción

$$\widetilde{S}_1(N)' = \Big\{[E,Q] \in \widetilde{S}_1(N) : j(E) \notin \{0, 1728\}\Big\}$$

por analogía a lo hecho con $S_1(N)'_{gd}$. Se cumple que el mapa

$$\sim_S : S_1(N)'_{gd} \to \widetilde{S}_1(N)' \text{ dado por } [E,Q] \mapsto [\widetilde{E}, \widetilde{Q}] \tag{4.3}$$

es sobreyectivo.

En el Sección 2.1 mencionábamos que $X_1(N)$ es una curva algebraica sobre $\mathbb{Q}$. El siguiente teorema nos indica para qué primos tiene buena reducción y nos da un mapa conmutativo que utilizaremos más adelante:

Teorema **4.18** (Teorema de Igusa)**.** *Sea $N \in \mathbb{N}$ y $p \in \mathbb{P}$ tal que $p \nmid N$. Entonces $X_1(N)$ tiene buena reducción módulo p y el siguiente diagrama conmuta:*

$$\begin{array}{ccc} S_1(N)'_{gd} & \xrightarrow{\psi_1} & X_1(N) \\ {\scriptstyle \sim_S}\downarrow & & \downarrow{\scriptstyle \sim_X} \\ \widetilde{S}_1(N)' & \xrightarrow{\widetilde{\psi}_1} & \widetilde{X}_1(N) \end{array} \tag{4.4}$$

donde ψ_1 es el mapa del Teorema 2.15 que admite una reducción $\widetilde{\psi}_1$ en la que no entraremos en detalle, $\sim_S$ es el presentado en la ecuación (4.3) y $\sim_X$ es la reducción de la ecuación asociada a $X_1(N)$ como curva algebraica sobre $\mathbb{Q}$.

Nos interesa estudiar un diagrama con T_p de la forma:

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N)) \\ {\scriptstyle \sim}\downarrow & & \downarrow{\scriptstyle \sim} \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\widetilde{T_p}} & \mathrm{Pic}^0(\widetilde{X}_1(N)) \end{array} \tag{4.5}$$

La prueba de que existe un diagrama como (4.5) queda por fuera de este trabajo, sin embargo calcularemos cual es la forma de $\widetilde{T}_p$. La descripción de $\widetilde{T}_p$ se conoce como la relación de Eichler-Shimura.

Por lo visto en la Sección 2.5.2, para $S_1(N)$ el operador de Hecke T_p es:

$$T_p[E,Q] = \sum_{\substack{C\leq E \\ |C|=p}} [E/C, Q+C].$$

Dado que $\widetilde{T_p}$ hace conmutar el diagrama (4.5), entonces $\widetilde{T_p}\circ \sim = \sim \circ T_p$, por lo que para entender $\widetilde{T_p}$, precisamos entender $\left[\widetilde{E/C}, \widetilde{Q+C}\right]$ para todos los subgrupos C de orden p y los dos casos de reducción de E.

Comencemos con E con reducción ordinaria. Sea C_0 el núcleo del mapa $\sim$: $E[p] \to \widetilde{E}[p]$. Como E está en un cuerpo de característica 0, $E[p] = (\mathbb{Z}/p\mathbb{Z})^2$ y como E tiene reducción ordinaria, $\widetilde{E}[p] = \mathbb{Z}/p\mathbb{Z}$. Por el Teorema 4.9, $\sim$ es sobreyectivo, y usando el Primer Teorema de Isomorfismo, tenemos que $|C_0| = p$.

Teorema **4.19.** *Sea E una curva elíptica con reducción ordinaria y C un subgrupo de E de orden p, entonces*

$$\left[\widetilde{E/C}, \widetilde{Q+C}\right] = \begin{cases} \left[\widetilde{E}^{\sigma_p}, \widetilde{Q}^{\sigma_p}\right] & Si\ C = C_0 \\ \left[\widetilde{E}^{\sigma_p^{-1}}, [p]\widetilde{Q}^{\sigma_p^{-1}}\right] & Si\ C \neq C_0 \end{cases}$$

Demostración. Caso $C = C_0$: Sean $E' = E/C_0$, $Q' = Q + C_0$ y $\varphi : E \to E'$ dado por $\varphi(x) = x + C_0$. En función del Teorema 3.5, podemos pasar de curvas elípticas a toros complejos; por lo tanto existen retículos Λ y Λ' tal que $E \simeq \mathbb{C}/\Lambda$, $E' \simeq \mathbb{C}/\Lambda'$, $\Lambda \subseteq \Lambda'$ y $\varphi(z+\Lambda) = z + \Lambda'$. Como $\ker(\varphi) = C_0$ cuyo orden es p, φ es p a 1 y por lo tanto la isogenia dual es $\psi : \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$ dada por $\psi(z+\Lambda') = pz + \Lambda \Rightarrow |\ker(\psi)| = deg(\psi) = p$.

Si pensamos a E' como el toro complejo $\mathbb{C}/\Lambda'$, tenemos que $|E'[p]| = p^2$ y utilizando el Primer Teorema de Isomorfismo, obtenemos que $|\psi(E'[p])| = \frac{|E'[p]|}{|\ker(\psi)|} = p$.

Además, como por el Teorema 2.12, $\varphi\psi = [p] \Rightarrow \varphi\psi(E'[p]) = [p](E'[p]) = \{0\} \Rightarrow \psi(E'[p]) \subseteq \ker(\varphi) = C_0$. Luego, como tiene el mismo orden, $\psi(E'[p]) = C_0$.

Consideremos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} E'[p] & \xrightarrow{\psi} & E[p] \\ \sim\downarrow & & \downarrow\sim \\ \widetilde{E'}[p] & \xrightarrow{\widetilde{\psi}} & \widetilde{E}[p]. \end{array}$$

Dado que $\widetilde{\psi}\circ \sim (E'[p]) = \sim \circ\psi(E'[p]) = \sim (C_0) = \sim (\ker(\sim)) = \{0\}$ y como $\sim$ es sobreyectiva, tenemos que $\widetilde{\psi}(\widetilde{E'}[p]) = \{0\} \Rightarrow \widetilde{E'}[p] \subseteq \ker(\widetilde{\psi})$.

Por otro lado, $\widetilde{\varphi}\widetilde{\psi} = [p]_{\widetilde{E'}} \Rightarrow \ker(\widetilde{\psi}) \subseteq \ker([p]_{\widetilde{E'}}) = \widetilde{E'}[p] \Rightarrow \ker(\widetilde{\psi}) = \widetilde{E'}[p]$.

Nos preocupamos ahora de los grados de todos los morfismos mencionados. En efecto, por el Teorema 4.17, $\deg(\widetilde{\varphi}) = \deg(\varphi) = |\ker(\varphi)| = p$, $\deg(\widetilde{\psi}) = \deg(\psi) = p$ y como $\deg([p]) = \deg(\varphi\psi) = \deg(\varphi)\deg(\psi) \Rightarrow \deg([p]) = p^2 = \deg([p]_{\widetilde{E'}})$.

Nos interesa ahora calcular los grados separables e inseparables. Dado que $\widetilde{\psi}$ es una isogenia, por el Teorema 4.14.(4), $\deg_{sep}(\widetilde{\psi}) = \left|\ker(\widetilde{\psi})\right| = p$. Luego, usando el Teorema 4.14.(1), obtenemos que $\deg_{ins}(\widetilde{\psi}) = 1$. Aplicando lo mismo a $[p]_{\widetilde{E'}}$, obtenemos que $\deg_{sep}([p]_{\widetilde{E'}}) = \ker([p]_{\widetilde{E'}}) = p \Rightarrow \deg_{ins}([p]_{\widetilde{E'}}) = p$.

Dado que $\deg_{sep}([p]_{\widetilde{E'}}) = \deg_{sep}(\widetilde{\psi})\deg_{sep}(\widetilde{\varphi}) \Rightarrow \deg_{sep}(\widetilde{\varphi}) = 1$ y aplicando lo mismo para $\deg_{ins}(\widetilde{\varphi})$, obtenemos que $\deg_{ins}(\widetilde{\varphi}) = p$.

De esta manera, obtenemos que $\widetilde{\varphi} = i \circ \sigma_p^e$ donde $deg(i) = 1$ y por lo tanto i es un isomorfismo que lleva $\widetilde{E}^{\sigma_p} \to \widetilde{E'}$ y $\widetilde{Q}^{\sigma_p} \to \widetilde{Q'}$ y $e = 1$.

Como los puntos del espacio de moduli son equivalentes módulo isomorfismos en las condiciones de i, tenemos que:

$$\left[\widetilde{E'}, \widetilde{Q'}\right] = \left[\widetilde{E}^{\sigma_p}, \widetilde{Q}^{\sigma_p}\right]$$

Caso $C \neq C_0$: Tomemos Q', E', φ y ψ de la misma manera que en el caso anterior y definamos $C' = \ker(\psi)$ y $C_0' = \ker(\sim')$. Consideremos el siguiente diagrama:

$$\begin{array}{ccc} E[p] & \xrightarrow{\varphi} & E'[p] \\ {\scriptstyle\sim}\downarrow & & \downarrow{\scriptstyle\sim'} \\ \widetilde{E}[p] & \xrightarrow{\widetilde{\varphi}} & \widetilde{E'}[p] \end{array} \tag{4.6}$$

Dado que E tiene reducción ordinaria, por el Teorema 4.9.(2), E' también y por tanto $\left|\widetilde{E'}[p]\right| = p$. Puesto que $|E'[p]| = p^2$, si aplicamos el Primer Teorema de Isomorfismo en la flecha vertical de la derecha, obtenemos que $|C_0'| = p$.

Dado que el diagrama anterior conmuta y que $C_0 = \ker(\sim)$ entonces $\varphi(C_0) \subseteq \ker(\sim') = C_0'$ y por tanto $|\varphi(C_0)| \in \{1, p\}$. Si $\varphi(C_0) = \{0\}$ entonces $C_0 \subseteq \ker(\varphi) = C$ y dado que ambos tienen orden p, entonces $C = C_0$ lo cual es absurdo. Por lo tanto $|\varphi(C_0)| = p \Rightarrow \varphi(C_0) = C_0'$.

Dado que $C_0 \subseteq E[p] \Rightarrow \{0\} = [p](C_0) = \psi\varphi(C_0) \Rightarrow \varphi(C_0) \subseteq \ker(\psi) = C'$. Por otro lado y en virtud de los Teoremas 2.12.(3) y 4.14.(4), $\deg(\psi) = \deg(\varphi) =$

$|\ker(\varphi)| = |\ker(\psi)| = |C'| = p$ y como $|\varphi(C_0)| = p \Rightarrow \varphi(C_0) = C'$.

El cardinal $|E[p]| = p^2$, entonces por el Primer Teorema de Isomorfismo, $|\varphi(E[p])| = \frac{|E[p]|}{|\ker(\varphi)|} = p$. Por otro lado $\psi\varphi(E[p]) = [p](E[p]) = \{0\}$, entonces $\varphi(E[p]) \subseteq \ker(\psi)$ y como tienen el mismo orden, $\varphi(E[p]) = \ker(\psi) = C'_0$. Luego, utilizando el diagrama (4.6), $\widetilde{\varphi} \circ \sim (E[p]) = \sim' \circ \varphi(E[p]) = \sim' (C'_0) = \{0\} \Rightarrow \widetilde{E}[p] \subseteq \ker(\widetilde{\varphi})$. Por otro lado, $\widetilde{\psi}\widetilde{\varphi} = [p]_{\widetilde{E}} \Rightarrow \ker(\widetilde{\varphi}) \subseteq \ker([p]_{\widetilde{E}}) = \widetilde{E}[p]$.

Analizando una vez más los grados, obtenemos que $\widetilde{\psi} = i \circ \sigma_p$ con i un isomorfismo que lleva $\widetilde{Q'}^{\sigma_p} \mapsto \widetilde{\psi}(\widetilde{Q'}) = \sim \circ \psi(Q')$.
Por otro lado, $\psi(Q') = \psi(Q + C) = \psi\varphi(Q) = [p](Q) \Rightarrow \widetilde{\psi}(\widetilde{Q'}) = [p]\widetilde{Q}$.

Aplicando σ_p^{-1} a los coeficientes de i, tenemos que $i^{\sigma_p^{-1}}$ es un isomorfismo que lleva $\widetilde{Q'} \mapsto [p]\widetilde{Q}^{\sigma_p^{-1}}$. □

Nos preocupamos ahora de cuando E es supersingular:

Teorema **4.20.** *Sea E una curva elíptica con reducción supersingular y C un subgrupo de E de orden p, entonces*

$$\left[\widetilde{E/C}, \widetilde{Q + C}\right] = \left[\widetilde{E}^{\sigma_p}, \widetilde{Q}^{\sigma_p}\right] = \left[\widetilde{E}^{\sigma_p^{-1}}, \widetilde{Q}^{\sigma_p^{-1}}\right].$$

Demostración. Tomemos Q', E', φ y ψ de la misma manera que en el Teorema 4.19.

Para la primer igualdad, $[p]_{\widetilde{E}} = \widetilde{\psi}\widetilde{\varphi} \Rightarrow \ker(\widetilde{\varphi}) \subseteq \ker([p]_{\widetilde{E}}) = \widetilde{E}[p] = \{0\}$ por tener E reducción supersingular.

Dado que φ es una isogenía de curvas elípticas, usando propiedades del grado tenemos que: $\deg(\varphi) = |\ker(\varphi)| = p = \deg(\widetilde{\varphi})$ y como $\widetilde{\varphi}$ es una isogenía de curvas elípticas pero en característica $p \Rightarrow \deg_{sep}(\widetilde{\varphi}) = |\ker(\widetilde{\varphi})| = 1 \Rightarrow \deg_{ins}(\widetilde{\varphi}) = p \Rightarrow \widetilde{\varphi} = i \circ \sigma_p$ con i un isomorfismo. Luego, se repite lo hecho en el Teorema 4.19 en el caso de $C = C_0$.

Para la segunda igualdad, tomemos una vez más $C' = \ker(\psi)$. Como E tiene reducción supersingular, por el Teorema 4.9.(2), E' también $\Rightarrow \widetilde{E'}[p] = \{0\}$.
$[p]_{\widetilde{E'}} = \widetilde{\varphi}\widetilde{\psi} \Rightarrow \ker(\widetilde{\psi}) \subseteq \ker([p]_{\widetilde{E'}}) = \widetilde{E'}[p] = \{0\}$.

Dado que φ es una isogenía de curvas elípticas, usando propiedades del grado tenemos que $\deg(\psi) = \deg(\varphi) = |\ker(\varphi)| = p = \deg(\widetilde{\psi})$ y como $\widetilde{\psi}$ es una isogenía de curvas elípticas pero en característica $p \Rightarrow \deg_{sep}(\widetilde{\psi}) = \left|\ker(\widetilde{\psi})\right| = 1 \Rightarrow \deg_{ins}(\widetilde{\psi}) = p \Rightarrow \widetilde{\psi} = i \circ \sigma_p$ con i un isomorfismo. Luego, se repite lo hecho en el Teorema 4.19 en el caso de $C \neq C_0$. □

Definimos un análogo al operador diamante de la ecuación (2.3) para Espacios de Moduli pero en $\widetilde{S}_1(N)$. Si $n \in \mathbb{N}$ tal que $\text{mcd}(n, N) = 1$, definimos

$\widetilde{\langle n\rangle} : \widetilde{S}_1(N) \to \widetilde{S}_1(N)$ dado por $\widetilde{\langle n\rangle}([E,Q]) = [E,[n]Q]$.

Dado que hay $p+1$ subgrupos de orden p (ver Sección 2.5.2), para el caso de E con reducción ordinaria, tenemos que

$$\sum_{C\leq E:|C|=p} [\widetilde{E/C}, \widetilde{Q+C}] = \left[\widetilde{E}^{\sigma_p}, \widetilde{Q}^{\sigma_p}\right] + p\left[\widetilde{E}^{\sigma_p^{-1}}, [p]\widetilde{Q}^{\sigma_p^{-1}}\right] = (\sigma_p + p\widetilde{\langle p\rangle}\sigma_p^{-1})\left[\widetilde{E}, \widetilde{Q}\right].$$

Y dado que en el caso de E con reducción supersingular es más simple y los dos tipos de subgrupos dan lo mismo, podemos escribirlo igual que el caso ordinario, teniendo la expresión:

$$\sum_{C\leq E:|C|=p} [\widetilde{E/C}, \widetilde{Q+C}] = (\sigma_p + p\widetilde{\langle p\rangle}\sigma_p^{-1})\left[\widetilde{E}, \widetilde{Q}\right]$$

para todos los casos de buena reducción de E.

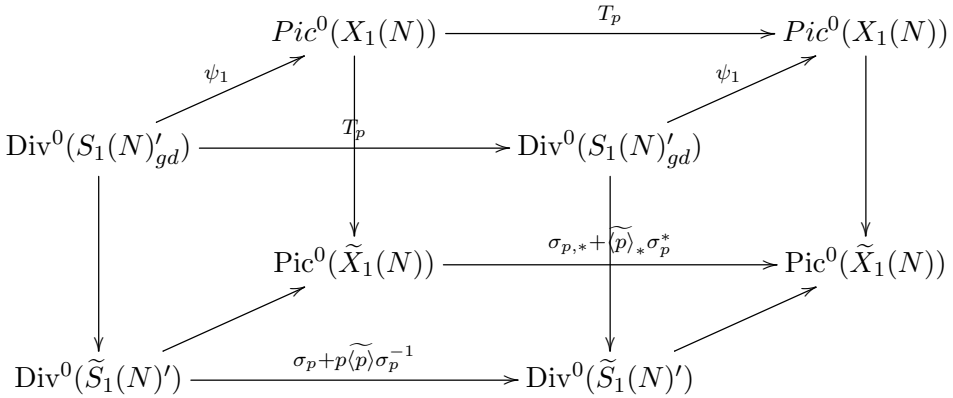
Trabajando con $S_1(N)'_{gd}$ y $\widetilde{S}_1(N)'$ tenemos entonces el siguiente diagrama:

$$\begin{array}{ccc} S_1(N)'_{gd} & \xrightarrow{T_p} & S_1(N)'_{gd} \\ \sim\downarrow & & \downarrow\sim \\ \widetilde{S}_1(N)' & \xrightarrow{\sigma_p+p\widetilde{\langle p\rangle}\sigma_p^{-1}} & \widetilde{S}_1(N)' \end{array}$$

que podemos extender rápidamente a divisores:

$$\begin{array}{ccc} \mathrm{Div}^0(S_1(N)'_{gd}) & \xrightarrow{T_p} & \mathrm{Div}^0(S_1(N)'_{gd}) \\ \sim\downarrow & & \downarrow\sim \\ \mathrm{Div}^0(\widetilde{S}_1(N)') & \xrightarrow{\sigma_p+p\widetilde{\langle p\rangle}\sigma_p^{-1}} & \mathrm{Div}^0(\widetilde{S}_1(N)'). \end{array} \tag{4.7}$$

Veamos ahora que podemos construir un diagrama 3D:



(4.8)

Numeremos las caras del cubo de la siguiente manera: la cara frontal será la cara '1', y luego para numerar las caras del '2' al '4', lo hacemos en sentido antihorario comenzando desde la cara 'l'. La cara '5' será la cara superior y la cara '6' la cara inferior.

Para demostrar que el cubo conmuta, necesitamos probar que las 6 caras conmutan. Probaremos primero 5 caras (todas menos la cara '3').

Cara 1

Es el diagrama (4.7).

Cara 5

Si usamos la función ψ_1 del Teorema 2.15, cambiando $Y_1(N)$ por $X_1(N)$ tenemos que $\psi_{1,*}$ lleva divisores de grado 0 en divisores de grado 0 y divisores principales en divisores principales, en virtud del Teorema 2.25. Luego usando la proyección cociente pasamos a Grupos de Picard obteniendo el siguiente diagrama:

$$\begin{array}{ccc}
\mathrm{Div}^0(S_1(N)) & \xrightarrow{T_p} & \mathrm{Div}^0(S_1(N)) \\
\downarrow{\scriptstyle \psi_{1,*}} & & \downarrow{\scriptstyle \psi_{1,*}} \\
\mathrm{Div}^0(X_1(N)) & \xrightarrow{T_p} & \mathrm{Div}^0(X_1(N)) \\
\downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\
\mathrm{Pic}^0(X_1(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N)).
\end{array}$$

Necesitaremos ver que $\pi \circ \psi_{1,*}$ es sobreyectivo. Sea $[D] \in \mathrm{Pic}^0(X_1(N))$. Dado que la cantidad de cúspides es finita (ver posterior a la definición 2.3), podemos aplicar el Teorema 2.26 para obtener un representante $D' \in [D]$ tal que D' sea cero en las cúspides. Luego, como el mapa $\psi_1 : S_1(N) \to Y_1(N)$ es biyectivo, $\psi_{1,*} : \mathrm{Div}^0(S_1(N)) \to \mathrm{Div}^0(Y_1(N))$ es biyectivo y por ende, existe un divisor $\widetilde{D} \in \mathrm{Div}^0(S_1(N))$ tal que $\psi_{1,*}(\widetilde{D}) = D'$ y por lo tanto $\pi\psi_{1,*}(\widetilde{D}) = [D]$.

Caras 2 y 4

Extendiendo el Teorema de Igusa para divisores y luego usando el Teorema 2.25 obtenemos:

$$\begin{array}{ccccc}
\mathrm{Div}^0(S_1(N)'_{gd}) & \xrightarrow{\psi_{1,*}} & \mathrm{Div}^0(X_1(N)) & \xrightarrow{\pi} & \mathrm{Pic}^0(X_1(N)) \\
\downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle \sim} \\
\mathrm{Div}^0(\widetilde{S}_1(N)') & \xrightarrow{\widetilde{\psi}_{1,*}} & \mathrm{Div}^0(\widetilde{X}_1(N)) & \xrightarrow{\pi} & \mathrm{Pic}^0(\widetilde{X}_1(N))
\end{array}$$

Cara 6

Daremos una idea sin detallar algunos diagramas. Primero, utilizando el mapa $\widetilde{\psi}_{1,*}$ de la cara 5, la definición de $\sigma_{p,*}$ dada en la Sección 4.2 y la proyección al Grupo de Picard, obtenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathrm{Div}^0(\widetilde{S}_1(N)') & \xrightarrow{\sigma_p} & \mathrm{Div}^0(\widetilde{S}_1(N)') \\ \downarrow{\scriptstyle \widetilde{\psi}_{1,*}} & & \downarrow{\scriptstyle \widetilde{\psi}_{1,*}} \\ \mathrm{Div}^0(\widetilde{X}_1(N)) & \xrightarrow{\sigma_{p,*}} & \mathrm{Div}^0(\widetilde{X}_1(N)) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\sigma_{p,*}} & \mathrm{Pic}^0(\widetilde{X}_1(N)). \end{array} \tag{4.9}$$

De la misma manera al diagrama (4.9), debido a la definición de σ_p^* en la Sección 4.2, tenemos un diagrama conmutativo con $p\sigma_p^{-1}$ y σ_p^*:

$$\begin{array}{ccc} \mathrm{Div}^0(\widetilde{S}_1(N)') & \xrightarrow{p\sigma_p^{-1}} & \mathrm{Div}^0(\widetilde{S}_1(N)') \\ \downarrow{\scriptstyle \widetilde{\psi}_{1,*}} & & \downarrow{\scriptstyle \widetilde{\psi}_{1,*}} \\ \mathrm{Div}^0(\widetilde{X}_1(N)) & \xrightarrow{\sigma_p^*} & \mathrm{Div}^0(\widetilde{X}_1(N)) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\sigma_p^*} & \mathrm{Pic}^0(\widetilde{X}_1(N)). \end{array} \tag{4.10}$$

Pese a que no formalizaremos en detalles, cabe mencionar que tenemos un diagrama 3D como el diagrama (4.8) para el operador diamante cambiando T_p por $\langle p\rangle$, a $\sigma_p + p\widetilde{\langle p\rangle}\sigma_p^{-1}$ por $\widetilde{\langle p\rangle}$ y a $\sigma_{p,*} + \widetilde{\langle p\rangle}_*\sigma_p^*$ por $\widetilde{\langle p\rangle}_*$. La cara inferior de ese diagrama 3D nos da el siguiente diagrama:

$$\begin{array}{ccc} \mathrm{Div}^0(\widetilde{S}_1(N)') & \xrightarrow{\widetilde{\langle p\rangle}} & \mathrm{Div}^0(\widetilde{S}_1(N)') \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\widetilde{\langle p\rangle}_*} & \mathrm{Pic}^0(\widetilde{X}_1(N)). \end{array} \tag{4.11}$$

Ahora basta con juntar los diagramas (4.9), (4.10) y (4.11) lo que nos da:

$$\begin{array}{ccc} \mathrm{Div}^0(\widetilde{S}_1(N)') & \xrightarrow{\sigma_p + p\widetilde{\langle p\rangle}\sigma_p^{-1}} & \mathrm{Div}^0(\widetilde{S}_1(N)') \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\sigma_{p,*} + \widetilde{\langle p\rangle}_*\sigma_p^*} & \mathrm{Pic}^0(\widetilde{X}_1(N)). \end{array} \tag{4.12}$$

que es la cara 6.

La cara '3' nos dará la relación Eichler-Shimura. Basta con ver el diagrama (4.5) de comienzo de la sección para identificar que en la cara '3' se encuentran todos los elementos del diagrama (4.5) salvo, por supuesto, $\widetilde{T}_p$, que es la función que hace conmutar al cubo.

Utilizando los diagramas (4.8) y (4.5) obtenemos los siguientes caminos:

$$\mathrm{Div}^0(S_1(N)'_{gd}) \xrightarrow{\pi\psi_{1,*}} \mathrm{Pic}^0(X_1(N)) \xrightarrow{\sim} \mathrm{Pic}^0(\widetilde{X}_1(N)) \xrightarrow{\sigma_{p,*}+\widetilde{\langle p\rangle}_*\sigma_p^*} \mathrm{Pic}^0(\widetilde{X}_1(N))$$

$$\mathrm{Div}^0(S_1(N)'_{gd}) \xrightarrow{\pi\psi_{1,*}} \mathrm{Pic}^0(X_1(N)) \xrightarrow{\sim} \mathrm{Pic}^0(\widetilde{X}_1(N)) \xrightarrow{\widetilde{T}_p} \mathrm{Pic}^0(\widetilde{X}_1(N)).$$

Dado que $\pi\psi_{1,*}$ y $\sim$ son sobreyectivos y los caminos son los mismos, obtenemos que $\widetilde{T}_p = \sigma_{p,*} + \widetilde{\langle p\rangle}_*\sigma_p^*$. Hemos demostrado:

Teorema **4.21** (Relación de Eichler-Shimura)**.** *Sea $N \in \mathbb{N}$ y $p \in \mathbb{P}$ tal que $p \nmid N$. Entonces el siguiente diagrama conmuta:*

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\sigma_{p,*}+\widetilde{\langle p\rangle}_*\sigma_p^*} & \mathrm{Pic}^0(\widetilde{X}_1(N)). \end{array}$$

En particular en $\widetilde{X}_0(N)$:

$$\begin{array}{ccc} \mathrm{Pic}^0(X_0(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_0(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_0(N)) & \xrightarrow{\sigma_{p,*}+\sigma_p^*} & \mathrm{Pic}^0(\widetilde{X}_0(N)). \end{array}$$

Para entender lo que ocurre en $\widetilde{X}_0(N)$, observemos que como $p \nmid N$, si C es un subgrupo de orden N en una curva elíptica E, entonces $[p]C = C$, puesto que cualquier generador de C es enviado por $[p]$ a otro generador de C, y por lo tanto $[E, C] = [E, [p]C]$ y entonces $\widetilde{\langle p\rangle}$ actúa trivialmente en $\widetilde{S}_0(N)$.

4.4. Relación entre formas modulares y curvas elípticas

La relación de Eichler-Shimura permite demostrar el siguiente corolario:

Teorema **4.22.** *Sea E una curva elíptica sobre $\mathbb{Q}$ con conductor N_E y sea $\alpha : X_0(N) \to E$ un morfismo sobreyectivo sobre $\mathbb{Q}$. Entonces, existe $f \in \mathcal{S}_2(\Gamma_0(M_f))$ una forma propia nueva tal que $M_f \mid N$ y $a_p(f) = a_p(E)$ $\forall p \in \mathbb{P}$ tal que $p \nmid N_E N$.*

Demostración. Si trabajamos momentáneamente en $\mathbb{C}$ (agregaremos un subíndice $\mathbb{C}$ para indicarlo en cada caso), utilizando los Teoremas 3.12 y 3.20 tenemos la siguiente isogenia:

$$\mathrm{Pic}^0(X_0(N)_{\mathbb{C}}) \xrightarrow{\varphi} \bigoplus_{f,n} A'_{f,\mathbb{C}}$$

donde n son divisores de N/M_f y f son representantes distintos de la equivalencia presentada previo al Teorema 3.19. De aquí, tenemos una isogenia dual

$$\bigoplus_{f,n} A'_{f,\mathbb{C}} \xrightarrow{\hat{\varphi}} \mathrm{Pic}^0(X_0(N)_{\mathbb{C}}).$$

El morfismo α, podremos extenderlo a un mapa $\alpha_{\mathbb{C}} : X_0(N)_{\mathbb{C}} \to E_{\mathbb{C}}$ de superficies de Riemann compactas que al igual que α será sobreyectivo.

Para cualquier $p \in \mathbb{P}$ tal que $p \nmid N_E N$, podemos considerar el siguiente diagrama:

$$\begin{array}{ccccc} \bigoplus_{f,n} A'_{f,\mathbb{C}} & & \xrightarrow{\prod_{f,n}(a_p(f)-a_p(E))} & & \bigoplus_{f,n} A'_{f,\mathbb{C}} \\ \downarrow{\scriptstyle \hat{\varphi}} & & & & \downarrow{\scriptstyle \hat{\varphi}} \\ \mathrm{Pic}^0(X_0(N)_{\mathbb{C}}) & & \xrightarrow{T_p - a_p(E)} & \mathrm{Pic}^0(X_0(N)_{\mathbb{C}}) & \xrightarrow{(\alpha_{\mathbb{C}})_*} \mathrm{Pic}^0(E_{\mathbb{C}}). \end{array} \tag{4.13}$$

Probemos que el diagrama anterior tiene las siguientes tres propiedades:

(a) Si $a_p(f) \neq a_p(E)$ el mapa de la fila superior lleva $\bigoplus_n A'_{f,\mathbb{C}}$ a $\bigoplus_n A'_{f,\mathbb{C}}$ de forma sobreyectiva.

(b) El cuadrado conmuta.

(c) El mapa compuesto en la fila inferior es el mapa nulo.

(a): Sea $\delta = a_p(f) - a_p(E)$. Como $a_p(f)$ es un entero algebraico (ver Teorema 3.14) y $a_p(E)$ es entero, entonces δ es solución de un polinomio mónico irreducible, es decir, $\delta^e + ... + a_e = 0$ con $a_e \neq 0$ puesto que $\delta \neq 0$. Reescribiendo, $\delta(\delta^{e-1} + ... + a_{e-1}) = -a_e$ y dado que $a_e \neq 0$, $-a_e$ es sobreyectivo como mapa entre variedades abelianas, y por tanto, también lo es δ ya que según lo observado luego de la ecuación (3.6), multiplicar es componer para los mapas de esa forma entre variedades abelianas.

(b): Es el diagrama (3.7) aplicado a A'_f y $J_0(N)$.

(c): Consideremos el siguiente diagrama:

$$\begin{array}{ccccc}
\mathrm{Pic}^0(X_0(N)) & \xrightarrow{T_p - a_p(E)} & \mathrm{Pic}^0(X_0(N)) & \xrightarrow{\alpha_*} & \mathrm{Pic}^0(E) \\
\sim\downarrow & & \sim\downarrow & & \downarrow\sim \\
\mathrm{Pic}^0(\widetilde{X}_0(N)) & \xrightarrow{\hat{\sigma}_{p,*}+\hat{\sigma}_p^*-\hat{a}_p(E)} & \mathrm{Pic}^0(\widetilde{X}_0(N)) & \xrightarrow{\widetilde{\alpha}_*} & \mathrm{Pic}^0(\widetilde{E}) \\
\mathrm{id}\downarrow & & & & \downarrow\mathrm{id} \\
\mathrm{Pic}^0(\widetilde{X}_0(N)) & \xrightarrow{\widetilde{\alpha}_*} & \mathrm{Pic}^0(\widetilde{E}) & \xrightarrow{\sigma_{p,*}+\sigma_p^*-a_p(E)} & \mathrm{Pic}^0(\widetilde{E}).
\end{array} \tag{4.14}$$

Para diferenciar el mapa $\sigma_{p,*} + \sigma_p^* - a_p(E) : \mathrm{Pic}^0(\widetilde{E}) \to \mathrm{Pic}^0(\widetilde{E})$ del mapa $\sigma_{p,*} + \sigma_p^* - a_p(E) : \mathrm{Pic}^0(\widetilde{X}_0(N)) \to \mathrm{Pic}^0(\widetilde{X}_0(N))$, le agregamos sombreros a este último como se puede ver en el diagrama (4.14).

Para ver porque el diagrama (4.14) conmuta, analicemos cada cuadrado. El cuadrado superior a la izquierda es la relación de Eichler-Shimura y a la derecha es el Teorema 4.17.(4). El cuadrado inferior conmuta por 4.12.(3) y 4.12.(4).

Ahora, por el Teorema 4.16, $\sigma_{p,*} + \sigma_p^* - a_p(E) = 0$ y por tanto $\sim \circ \alpha_* \circ (T_p - a_p(E)) = (\sigma_{p,*} + \sigma_p^* - a_p(E)) \circ \widetilde{\alpha}_* \circ \sim = 0$. Como la función $\sim$ es sobreyectiva, $\alpha_* \circ (T_p - a_p(E))$ no es sobreyectivo. Finalmente, dado que el mapa $\alpha_* \circ (T_p - a_p(E))$ es un mapa de una variedad a $\mathrm{Pic}^0(E)$ que es isomorfo a la curva algebraica E según el Teorema 3.6, puede ser nulo o sobreyectivo, y por lo tanto es nulo. Luego $\alpha_{\mathbb{C},*} \circ (T_p - a_p(E))$ es nulo.

Teniendo estas tres propiedades, podremos ahora terminar de demostrar este corolario.

Si $a_p(f) \neq a_p(E)$ para alguna f y para algún $p \nmid N_E N$, entonces por (a), el mapa $\prod_n (a_p(f) - a_p(E))$ del diagrama (4.13) que lleva $\bigoplus_n A'_{f,\mathbb{C}}$ en $\bigoplus_n A'_{f,\mathbb{C}}$ es sobreyectivo y como el diagrama conmuta por la propiedad (b), entonces $(T_p - a_p(E)) \circ \hat{\varphi}(\bigoplus_n A'_{f,\mathbb{C}}) = \hat{\varphi}(\bigoplus_n A'_{f,\mathbb{C}})$. Por la propiedad (c), dado que $\alpha_{\mathbb{C},*} \circ (T_p - a_p(E))$ es el mapa nulo, tenemos que $\hat{\varphi}(\bigoplus_n A'_{f,\mathbb{C}}) \subseteq \ker(\alpha_{\mathbb{C},*})$. Por lo tanto, si para cada f, hay un primo p para el cual $a_p(f) \neq a_p(E)$, entonces tenemos que $\hat{\varphi}(\bigoplus_{f,n} A'_{f,\mathbb{C}}) = \mathrm{Pic}^0(X_0(N)_{\mathbb{C}}) \subseteq \ker(\alpha_{\mathbb{C},*})$, y esto es absurdo pues $\alpha_{\mathbb{C},*}$ es un mapa sobreyectivo. Por lo tanto, tiene que existir una forma nueva f para la cual $a_p(f) = a_p(E)$ para todo $p \nmid N_E N$. □

Juntemos todo lo obtenido hasta ahora para dar una idea de como se obtiene el recíproco del Teorema de Modularidad. Sea $f \in \mathcal{S}_2(\Gamma_0(M_f))$ una forma propia nueva con coeficientes racionales. Por lo visto en el Teorema 3.21 y en el comentario posterior al mismo, A'_f es una curva elíptica y existe $\alpha : X_0(N) \to A'_f$ un morfismo sobreyectivo sobre $\mathbb{Q}$. Utilizando el Teorema 4.22, obtenemos que hay una forma nueva $g \in \mathcal{S}_2(\Gamma_0(M_f))$ tal que $a_p(g) = a_p(A'_f)$ para todos salvo finitos $p \in \mathbb{P}$.

Carayol en [Car86], completó el resultado anterior, demostrando que de hecho $f = g$, que $a_p(g) = a_p(A'_f)$ para todo $p \in \mathbb{P}$ y que M_f es igual al conductor de A'_f.

Definición **4.23.** *Sea E una curva elíptica sobre $\mathbb{Q}$ con conductor N_E. Definimos la función L de E de Hasse-Weil como:*

$$L(s, E) = \prod_{p \in \mathbb{P}} (1 - a_p(E)p^{-s} + \boldsymbol{1}_E(p)p^{1-2s})^{-1} \tag{4.15}$$

donde

$$\boldsymbol{1}_E(p) = \begin{cases} 1 & Si \quad p \nmid N_E \\ \\ 0 & Si \quad p \mid N_E \end{cases}$$

El valor de $\mathbf{1}_E(p)$ se asocia a si E tiene o no buena reducción módulo p. Por otro lado:

Definición **4.24.** *Sea $f \in \mathcal{S}_2(\Gamma_0(M_f))$ una forma propia de todos los Operadores de Hecke, nueva y normalizada. Definimos la función L de f como:*

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s}$$

cuando $f(z) = \sum_{n=1}^{\infty} a_n(f)q^n$.

Como f es una forma propia nueva normalizada, $a_n(f)$ es valor propio de T_n, y debido a la definición de T_n, $a_n(f)$ puede descomponerse en los $a_p(f)$ con $p \in \mathbb{P}$ de la misma forma que T_n lo hace en los T_p. Tenemos por tanto la siguiente relación para los coeficientes de f:

(1) $a_1(f) = 1$.

(2) $a_{p^r}(f) = a_p(f)a_{p^{r-1}}(f) - \mathbf{1}_N(p)pa_{p^{r-2}}$.

(3) $a_{mn}(f) = a_m(f)a_n(f)$ si $\text{mcd}(m, n) = 1$.

donde

$$\mathbf{1}_N(p) = \begin{cases} 1 & Si \quad p \nmid N \\ \\ 0 & Si \quad p \mid N \end{cases}$$

Para compararla con $L(s, E)$, buscamos escribir a $L(f, s)$ como producto de Euler. En efecto:

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \left(1 + \frac{a_2}{2^s} + \frac{a_{2^2}}{2^{2s}} + \cdots\right)\left(1 + \frac{a_3}{3^s} + \frac{a_{3^2}}{3^{2s}} + \cdots\right)\cdots =$$

$$= \prod_{p \in \mathbb{P}} \left(\sum_{r=0}^{\infty} a_{p^r} p^{-rs}\right)$$

donde en las igualdades anteriores se utilizaron las propiedades (1) y (3) de los $a_n(f)$. Ahora:

$$\sum_{r=0}^{\infty} a_{p^r} p^{-rs} \left(1 - a_p p^{-s} + \mathbf{1}_N(p) p^{1-2s}\right) =$$

$$= a_1 + p^{-s} a_p (1 - a_1) + \sum_{r=2}^{\infty} p^{-rs} \left(a_{p^r} - a_p a_{p^{r-1}} + \mathbf{1}_N(p) p a_{p^{r-2}}\right) = 1.$$

puesto que por la condición (2), cada término de la sumatoria es cero y por la condición (1), $a_1 = 1$. Juntando todo obtenemos:

$$L(s, f) = \prod_{p \in \mathbb{P}} (1 - a_p(f) p^{-s} + \mathbf{1}_N(p) p^{1-2s}). \tag{4.16}$$

Dado que A'_f es una curva elíptica, que $a_p(f) = a_p(A'_f)$ para todo $p \in \mathbb{P}$ y que M_f es igual al conductor de A'_f, observando las ecuaciones (4.15) y (4.16) concluimos que:

$$L(f, s) = L(A'_f, s).$$

Y esto completa el Recíproco del Teorema de Modularidad, puesto que dada $f \in \mathcal{S}_2(\Gamma_0(M_f))$ una forma propia nueva, construimos una curva elíptica A'_f tal que sus L-series coinciden.

Lista de Símbolos

A_f Variedad abeliana como cociente de $J_1(N)$ asociada a f. 39

A'_f Variedad abeliana como cociente de $J_0(N)$ asociada a f. 41

$a_n(f)$ Coeficiente de Fourier n-ésimo de f. 8

$a_{p^e}(E)$ Forma modificada de contar las soluciones de la curva elíptica E móodulo p^e. 49

$\mathbb{C}/\Lambda$ Toro complejo obtenido de un retículo Λ. 20

$\deg(\varphi)$ Grado de la isogenia φ. 22

$\Delta(E)$ Discriminante de la curva elíptica E. 31

$\Delta_{mn}(E)$ Discriminante de la ecuación de Weierstrass mínima global de E. 45

$\mathrm{Div}(X)$ Conjunto de divisores para X. 23

$\mathrm{Div}^0(X)$ Conjunto de divisores de grado 0 de X. 25

$\mathrm{Div}^\ell(X)$ Conjunto de divisores de grado ℓ de X. 25

E Curva elíptica. 31

$E(\overline{k})$ Conjunto de los puntos solución de la curva elíptica E en el cuerpo $\overline{k}$. 31

E_Λ Curva elíptica construida a partir del retículo Λ. 33

$\tilde{E}$ Reducción de la curva elíptica E módulo p. 45

e_x Grado de ramificación en x de un mapa entre superficies de Riemann. 24

$\mathbb{F}_p$ Cuerpo de p elementos. 43

$\overline{\mathbb{F}}_p$ Clausura algebrabica de $\mathbb{F}_p$. 43

g Género. 35

Γ Subgrupo de congruencia. 7

Lista de Símbolos

$\Gamma(N)$ Subgrupo de congruencia principal de nivel N. 7

$\Gamma_0(N)$ Subgrupo de congruencia. 8

$\Gamma_1(N)$ Subgrupo de congruencia. 8

$[\gamma]_k$ Operador de peso k. 8

$[\Gamma_1 \alpha \Gamma_2]_k$ Operador de Hecke de Γ_1 a Γ_2 con matriz asociada α para formas modulares de peso k. 10

$[\Gamma_1 \alpha \Gamma_2]$ Operador de Hecke de Γ_1 a Γ_2 con matriz asociada α para divisores y Grupos de Picard. 27

$\mathrm{GL}_2^+(\mathbb{Q})$ Matrices 2×2 con coeficientes racionales y determinante positivo. 10

$\mathcal{H}$ Semiplano superior complejo. 8

$\mathcal{H}^*$ Semiplano superior complejo extendido. 8

$H_1(X,\mathbb{Z})$ Grupo de homología de X. 35

h^* Pullback entre divisores. 25

h_* Pushforward entre divisores. 25

$j(E)$ Invariante de la curva elíptica E. 31

$J_0(N)$ Jacobiano de $X_0(N)$. 36

$J_1(N)$ Jacobiano de $X_1(N)$. 36

$\mathrm{Jac}(X)$ Jacobiano de X. 36

$\overline{k}(C)$ Cuerpo de funciones de C. 48

$\overline{k}[C]$ Anillo de coordenadas de C. 48

$\mathbb{K}_f$ Cuerpo de coeficientes de f. 39

λ_f Morfismo que de vuelve el valor propio de un Operador de Hecke. 38

Λ_z Retículo generado por z y 1. 21

$\mathcal{M}(\Gamma)$ Conjunto de las formas modulares de cualquier peso con respecto a Γ. 9

$\mathcal{M}_k(\Gamma)$ Conjunto de las formas modulares de peso k con respecto a Γ. 9

$[N]$ Isogenia de sumar N veces un punto de una curva elíptica. 33

$\langle n \rangle$ Operador diamante para el entero n. 11

N_E Conductor de la curva elíptica E. 46

$\nu_p(E)$ Valuación para el primo p de la curva elíptica E. 45

$\nu_x(f)$ Orden de anulación de f en x. 25

$\mathbb{P}$ Conjunto de los números primos. 11

$\mathfrak{p}$ Ideal maximal de $\overline{\mathbb{Z}}$. 43

$\wp_\Lambda$ Función $\wp$ de Weierstrass. 33

$\hat{\varphi}$ Isogenia dual. 22

$\mathrm{Pic}^0(X)$ Grupo de Picard de X. 26

ψ_0 Biyección entre $S_0(N)$ e $Y_0(N)$ presentada en el Teorema 2.15. 23

ψ_1 Biyección entre $S_1(N)$ e $Y_1(N)$ presentada en el Teorema 2.15. 23

q_h $e^{\frac{2\pi iz}{h}}$ con z en el disco unidad pinchado. 8

$\mathcal{S}(\Gamma)$ Conjunto de las formas cuspidales de cualquier peso con respecto a Γ. 9

$S_0(N)$ Espacio de Moduli para $\Gamma_0(N)$. 23

$S_1(N)$ Espacio de Moduli para $\Gamma_1(N)$. 23

$S_1(N)'_{gd}$ Puntos del espacio de Moduli en característica 0 de buena reducción y $j(E) \neq 0{,}1728$. 51

$\widetilde{S}_1(N)'$ Puntos del espacio de Moduli reducido con $j(E) \neq 0{,}1728$. 51, 55

$\widetilde{S}_1(N)$ Puntos del espacio de Moduli en característica p. 51

σ Encaje de un cuerpo en $\mathbb{C}$. 39

σ_p Automorfismo de Frobenius para el primo p. 47

σ_p^* Pullback para σ_p. 47

$\sigma_{p,*}$ Pushforward de σ_p. 47

σ_{p^e} Automorfismo de Frobenius para p^e. 47

$\mathcal{S}_k(\Gamma)$ Conjunto de las formas cuspidales de peso k con respecto a Γ. 9

$\mathcal{S}_k(\Gamma_1(N))^{new}$ Conjuntos de formas cuspidales nuevas de peso k y de nivel N. 16

$\mathcal{S}_k(\Gamma_1(N))^{old}$ Conjuntos de formas cuspidales viejas de peso k y de nivel N. 16

$\mathrm{SL}_2(\mathbb{Z})$ Matrices 2×2 con coeficientes enteros y determinante 1. 7

Lista de Símbolos

$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ Matrices 2×2 con coeficientes en $\mathbb{Z}/N\mathbb{Z}$ y determinante 1 (mód N). 7

$T^0(N)$ Conjunto de los Operador de Hecke coprimos con N. 14

$\mathbb{T}_{\mathbb{C}}$ Álgebra de Hecke sobre $\mathbb{C}$. 38

T_n Operador de Hecke para n natural. 13

$\mathrm{Tor}(E)$ Subgrupo de torsión de la curva elíptica E. 3

T_p Operador de Hecke para p primo. 11

$\mathbb{T}_{\mathbb{Z}}$ Álgebra de Hecke sobre $\mathbb{Z}$. 38

$(\omega_j)_{j\in J}$ Diferencial holomorfo sobre una superficie de Riemann. 35

$\Omega^1_{hol}(V)$ Conjunto de las formas diferenciales en el abierto V. 34

$\Omega^1_{hol}(X)$ Conjunto de las formas diferenciales en la superficies de Riemann X. 35

$\Omega^1_{hol}(X)^\wedge$ Espacio dual de $\Omega^1_{hol}(X)$. 35

$X(\Gamma)$ Curva modular compacta para Γ. 19

$X_0(N)$ Curva modular compacta para $\Gamma_0(N)$. 19

$X_1(N)$ Curva modular compacta para $\Gamma_1(N)$. 19

$Y(\Gamma)$ Curva modular no compacta para Γ. 19

$Y_0(N)$ Curva modular no compacta para $\Gamma_0(N)$. 19

$Y_1(N)$ Curva modular no compacta para $\Gamma_1(N)$. 19

$\overline{\mathbb{Z}}_{(\mathfrak{p})}$ Localización de $\overline{\mathbb{Z}}$ con el ideal $\mathfrak{P}$. 43

$\mathbb{Z}_{(p)}$ Localización de $\mathbb{Z}$ con el ideal $p\mathbb{Z}$. 44

Índice

Referencias

[Car86] H. Carayol. *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*. 1986.

[DS00] Fred Diamond and Jerry Shurman. *A first Course in Modular Forms*. 2000.

[Hat01] Allen Hatcher. *Algebraic Topology*. 2001.

Esta es la última página.
Compilado el martes 3 julio, 2018.
http://www.cmat.edu.uy/