Contents

0.1 Introducción

Panorama histórica

El propósito de esta tesis es describir la prueba de un caso particular, pero muy importante, de la conjetura de Shimura-Taniyama-Weil (STW). La fama de STW claramente viene de su rol en la prueba del Último Teorema de Fermat (UTF) que dice: para $n > 2$ tenemos

$$\exists x, y, z \in \mathbb{Z} \text{ tales que } x^n + y^n = z^n \quad \Longrightarrow \quad xyz = 0. \qquad \Big[\mathrm{UTF}(n)\Big]$$

Claramente si $d \mid n$, entonces $\mathrm{UTF}(d) \Longrightarrow \mathrm{UTF}(n)$. Esto quiere decir que solamente hay que considerar los casos cuando $n = p$ un primo impar; el caso $n = 4$ fue probado por el mismo Pierre de Fermat (1607-1665) cuando demostró que la ecuación $x^4 - y^4 = z^2$ no tiene soluciones enteras.

Hasta mediados del siglo XIX, algunos casos particulares de UTF se fueron probando: Euler probó el UTF para $n = 3$ en 1753, Dirichlet y Legendre ambos probaron el caso $n = 5$ en los 1820's y en 1839 Lamé prueba el caso $n = 7$. Ocho años después, Lamé presentó una prueba completa del UTF, pero resultó estar equivocada pues había asumido, incorrectamente, que el anillo de enteros $\mathbb{Z}[e^{2\pi i/p}]$ era un dominio de factorización única para todo primo p, pero esto no es cierto (e.g. $p = 23$). Usando estas ideas, Kummer probó el UTF para todo primo regular.[1]

Todo cambió cuando Frey sugirió una nueva alternativa en los 80's. Para ese entonces la geometría algebráica estaba bien fundamentada y ofrecía herramientas poderosas para estudiar el UTF. En el área particular de curvas elípticas, ya se había formado una conjetura importante:

$$\text{Toda curva elíptica sobre } \mathbb{Q} \text{ es modular.} \qquad \big[\mathrm{STW}\big]$$

Frey sugirió que de un contraejemplo $a^p + b^p = c^p$ de $\mathrm{UTF}(p)$, la curva elíptica asociada

$$E_{a,b,c,p} : \; y^2 = x(x - a^p)(x + b^p).$$

podría ser un contraejemplo de STW. Esta curva se llama la *curva de Frey* en su honor apesar de que la conexión entre la curva de Frey y el UTF fue establecido por Hellegouarch unos años antes.

Para argumentar porqué $E = E_{a,b,c,p}$ podría contradecir STW, Frey, junto con Serre, describieron las propiedades de las representaciones $\bar{\rho} = \bar{\rho}_{E,p}$ de Galois asociadas a los puntos de $p-$torsión de E. En particular, ellos probaron que $\bar{\rho}$ era impar, absolutamente irreducible, no-ramificado fuera de $2p$ y plano sobre p. Cumplir al mismo tiempo estas cuatro propiedades es excepcional para una representación de Galois y sugiere fuertemente que tal $\bar{\rho}$ no puede existir.

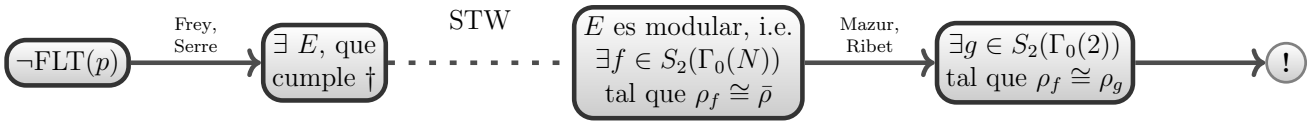
Serre formuló explícitamente varias conjeturas sobre cómo clasificar representaciones de Galois, e.g. $\bar{\rho}$, según la teoría de formas modulares. Más precisamente, estudió cómo asociar representaciones ρ_f a ciertas formas modulares f y cuando pasaba que una representación arbitraria ρ era de la forma $\rho = \rho_f$, i.e. cuando ρ era modular. En particular, Serre conjeturó que a las representaciones modulares ρ_f que además cumplían las propiedades extraordinarias de $\bar{\rho}$, se les podía bajar su *nivel* hasta su conducto de Artin.

La reducción de nivel de (ciertas) representaciones modulares lo probaron Ribet y Mazur en los 80's y por fin la intuición de Frey se confirmó: el conductor de Artin de $\bar{\rho}$ es 2, entonces si STW fuese cierto y E fuese modular, la representación $r\bar{h}o$ sería modular y por el teorema de

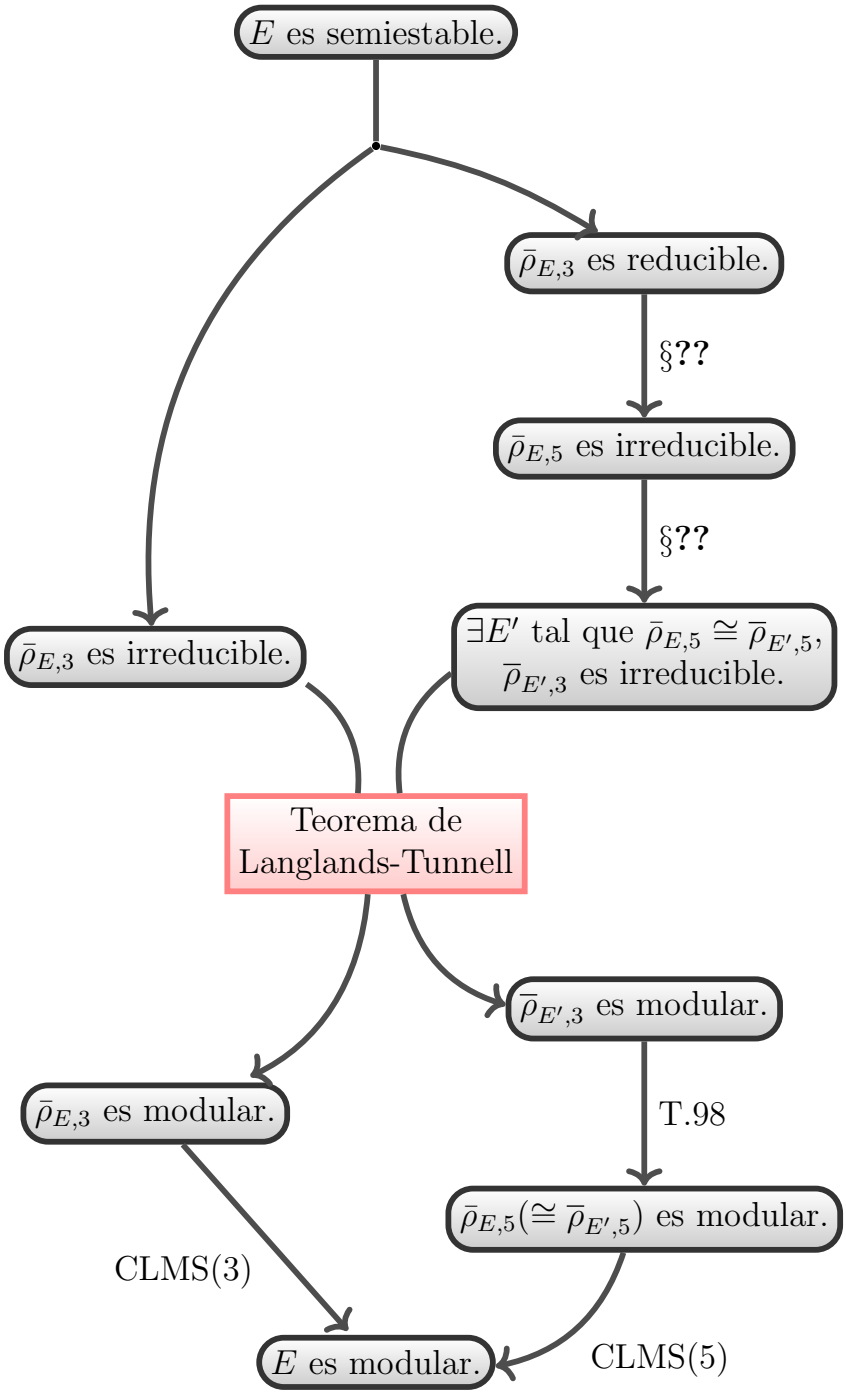
[1] Un primo p es *regular* si $p \nmid h_K$ donde h_K es el número de clase del campo $K = \mathbb{Q}(e^{2\pi i/p})$, i.e. el orden del grupo de Picard de $\mathrm{Spec}(\mathcal{O}_K)$.

Mazur-Ribet induce una representación modular de nivel 2 asociado a una forma modular cuspidal f de nivel 2 no trivial, pero era bien conocido que el espacio de tales formas modulares es nulo; contradicción. Por lo tanto la curva de Frey era un contraejemplo de STW. El camino a la prueba del UTF se iluminó: pruebas la conjetura de Shimura-Taniyama-Weil y pruebas el Último teorema de Fermat.

Esquemáticamente, la prueba del UTF se ve así:



Sobre la tesis



Chapter 1

Preliminares

1.1 Formas modulares

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

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

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

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

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

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

Esta acción no es fiel[2], en efecto $(\lambda\gamma)z = \gamma z$ para toda $\lambda > 0$. Por lo tanto la acción desciende al cociente con las matrices escalares y así obtenemos el isomorfismo:

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

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

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

Además, el subgrupo de isotropía de i es:

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

Por lo tanto tenemos una función continua y biyectiva $\mathrm{GL}_2^+(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}) \to \mathbb{H}$, más aún, esta biyección es un homeomorfismo[1].

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

cita de pontryagin

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

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

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

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

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

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

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

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

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

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

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

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

[1]En general, si hay una acción $G \curvearrowright X$ entonces la función natural $G/G_x = \mathrm{Orb}(x)$ es continua y biyectiva. Si además pedimos que G y X sean localmente compactos, y G sea segundo numerable, entonces esa función es un homeomorfismo. La prueba es estándar y usa el teorema de Baire (c.f. la proposición 1.2 y el lema 1.3 de §1.1 de [Milne, 2017]).

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

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

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

Las vecindades de $z \in \mathbb{Q} \cup \infty$ se llaman vecindades horocíclicas. En la figura 1.1 viene un ejemplo de un elemento de cada tipo de base local. De esta misma figura es claro que $\mathbb{H}^*$ es un espacio Hausdorff.

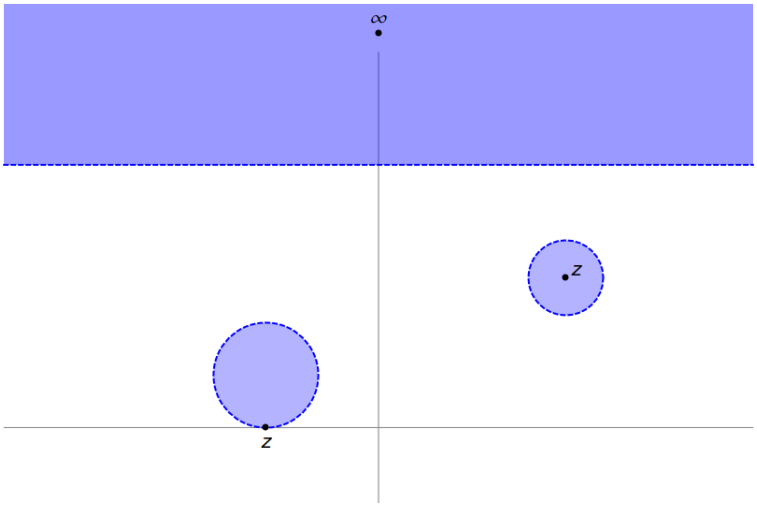


Figure 1.1: Un ejemplo de cada tipo de abierto básico de la topología de $\mathbb{H}^*$.

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

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

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

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

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

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

Proof. Aquí solamente esbozamos la prueba, para más detalles nos referimos a [Shimura, 1994, §1.3, teorema 1.28 y proposición 1.29 respectivamente]. La conexidad se sigue de que $\mathbb{H}^*$ es conexo. Ser Hausdorff se sigue de que la acción $\Gamma \curvearrowright \mathbb{H}^*$ es totalmente disconexa[2]. Lo localmente compacto se sigue de que existe una vecindad $V_C = \{z \in \mathbb{H}^* \mid \Im(z) \geq C\}$ de la cúspide ∞, tal que V_C/Γ_∞ queda identificado con V_C/Γ y así se calcula que

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

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

De hecho, a $X(\Gamma)$ le podemos dar una estructura de superficie de Riemann compacta (nos referimos a [Diamond and Shurman, 2005, §2.2, §2.3, §2.4] para detalles).

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

Proof. Es bien conocido que el conjunto

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

es un *dominio fundamental*[3] para la acción $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{H}$ (Véase la figura 1.2). Además $\mathcal{F}' := \mathcal{F} \cup \{\infty\} \subset \mathbb{H}^*$ es compacto. En efecto, dada cualquier cubierta abierta de $\mathcal{F}' \subseteq \bigcup U_i$, un abierto U_j contiene a ∞ y así contiene a un abierto de la forma $V = \{z \in \mathbb{H} \mid \Im(z) > C\} \cup \{\infty\}$. Por lo tanto

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

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

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

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

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

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

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

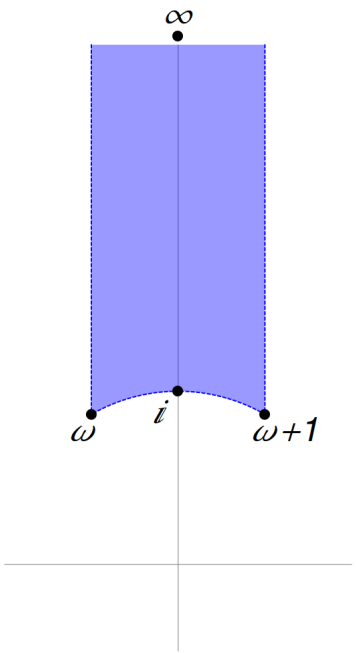


Figure 1.2: El dominio fundamental $\mathcal{F}$ de la acción $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{H}^*$ (aquí, $\omega = e^{2\pi i/3}$).

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

1.1.2 Subgrupos de congruencia

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

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

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

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

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

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

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

Tenemos que $\Gamma(N)$ es un subgrupo normal de $\mathrm{SL}_2(\mathbb{Z})$. En efecto si extendemos la proyección natural $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/N\mathbb{Z}$ a $\mathrm{SL}_2(\mathbb{Z})$, entrada por entrada, obtenemos un homomorfismo de grupos $\Gamma(1) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ que resulta ser sobre (c.f. [Shimura, 1994, §1.6, lema 1.38]). Por lo tanto tenemos la siguiente sucesión exacta:

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

Como consecuencia directa de esto tenemos que

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

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

Podemos calcular explícitamente el índice de $\Gamma(N)$. Es conocido que $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ tiene $(p^2-1)(p^2-p)$ elementos (c.f. [Rotman, 1995, Teorema 8.5, pg 219]) y en general:

$$\begin{aligned} \#\mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) &= p^{4\alpha}\left(1-\tfrac{1}{p}\right)\left(1-\tfrac{1}{p^2}\right), \\ \#\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) &= p^{3\alpha}\left(1-\tfrac{1}{p^2}\right), \end{aligned} \tag{1.1}$$

(c.f. [Shimura, 1994, §1.6]). Si $N = \prod p_i^{\alpha_i}$ es la factorización en primos, el teorema chino del residuo nos da el isomorfismo $\mathbb{Z}/N\mathbb{Z} \cong \prod(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$ que induce (otra vez por el teorema chino del residuo) el isomorfismo $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod \mathrm{SL}_2(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$. Con la fórmula (1.1) podemos concluir que

$$(\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)) = \#\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{p|N}\left(1-\tfrac{1}{p^2}\right). \tag{1.2}$$

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

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

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

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

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

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

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

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

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

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

ya que si tomamos $\gamma \in \Gamma_0(N)$ con $\det \gamma = ad - bc = 1$, la hipótesis de $c \equiv 0 \pmod N$ implica que $ad \equiv 1 \pmod N$. Para elegir un elemento arbitrario de $\Gamma_0(N)/\Gamma(N)$, solamente hay $\phi(N)$ maneras de elegir la entrada a y N maneras de elegir la entrada b.[4] Por lo tanto tenemos

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

donde hemos usado una fórmula muy conocida de ϕ [Ireland and Rosen, 1990, Proposición 2.2.5].

Con la fórmula anterior y con la fórmula para $(\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N))$ que calculamos en (1.2), podemos calcular el índice de $\Gamma_0(N)$ en $\mathrm{SL}_2(\mathbb{Z})$:

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

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

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

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

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

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

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

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

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

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

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

Proof. (c.f. [Shimura, 1994, §1.6, proposición 1.43]) □

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

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

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

Proof. La observación clave para aplicar la fórmula de Hurwitz es que el índice de ramificación de un elemento $z\Gamma_0(N) \in X_0(N)$ en la preimagen de $z\Gamma(1) \in X(1)$ bajo la función natural $X_0(N) \to X(1)$ es exactamente el índice $(\overline{\Gamma(1)_z} : \overline{\Gamma_0(N)_z})$ dentro de $\mathrm{PSL}_2(\mathbb{Z})$ (c.f. [Shimura, 1994, §1.5, proposición 1.37]). Para una prueba completa de este teorema ve [Shimura, 1994, §1.6, proposición 1.40] o ve [Diamond and Shurman, 2005, Teorema 3.1.1] para una prueba más detallada). □

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

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

además,

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

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

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

Por lo tanto el género de $X_0(15)$ es 1, es decir $X_0(15)$ es una curva elíptica. Observa que las cuatro cúspides son $0, \frac{1}{3}, \frac{1}{5}, \frac{1}{15}$ (donde $\frac{1}{15}$ es la cúspide ∞)

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

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

La figura 1.3 ilustra el dominio fundamental de $\Gamma_0(15)$ y muestra sus cuatro cúspides. Cada sección del dominio fundamental es la traslación del dominio fundamental de $\mathrm{SL}_2(\mathbb{Z})$ por un representante de los elementos de $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(N)$ En el apéndice viene otra imagen del dominio fundamental donde cada sección viene etiquetada con la matriz representante.

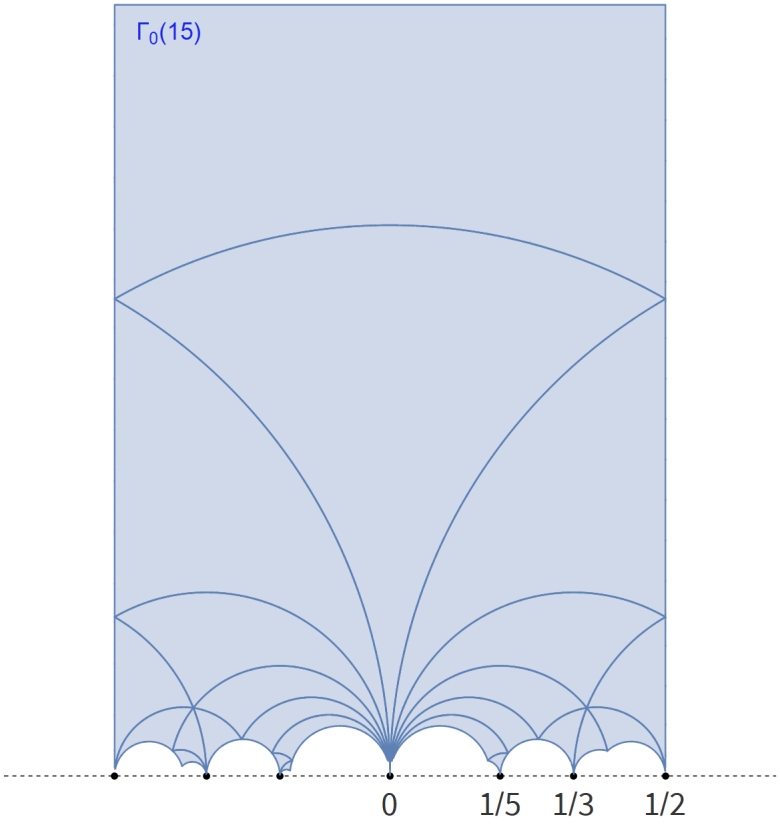


Figure 1.3: El dominio fundamental del subgrupo de congruencia $\Gamma_0(15)$

1.1.3 Formas Modulares y Operadores de Hecke

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

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

Pimero definimos dos conceptos fundamentales:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

y por lo anterior, f es $h\mathbb{Z}$-periódica. Esto quiere decir que f deciende a $\mathbb{H}/h\mathbb{Z}$, el espacio cociente de la acción $h\mathbb{Z} \curvearrowright \mathbb{H}$ de traslaciones $\{z \mapsto z + hk\}_{k\in\mathbb{Z}}$; por el momento, denotamos a este espacio cociente por $\widetilde{\mathbb{H}}$. Por lo tanto existe una función $\tilde{f} : \widetilde{\mathbb{H}} \to \mathbb{C}$ tal que $f = \tilde{f} \circ \pi$, donde $\pi : \mathbb{H} \twoheadrightarrow \widetilde{\mathbb{H}}$ es la proyección natural (véase el diagrama conmutativo 1.3).

Por otro lado, la función exponencial:

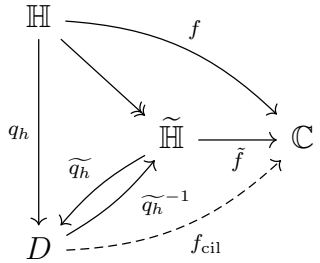
$$q_h : \mathbb{H} \longrightarrow D \qquad \text{definido por} \quad z \mapsto e^{2\pi i z/h},$$

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

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

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

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



(1.3)

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

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

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

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

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

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

La existencia de una extensión holomorfa $\widehat{f_{\text{cil}}}$ implica que f_{cil} es acotado cuando $q \to 0$. Gracias al comentario sobre el diagrama conmutativo (1.3), esto es equivalente a que $\Im(f(z))$ es acotado cuando $\Im(z) \to \infty$. Por lo tanto tenemos una condición suficiente para que una función débilmente modular sea holomorfa en ∞:

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

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

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

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

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

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

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

donde (*) se sigue de $\tau' \in \Gamma$ y f siendo débilmente $(\Gamma, k)-$modular. Acabamos de probar que $f[\gamma]_k$ es invariante bajo los $[\tau]_k-$operadores cuando $\tau \in \gamma^{-1}\Gamma\gamma$, es decir $f[\gamma]_k$ es débilmente $(\gamma^{-1}\Gamma\gamma, k)-$modular.[6] Por lo tanto tiene sentido hablar de holomorfía en ∞ de la función $f[\gamma]_k$. Además, simbólicamente tenemos que

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

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

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

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

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

Ahora estamos en posición para definir las formas modulares:

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

i) f es holomorfo.

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

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

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

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

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

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

[6] Podemos hablar de modularidad débil con respecto de $\gamma^1\Gamma\gamma$ porque éste es un subgrupo de congruencia cuando Γ lo es (c.f. [Bump, 1998, §1.4, lema 1.4.1]).

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

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

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

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

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

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

donde $\mu z = dxdy/y^2$ *(donde* $z = x + iy$*) es la medida hiperbólica de* $\mathbb{H}$ *y* V_Γ *es el volumen hiperbólico*[7] *de* $X(\Gamma)$*. i.e.* $V_\Gamma = \int_{X(\Gamma)} d\mu$*. A veces quitamos el "*Γ*" de la notación del producto interior cuando* Γ *es claro del contexto.* buscar cita

Proof. El inciso (i) es una aplicación clásica del teorema de Riemann-Roch[8]. El inciso (ii) se sigue de que $f \mapsto fdz$ es un isomorfismo entre $S_2(\Gamma)$ y el espacio de 1-formas diferenciales sobre $X_0(N)$ (c.f. el corolario 2.17 de [Shimura, 1994]). La igualdad $\dim S_2(\Gamma) = g$ se deduce (otra vez) de Riemann-Roch y el caso particular se sigue de que $X(\Gamma(1)) = \mathbb{H}^*/\Gamma(1) \approx \widehat{\mathbb{C}}$, la esfera de Riemann. El (iii) es trivial pues $M_k(\Gamma) \cdot M_{k'}(\Gamma) \subseteq M_{k+k'}(\Gamma)$. La prueba del inciso (iv) es elemental pero un poco técnica, entonces referimos al lector a §5.4 de [Diamond and Shurman, 2005]. □

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

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

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

La multiplicación por la izquierda induce una acción $\Gamma \curvearrowright \Gamma\alpha\Gamma'$. Como Γ y Γ' son de congruencia, entonces esta acción particiona a la clase bilateral en una cantidad finita de órbitas (c.f. lemas 5.1.1 y 5.1.2 de [Diamond and Shurman, 2005]), más precisamente:

$$\exists \beta_1, \ldots, \beta_n \in \Gamma\alpha\Gamma' \text{ tal que } \Gamma\alpha\Gamma' = \bigsqcup_{i=1}^{n} \Gamma\beta_i, \tag{1.4}$$

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

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

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

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

donde $H^0(X, \mathcal{L}(D))$ es el primer grupo de cohomología de la gavilla invertible $\mathcal{L}(D)$ asociada a D bajo el isomofismo $\mathrm{Cl}(X) \cong \mathrm{Pic}(X)$ entre el grupo de divisores módulo divisores principales y el grupo de Picard (c.f. el teorema 1.3 del capítulo IV de [Hartshorne, 1977] para una prueba).

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

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

donde $\Gamma\alpha\Gamma' = \sqcup\Gamma\beta_i$ es una descomposición como en (1.4).

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

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

De esta manera:

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

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

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

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

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

$$\big(f[\Gamma\alpha\Gamma']_k\big)[\gamma']_k = \Big(\sum f[\beta_i]_k\Big)\,[\gamma']_k = \sum f[\beta_i\gamma']_k = \sum f[\beta_i]_k = f[\Gamma\alpha\Gamma']_k.$$

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

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

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

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

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

$$\alpha_p = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}), \tag{1.5}$$

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

Definición 21. Sea p un número primo, $k \in \mathbb{N}$ y $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ un subgrupo de congruencia. El *$p-$ésimo operador de Hecke de peso k con respecto de* Γ es el operador $T_p : M_k(\Gamma) \to M_k(\Gamma)$ definido por la clase lateral $\Gamma\alpha_p\Gamma$, i.e. $T_p = [\Gamma\alpha_p\Gamma]_k$ (véase (1.5) para la definición de α_p).

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

Recuerde que hay un epimorfismo $\Gamma_0(N) \twoheadrightarrow (\mathbb{Z}/N\mathbb{Z})^*$ con núcleo $\Gamma_1(N)$ (c.f. la sección 1.1.2). Entonces $\Gamma_1(N)$ es un subgrupo normal de $\Gamma_0(N)$. Así, cuando $\alpha \in \Gamma_0(N)$, tenemos que $\alpha^{-1}\Gamma_1(N)\alpha = \Gamma_1(N)$ y por lo tanto el cociente $\Gamma_1(N) \setminus \Gamma_1(N)\alpha\Gamma_1(N)$ tiene solamente un elemento: $\Gamma_1(N)\alpha$. De esta manera, si $f \in M_k(\Gamma_1(N))$, entonces:

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

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

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

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

Una propiedad importante que cumplen los operadores diamante es:

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

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

donde definimos

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

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

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

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

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

donde $\langle e\rangle\langle d\rangle = \langle ed\rangle$ por la proposición 24 abajo. Como $e \mapsto de$ es una permutación de $(\mathbb{Z}/N\mathbb{Z})^*$, lo que está en paréntesis es simplemente $\pi_{\chi'}(f)$ que, por cierto, no depende de d. De las relaciones de ortogonalidad bien conocidas que cumplen los caracteres de grupos finitos[9] obtenemos:

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

Simbólicamente

$$\pi_\chi^2 = \pi_\chi \quad \text{y} \quad \pi_{\chi'}\pi_\chi = 0 \quad (\chi \neq \chi'). \tag{1.6}$$

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

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

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

donde $(*)$ se sigue del hecho de que la suma dentro de los paréntesis suma 0 cuando $d \neq 1$.[10] Estas dos igualdades implican respectivamente que

$$\pi_\chi(M_k(\Gamma_1(N))) \subseteq M_k(\Gamma_1(N),\chi) \quad \text{y} \quad \sum_{\chi\in G}\pi_\chi = \mathrm{Id}. \tag{1.7}$$

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

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

y por lo tanto

$$\pi_\chi|_{M_k(\Gamma_1(N),\chi)} = \mathrm{Id}. \tag{1.8}$$

De (1.6), (1.7) y (1.8) se sigue que $M_k(\Gamma_1(N),\chi)$ es un sumando directo de $M_k(\Gamma_1(N))$. De la segunda parte de (1.7) se sigue que los subespacios $M_k(\Gamma_1(N),\chi)$ generan a $M_k(\Gamma_1(N))$ y de la segunda parte de (1.6) se sigue que la intersección de esos subespacios es trivial. Por lo tanto $M_k(\Gamma_1(N))$ es la suma directa de sus subespacios $M_k(\Gamma_1(N),\chi)$ donde χ corre sobre G. □

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

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

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

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

[9] Véase, por ejemplo, el capítulo 16, §3 de [Ireland and Rosen, 1990] y en particular la proposición 16.3.1.

[10] Como $d \neq 1$, d determina un caracter no trivial del grupo finito G y es conocido que la suma de todos los valores un caracter no trivial es 0. Este argumento está en la prueba de la proposición 16.3.1 de [Ireland and Rosen, 1990].

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

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

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

Proof. Esto es exactamente la proposición 5.2.4 de [Diamond and Shurman, 2005]. □

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

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

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

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

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

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

$$T_m\langle n\rangle = \langle n\rangle T_m \qquad \forall n, m \in \mathbb{Z}^+. \tag{1.9}$$

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

$$T_mT_n = T_{nm} = T_nT_m \qquad \forall (n,m) = 1 \tag{1.10}$$

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

Nota. Con respecto del producto interior de Petersson, si $p \nmid N$, el operador adjunto de $\langle p\rangle$ es $\langle p^{-1}\rangle$ (donde p^{-1} es el inverso de $p \mod N$) y el operador adjunto de T_p es $\langle p^{-1}\rangle T_p$ (c.f. el teorema 5.5.3 de [Diamond and Shurman, 2005]). Por lo tanto la proposición 24 nos garantiza que $\langle p\rangle$ y T_p son operadores normales (i.e. conmutan con su operador adjunto) de la cual se sigue el siguiente resultado:

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

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

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

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

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

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

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

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

Proof. c.f. a la proposición 5.3.1 de [Diamond and Shurman, 2005]. □

1.1.4 Formas primitivas

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sea d es un divisor de N definimos la función:

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

Definimos:

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

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

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

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

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

Estos dos subespacios son invariantes bajo la acción de los operadores de Hecke:

Proposición 31. *Sea $\mathcal{H} = \{T_n, \langle n\rangle : S_k(\Gamma_0(N)) \to S_k(\Gamma_0(N)) \mid n > 0\}$ la familia de los operadores de Hecke, entonces:*

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

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

Proof. [Diamond and Shurman, 2005, §5.7] □

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

Nota. Puede suceder que una forma $f \in S_k$ no sea vector propio simultáneo para todo operador de Hecke pero sí lo sea para todos los operadores salvo una cantidad finita, e.g. la familia $\{T_n, \langle n\rangle \mid (n, N) = 1\}$. En este caso decimos que f es una *eigenforma fuera de N*. Similarmente, si f es además una forma nueva normalizada, decimos que es una *forma primitiva fuera de N*. Como esta condición es más general, la usaremos más seguido.

Los coeficientes de Fourier de una forma primitiva son sus valores propios con respecto de los operadores de Hecke $\{T_n \mid n > 0\}$, en efecto:

Proposición 33. *Sea $f \in S_k(\Gamma_0(N))$ una eigenforma (fuera de N) con coeficientes de Fourier $\lambda_n := a_n(f)$. Entonces existe un caracter $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ tal que $f \in S_k(\Gamma_0(N), \chi)$ (cf. proposición 23), en particular $\langle n\rangle f = \chi(n)f$ para todo $(n, N) = 1$. Si $\lambda_1 = 0$, entonces $T_n f = 0$ y $f \in S_k^{\text{old}}(\Gamma_0(N))$, Si $\lambda_1 \neq 0$ entonces:*

$$T_n f = \frac{\lambda_n}{\lambda_1} f \qquad \forall (n, N) = 1.$$

En particular si f está normalizada, i.e. $\lambda_1 = 1$, los valores propios de f bajo los operadores T_n son precisamente sus coeficientes de Fourier.

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

$$T_n f = b_n f \quad \text{y} \quad \langle n\rangle f = c_n f \qquad \text{donde } (n, N) = 1. \tag{1.11}$$

Por las propiedades del los operadores diamante, tenemos:

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

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

Solamente nos falta probar que $T_n f = (\lambda_n/\lambda_1)f$. Para esto calculamos $a_1(T_n f)$ de dos maneras distintas. Ya tenemos una fórmula general para calcular $a_1(T_n f)$ en la proposición 28. Por esta vía tenemos:

$$a_1(T_n f) = a_n(f) = \lambda_n \qquad \forall n > 0. \tag{1.12}$$

Por el otro lado, f es una eigenforma fuera de N, entonces por (1.11) tenemos

$$\lambda_n = a_1(T_n f) = a_1(b_n f) = b_n a_1(f) = b_n \lambda_1. \tag{1.13}$$

Aquí llegamos a dos casos: si $\lambda_1 \neq 0$, entonces tenemos

$$\frac{\lambda_n}{\lambda_1} = b_n \qquad \forall\ (n, N) = 1. \tag{1.14}$$

Pero si $\lambda_1 = 0$ entonces $\lambda_n = 0$ para toda $(n, N) = 1$. Por un resultado famoso debido a Atkin y Lehner publicado en en 1970, f necesariamente es una forma vieja, i.e. $f \in S_k^{\text{old}}(\Gamma_0(N))$, [Atkin and Lehner, 1970]. En [Diamond and Shurman, 2005, §5.7] viene una prueba detallada debida a David Carlton. □

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

Proposición 34. *Sea $f \in S_k^{\text{new}}(\Gamma_0(N), \chi)$ una forma primitiva. Entonces si denotamos $\lambda = \{a_n(f), \chi(n)\}_{n\geq 1}$, la extensión $\mathbb{Q}(\lambda)$ de $\mathbb{Q}$ es finita. Al campo $\mathbb{Q}(\lambda)$ se denota por K_f y se llama el* campo numérico de f.

Proof. Para una prueba con geometría algebráica, consulte [Deligne and Serre, 1974, proposición 2.7.3 de §2] o [Diamond and Shurman, 2005, §6.5]. En seguida escribimos una prueba elemental debida a Serre que aparece en [Serre, 1977b, §2.5]. buscar cita y poner prueba

Primero comentamos que $\mathbb{Q}(a_n(f) \mid n \geq 1) = \mathbb{Q}(a_p(f) \mid p \text{es primo})$ porque cada $a_n(f)$ es un combinación algebráica de las $a_p(f)$'s. Introducimos la siguiente notación: a cada forma primitiva $g \in S_k^{\text{new}}(\Gamma_0(N), \chi)$ le asociamos su sistema de valores propios afuera de N como el vector:

$$\lambda(g) = \{a_p(g)\}_{p \nmid N}.$$

Al conjunto de sistemas de valores propios lo denotamos por:

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

Como $S_k(\Gamma_0(N), \chi)$ es de dimensión finita, solamente puede haber una cantidad finita de sistemas de valores propios (c.f. corolario 27). Escribimos $\mathbb{Q}(\chi)$ para denotar la extensión de $\mathbb{Q}$ por la imagen del caracter χ y denotamos $G = \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}(\chi))$. Este gupo de Galois actúa sobre los coeficientes de Fourier de las formas primitivas. Más precisamente, si $g \in S_k^{\text{new}}(\Gamma_0(N), \chi)$ es una forma primitiva con serie de Fourier $g(z) = \sum a_m(g)q^m$ y $\sigma \in G$, entonces definimos g^σ con la serie de Fourier: explicar porque $a_n(f) \in \overline{\mathbb{Q}}$

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

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

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

y por lo tanto $(\chi(n)g)^\sigma = \chi(n)g^\sigma$. Además citamos sin prueba que

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

Una prueba para $k = 2$ se encuentra en [Diamond and Shurman, 2005, teorema 6.5.4] y el caso $k \geq 2$ se encuentra en [Shimura, 1994, §3.5]). Por último para probar el caso $k = 1$, se requiere de un truco técnico que aparece en la prueba que estamos siguiendo. Este resultado implica que:

$$\langle n \rangle g^\sigma = \chi^\sigma(n)g^\sigma = \chi(n)g^\sigma = (\chi(n)g)^\sigma = (\langle n \rangle g)^\sigma. \tag{1.15}$$

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

$$\begin{aligned}
a_m(T_p g)^\sigma &= \left(\sum_{d|(m,p)} d^{k-1} a_{pm/d^2}(\langle d \rangle g) \right)^\sigma = \sum_d (d^{k-1})^\sigma \chi^\sigma(d) \big(a_{pm/d^2}(g)\big)^\sigma \\
&= \sum_d d^{k-1} \chi(d) \big(a_{pm/d^2}(g)\big)^\sigma \qquad \big(\text{porque } \chi^\sigma = \chi\big) \\
&= \sum_d d^{k-1} \chi(d) a_{pm/d^2}(g^\sigma) = \sum_d d^{k-1} a_{pm/d^2}(\chi(d)g^\sigma) \\
&\overset{(1.15)}{=} \sum_d d^{k-1} a_{pm/d^2}(\langle d \rangle g^\sigma) \\
&= a_m(T_p g^\sigma) \quad \forall m \geq 1. \\
\therefore \quad T_p g^\sigma = (T_p g)^\sigma &= \big(a_p(g)g\big)^\sigma = a_p(g)^\sigma g^\sigma.
\end{aligned}$$

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

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

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

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

Nota. En la prueba con geometría algebraica de [Deligne and Serre, 1974], concluyen algo más fuerte que K_f sea una extensión finita. Con sus métodos deducen que además $a_n(f) \in \mathcal{O}_f$, el anillo de enteros de K_f. De esta manera es posible calcular congruencias módulo ideales primos de $\mathcal{O}_f$; esto es un detalle importante para la prueba de la modularidad de $\bar{\rho}_{E,3}$ de la sección 2.1. En este trabajo solamente probamos que $K_f/\mathbb{Q}$ es finito porque la prueba es elemental y más concisa. Para una prueba más detallada que la prueba de Deligne y Serre, véase el teorema 6.5.1 de [Diamond and Shurman, 2005].

1.1.5 Series de Eisenstein

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

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

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

Toda matriz

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

induce una permutación

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

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

$$\begin{aligned} E_{2k}\left(\frac{az+b}{cz+d}\right) &= \frac{1}{2}\sum_{n,m\in\mathbb{Z}}{}' \frac{1}{(m\frac{az+b}{cz+d}+n)^{2k}} = \frac{1}{2}\sum_{n,m\in\mathbb{Z}}{}' \frac{(cz+d)^{2k}}{(maz+mb+ncz+d)^{2k}} \\ &= \frac{(cz+d)^{2k}}{2}\sum_{n,m\in\mathbb{Z}}{}' \frac{1}{((ma+nc)z+(mb+nd))^{2k}} \\ &= \frac{(cz+d)^{2k}}{2}\sum_{n,m\in\mathbb{Z}}{}' \frac{1}{(mz+n)^{2k}} \\ &= (cz+d)^{2k} E_{2k}(z). \end{aligned} \tag{1.16}$$

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

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

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

Proposición 35. *Sea $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subset \mathbb{C}$ una retícula, entonces:*

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

Nota. Serre da dos pruebas en [Serre, 1973, §VII.2.2] y Shimura da otra prueba en [Shimura, 2012, §III.8].

Por lo tanto, cuando $k \geq 2$, la fórmula (1.16) es válida y concluimos que la serie de Eisenstein E_{2k} es débilmente $(\Gamma(1), 2k)-$modular. Para terminar de probar que E_{2k} es una forma modular, debemos probar que es holomorfa en ∞ (recuerde que $\Gamma(1)$ solamente tiene una cúspide).

Es bien conocido (por ejemplo [Bump, 1998, §1.3, pg. 28]) que E_{2k} tiene la siguiente expansión en serie de Fourier:

$$E_{2k}(z) = \zeta(2k) + \frac{(-1)^k(2\pi)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \left(\sum_{d|n} d^{2k-1} \right) e^{2\pi i n z} \tag{1.17}$$

Esta fórmula claramente prueba que $E_{2k}(z)$ es holomorfa en ∞ porque no tiene coeficientes negativos de Fourier. Concluimos que las fórmulas (1.16) y (1.17) implican que $E_{2k} \in M_{2k}(\Gamma(1))$.

Si usamos los números de Bernoulli y la identidad famosa

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

descubierta por Euler en 1735 [Euler, 1740], podemos reescribir la serie de Fourier como:

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

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

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

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

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

Definición 36. Sea $k \in \mathbb{Z}$ y $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ un caracter de Dirichlet módulo N, entonces la *serie de Eisenstein de peso k, caracter χ y parametro $s \in \mathbb{C}$* se define como

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

donde $z \in \mathbb{H}$.

Proposición 37. *La serie de Eisenstein $E_{k,\chi}$ satisface la ecuación de transfomación:*

$$E_{k,\chi}(\gamma z, s) = (cz+d)^k \left|cz+d\right|^{2s} \chi(d) E_{k,\chi}(z,s) \qquad \Re(s) > 1 - \tfrac{k}{2}. \tag{1.18}$$

Proof. Por proposición 35 la serie $E_{k,\chi}(z,s)$ es absolutamente convergente cuando $k + 2\Re(s) > 2$ o equivalentemente $\Re(s) > 1 - \frac{k}{2}$ (observa que el factor $\chi(m)$ no afecta la convergencia absoluta porque $|\chi(m)| = 1$). Además la serie es uniformemente convergente en cualquier conjunto compacto K en el semiplano $\Re(s) > 1 - \frac{k}{2}$ porque para cualquier compacto en este semiplano, existe una $\varepsilon > 0$ tal que $\Re(s) > 1 - \frac{k}{2} + \frac{\varepsilon}{2}$ para toda $s \in K$. De esta manera $k + 2\Re(s) > 2 + \varepsilon$ y tenemos que:

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

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

Sea

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

entonces:

$$\begin{aligned} E_{k,\chi}(\gamma z, s) &= \sum_{n,m\in\mathbb{Z}}{}' \frac{\chi(m)}{\left(m\frac{az+b}{cz+d}+n\right)^k \left|m\frac{az+b}{cz+d}+n\right|^{2s}} \\ &= \sum_{n,m\in\mathbb{Z}}{}' \frac{\chi(m)(cz+d)^k \left|cz+d\right|^{2s}}{((ma+nc)z+(mb+nd))^k \left|(ma+nc)z+(mb+nd)\right|^{2s}} \\ &= (cz+d)^k \left|cz+d\right|^{2s} \sum_{n,n\in\mathbb{Z}}{}' \frac{\chi(m)}{((ma+nc)z+(mb+nd))^k \left|(ma+nc)z+(mb+nd)\right|^{2s}}. \end{aligned} \tag{1.19}$$

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

$$\chi(ma+cn) = \chi(ma) = \chi(m)\chi(a) \quad \Longrightarrow \quad \chi(m) = \chi(ma+cn)\chi(d).$$

Sustituimos esta fórmula para $\chi(m)$ en (1.19) y recordamos que $(m,n) \mapsto (ma+nc, mb+nd)$ permuta los elementos de $\mathbb{Z}\times\mathbb{Z}$ para concluir que:

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

Por lo tanto

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

y terminamos. □

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

Este proceso es parte de un fenómeno más general; nos referimos a [Miyake, 1989, §7.2] para los detalles del caso general. En la aplicación del teorema de Langlands-Tunnel, se usa una serie de Eisenstein particular de peso $k=1$ torcida por el símbolo de Legendre módulo 3 definido por

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

Observemos que para cualquier caracter impar, i.e. $\chi(-1) = -1$, tenemos que

$$\frac{\chi(-m)}{(-mz+n)|-mz+n|^{2s}} = \frac{\chi(m)}{(mz-n)|mz-n|^{2s}}. \tag{1.20}$$

Por lo tanto obtenemos:

Proposición 38. *Sea $k=1$ y χ un caracter de Dirichlet impar. Además definimos la función auxiliar*

$$\phi(z;s) := \frac{1}{z^{1+s}\bar{z}^s} \qquad (z\in\mathbb{H},\ \Re(s)>\tfrac{1}{2}).$$

Con esta notación tenemos la siguiente identidad:

$$E_{1,\chi}(z,s) = 2\sum_{m=1}^{\infty} \chi(m) m^{-1-2s} \sum_{r=0}^{m-1} \sum_{n'=-\infty}^{\infty} \phi\left(z+\tfrac{r}{m}+n';s\right) \qquad (z\in\mathbb{H},\ \Re(s)>\tfrac{1}{2}). \tag{1.21}$$

Proof. Por la proposición anterior, la serie $E_{1,\chi}(z,s)$ converge absolutamente cuando $\Re(s) > 1/2$.

Como χ es impar, podemos usar (1.20) para calcular:

$$\begin{aligned}
E_{1,\chi}(z,s) &= \sum_{n,m\in\mathbb{Z}}{}' \frac{\chi(m)}{(mz+n)\,|mz+n|^{2s}} \\
&= \sum_{\substack{m=-\infty \\ m\neq 0}}^{\infty} \sum_{n=-\infty}^{\infty} \frac{\chi(m)}{(mz+n)\,|mz+n|^{2s}} \qquad (\text{porque } \chi(0)=0) \\
&= \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{\chi(m)}{(mz+n)\,|mz+n|^{2s}} + \frac{\chi(-m)}{(-mz+n)\,|-mz+n|^{2s}} \\
&= \sum_{m=1}^{\infty} \chi(m) \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)\,|mz+n|^{2s}} + \frac{1}{(mz-n)\,|mz-n|^{2s}} \\
\therefore E_{1,\chi}(z,s) &= 2\sum_{m=1}^{\infty} \chi(m) \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)\,|mz+n|^{2s}} \qquad (\Re(s)>\tfrac{1}{2}). \qquad (1.22)
\end{aligned}$$

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

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

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

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

Por lo tanto:

$$\sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)\,|mz+n|^{2s}} = \sum_{r=0}^{m-1} \sum_{n'\in\mathbb{Z}} \frac{m^{-1-2s}}{\left(z+\frac{r}{m}+n'\right)^{1+s}\left(\bar{z}+\frac{r}{m}+n'\right)^{s}}. \qquad (1.23)$$

podemos reescribir la ecuación (1.23) como

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

para que la ecuación (1.22), se reduzca a:

$$E_{1,\chi}(z,s) = 2\sum_{m=1}^{\infty} \chi(m) m^{-1-2s} \sum_{r=0}^{m-1} \sum_{n'=-\infty}^{\infty} \phi\left(z+\tfrac{r}{m}+n';s\right) \qquad (z\in\mathbb{H},\ \Re(s)>\tfrac{1}{2}).$$

□

Introducimos más notación: escribimos

$$S(z;s) := \sum_{n=-\infty}^{\infty} \phi(z+n;s), \qquad z\in\mathbb{H},\ \Re(s)>\tfrac{1}{2}. \qquad (1.24)$$

Esta notación nos resume la ecuación (1.21) a:

$$E_{1,\chi}(z,s) = 2\sum_{m=1}^{\infty}\chi(m)m^{-1-2s}\sum_{r=1}^{m-1}S\big(z+\tfrac{r}{m};s\big), \qquad z\in\mathbb{H},\ \Re(s)>\tfrac{1}{2}. \tag{1.25}$$

En lo que sigue, vamos a desarrollar la serie de Fourier de S como función de $x=\Re(z)$. Para esto usamos las siguientes notaciones: para $z=x+iy\in\mathbb{H}$,

$$\phi_{y,s}(x) := \phi(x+iy;s) \qquad , \qquad S_{y,s}(x) := S(x+iy;s).$$

Fijamos $y>0$ y $s\in\mathbb{C}$ tal que $\Re(s)>\frac{1}{2}$ junto con una constante $\frac{1}{2}<\delta<\Re(s)$. Observe que

$$\begin{aligned} &|\phi(x+iy;s)| = |x+iy|^{-\Re(s)-1}\,|x-iy|^{-\Re(s)} = |x+iy|^{-2\Re(s)-1}, \\ &\therefore \quad |\phi_{y,s}(x)| = O(|x|^{-2\delta-1}). \end{aligned} \tag{1.26}$$

Lema 39. *La serie*

$$S_{y,s}(x) = \sum_{n=-\infty}^{\infty}\phi_{y,s}(x+n)$$

converge absolutamente y uniformemente sobre $0\le x\le 1$. *En particular* $S_{y,s}(x)$ *es una función continua sobre el intervalo* $[0,1]$ *y* $1-$*periódico.*

Proof. Sea $0\le x\le 1$. En este caso, (1.26) implica que

$$|\phi_{y,s}(x+n)| = |x+n+iy|^{-2\Re(s)-1} \le |n-1+iy|^{-2\Re(s)-1} = O(n^{-2\delta-1}) \qquad (0\le x\le 1)$$

y así la serie $\sum\phi_{y,s}(x+n)$ converge absolutamente uniformemente sobre el intervalo $[0,1]$. Por lo tanto $S_{y,s}(x)$ es continua sobre el mismo intervalo. Por otro lado, es claro que

$$S_{y,s}(x+1) = \sum_{n\in\mathbb{Z}}\phi_{y,s}(x+n+1) = \sum_{n\in\mathbb{Z}}\phi_{y,s}(x+n) = S_{y,s}(x),$$

y terminamos. □

Como consecuencia del lema anterior $S_{y,s}$ tiene una serie de Fourier $\sum a_m e^{2\pi imx}$ cuyos coeficientes son:

$$\begin{aligned} a_m &= \int_0^1 S_{y,s}(x)e^{-2\pi imx}dx = \int_0^1\sum_{n\in\mathbb{Z}}\phi_{y,s}(x+n)e^{-2\pi imx}dx \\ &= \sum_{n\in\mathbb{Z}}\int_0^1\phi_{y,s}(x+n)e^{-2\pi imx}dx = \sum_{n\in\mathbb{Z}}\int_n^{n+1}\phi_{y,s}(x)e^{-2\pi im(x-n)}dx \\ &= \int_{-\infty}^{\infty}\phi_{y,s}(x)e^{-2\pi imx}dx \\ \therefore \quad a_m &= \hat{\phi}_{y,s}(m), \end{aligned}$$

donde $\hat{\phi}_{y,s}$ denota su transformada de Fourier que, por (1.26), existe cuando $\Re(s)>\frac{1}{2}$.

Para probar que $S_{y,s}$ es igual a su serie de Fourier, i.e.

$$S_{y,s}(x) = \sum_{n=-\infty}^{\infty} \hat{\phi}_{y,s}(n) e^{2\pi i n x}, \tag{1.27}$$

solamente nos falta probar[11] que la serie de Fourier converge absolutamente, es decir:

$$\sum_{n=-\infty}^{\infty} |\hat{\phi}_{y,s}(n)| < \infty \qquad (y > 0,\ \Re(s) > \tfrac{1}{2}). \tag{1.28}$$

Para este fin tenemos la siguiente proposición técnica que probamos en el apéndice y que viene, de manera más general, en [Miyake, 1989, §7.2].

Proposición 40. *Sean $y > 0$ y $n \in \mathbb{Z}$ fijos y denota $\varphi_{y,n}(s) := \hat{\phi}_{y,s}(n)$. Entonces:*

i) $\varphi_{y,n}(s)$ es holomorfa en el semiplano $\mathbb{H}' = \{z \in \mathbb{C} \mid \Re(z) > 0\}$.

ii) $\varphi_{y,n}(s)$ admite una extensión holomorfa a todo $\mathbb{C}$ definida por

$$\varphi_{y,n}(s) = \hat{\phi}_{y,s}(n) = \begin{cases} \dfrac{i\pi^s n^{s-1} e^{-2\pi n y}}{2\Gamma(s) y^{s+1}} \widetilde{\sigma}(4\pi n y; s, s+1) & n > 0 \\ 2\pi i (2y)^{-2s} \Gamma(2s) \Gamma(s)^{-1} \Gamma(s+1)^{-1} & n = 0 \\ \dfrac{2i\pi^{s+1} |n|^s e^{-2\pi |n| y}}{y^s \Gamma(s+1)} \widetilde{\sigma}(4\pi |n| y; s+1, s) & n < 0 \end{cases}. \tag{1.29}$$

donde

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

admite una extensión holomorfa a todo $\mathbb{H}' \times \mathbb{C} \times \mathbb{C}$.

iii) En particular:

$$\varphi_{y,n}(0) = \hat{\phi}_{y,0}(n) = \begin{cases} 0 & n > 0 \\ 2\pi i e^{2\pi n y} & n \leq 0 \end{cases}.$$

iv) Para todo subconjunto compacto $Q \subset \mathbb{C}$ existen constantes $A, B > 0$ tales que

$$|\varphi_{y,n}(s)| = |\hat{\phi}_{y,s}(n)| \leq \begin{cases} A y^{-\Re(s)-1} n^{\Re(s)-1} (1 + (4\pi n y)^{-B}) e^{-2\pi n y} & n > 0 \\ A y^{-\Re(s)} |n|^{\Re(s)} (1 + (4\pi |n| y)^{-B}) e^{-2\pi |n| y} & n < 0 \end{cases}.$$

Con esta proposición podemos probar la convergencia absoluta de la serie de Fourier de $S_{y,s}$, i.e.

$$\sum_{n=-\infty}^{\infty} |\hat{\phi}_{y,s}(n)| < \infty, \qquad y > 0,\ \Re(s) > \tfrac{1}{2},$$

[11] Esto es un resultado estándar del análsis de Fourier. Véase, por ejemplo, el corolario 2.3 de [Stein and Shakarchi, 2002] para una prueba explícita.

Para probar esto introducimos la siguiente notación:

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

y separamos esta serie en las dos series

$$S_{+}(z;s) := \sum_{n=1}^{\infty} \hat{\phi}_{y,s}(n) e^{2\pi i n x} \quad \text{y} \quad S_{-}(z;s) := \sum_{n=1}^{\infty} \hat{\phi}_{y,s}(-n) e^{-2\pi i n x}.$$

Corolario 41. *$S(z;s)$ admite una continuación holomorfa a $\mathbb{H} \times \{\Re(s) > -\frac{1}{2}\}$ definida por la fórmula:*

$$S(z;s) = \sum_{\substack{n=-\infty \\ n\neq 0}}^{\infty} \hat{\phi}_{y,s}(n) e^{2\pi i n x} = \hat{\phi}_{y,s}(0) + S_{\pm}(z;s), \qquad z = x+iy \in \mathbb{H},\ \Re(s) > -\tfrac{1}{2}, \tag{1.30}$$

donde $S_{\pm}$ es holomorfa sobre $\mathbb{H} \times \mathbb{C}$ y $\hat{\phi}_{y,s}(0)$ es meromorfa sobre $\mathbb{H} \times \mathbb{C}$ con polos en $s = -\frac{1}{2}, -\frac{3}{2}, -\frac{5}{2}, \ldots$. Además, para todo compacto $Q \subset \mathbb{H} \times \{\Re(s) > -\frac{1}{2}\}$, existen constantes $\varepsilon, A, B, M > 0$ tales que

$$|S(z;s)| \leq A \sum_{n=1}^{\infty} n^M (1 + (4\pi\varepsilon n)^{-B}) e^{-2\pi\varepsilon n} \qquad \forall (z,s) \in Q.$$

Proof. Ya habíamos mencionado en (1.28) que la fórmula (1.30) se siguiría de Con esta notación tenemos:

$$S(z;s) = \hat{\phi}_{y,s}(0) + S_{\pm}(z;s) = \hat{\phi}_{y,s}(0) + S_{+}(z;s) + S_{-}(z;s).$$

Probaremos que las series S_+ y S_- convergen absolutamente y uniformemente sobre cualquier subconjunto compacto de $\mathbb{H} \times \mathbb{C}$. Aquí estamos usando tácitamente la proposición anterior que define $\hat{\phi}_{y,s}$ para todo valor de $s \in \mathbb{C}$. Todo esto implicaría que la serie de Fourier $\sum \hat{\phi}_{y,s}(n) e^{2\pi i n x}$ de $S_{y,s}$ converge absolutamente (y uniformemente); precisamente lo que necesitamos. Además implicaría que $S_{\pm}(z;s)$ es holomorfa sobre $\mathbb{H} \times \mathbb{C}$. Procedemos a probar la convergencia absoluta y uniforme de S_+ y S_- sobre compactos de $\mathbb{H} \times \mathbb{C}$.

Sea $Q \subset \mathbb{H} \times \mathbb{C}$ un subconjunto compacto y $(z,s) \in Q$ donde $z = x+iy$. De una vez elegimos $\delta > 0$ tal que $\delta < y$ para toda $(x+iy, s) \in Q$. Gracias a la aproximación de la proposición 40 inciso iv) existen constantes $A, B > 0$ tales que:

$$\begin{aligned} |\hat{\phi}_{y,s}(n)| &\leq A y^{-\Re(s)-1} n^{\Re(s)-1} (1 + (4\pi n y)^{-B}) e^{-2\pi n y} \\ &\leq A y^{-\Re(s)-1} n^{\Re(s)-1} (1 + (4\pi n \delta)^{-B}) e^{-2\pi n \delta}, \quad \forall (z,s) \in Q\ n > 0. \end{aligned}$$

Además $\Re(s)$ está acotada superiormente por ejemplo $\Re(s) < M+1$, entonces $n^{\Re(s)-1} \leq n^M$ para toda $n \geq 1$ y así

$$|\hat{\phi}_{y,s}(n)| \leq A y^{-\Re(s)-1} n^M (1 + (4\pi n \delta)^{-B}) e^{-2\pi n \delta}, \quad \forall (z,s) \in Q\ n > 0. \tag{1.31}$$

Similarmente si $n < 0$ y $(z,s) \in Q$ tenemos que

$$|\hat{\phi}_{y,s}(n)| \leq A y^{-\Re(s)} |n|^{M+1} (1 + (4\pi |n| \delta)^{-B}) e^{-2\pi |n| \delta}, \quad \forall (z,s) \in Q\ n < 0. \tag{1.32}$$

Entonces:

$$|S_+(z;s)| = \left|\sum_{n=1}^{\infty} \hat{\phi}_{y,s}(n)e^{2\pi inx}\right| \leq \sum_{n=1}^{\infty} |\hat{\phi}_{y,s}(n)e^{2\pi inx}|$$
$$\leq Ay^{-\Re(s)-1}\sum_{n=1}^{\infty} n^M(1+(4\pi n\delta)^{-B})e^{-2\pi n\delta} \quad \forall (z,s)\in Q.$$

Además, como $y^{-\Re(s)-1}$ es una función continua sobre Q, está acotado por una constante que podemos tomar como $L/A > 0$ para alguna $L > 0$. Por lo tanto: para toda $(z,s) \in Q$ existen constantes $\delta, B, L, M > 0$ tales que:

$$|S_+(z;s)| \leq L\sum_{n=1}^{\infty} n^M(1+(4\pi n\delta)^{-B})e^{-2\pi n\delta} < \infty. \tag{1.33}$$

Así $S_+(z;s)$ converge absolutamente y uniformemente sobre Q para todo compacto $Q \subset \mathbb{H}\times\mathbb{C}$. Similarmente para toda $(z,s)\in Q$,

$$|S_-(z;s)| \leq L\sum_{n=1}^{\infty} n^{M+1}(1+(4\pi n\delta)^{-B})e^{-2\pi n\delta} < \infty,$$

y por lo tanto la serie $S_-(z;s)$ converge absolutamente y uniformemente sobre cualquier subconjunto compacto de $\mathbb{H}\times\mathbb{C}$. Concluimos que S_+ y S_- son funciones holomorfas sobre $\mathbb{H}\times\mathbb{C}$ y de esta manera, $S_\pm = S_+ + S_-$ también es holomorfa sobre $\mathbb{H}\times\mathbb{C}$. Además, si cambiamos M por $M+1$ en (1.33) obtenemos

$$|S_\pm(z;s)| \leq 2A\sum_{n=1}^{\infty} n^{M+1}(1+(4\pi\varepsilon n)^{-B})e^{-2\pi\varepsilon n}. \tag{1.34}$$

En particular, si $Q \subset \mathbb{H}\times\{\Re(s) > -\frac{1}{2}\}$, el término

$$\hat{\phi}_{y,s}(0) = \frac{2\pi i(2y)^{-2s}\Gamma(2s)}{\Gamma(s)\Gamma(s+1)}$$

es una función continua de s pues $\Gamma(2s)/\Gamma(s)$ es continuo para $2s > -1$. Entonces $|\hat{\phi}_{y,s}(0)|$ es acotado por una constante $C > 0$ sobre Q. Esta cota la absorbe la constante A de (1.34) y con esto deducimos la aproximación que necesitábamos demostrar.

Por lo tanto podemos concluir que $S_{y,s}$ es igual a su serie de Fourier:

$$S(z;s) = \hat{\phi}_{y,s}(0) + \sum_{\substack{n=-\infty\\ n\neq 0}}^{\infty} \hat{\phi}_{y,s}(n)e^{2\pi inx} = \underbrace{\frac{2\pi i(2y)^{-2s}\Gamma(2s)}{\Gamma(s)\Gamma(s+1)}}_{*} + S_\pm(z;s). \tag{1.35}$$

Esto quiere decir que $S(z;s)$ es suma de la función holomorfa $S_\pm$ con el cociente (*) que es una función meromorfa con polos en $s = -\frac{1}{2}, -\frac{3}{2}, -\frac{5}{2}\ldots$, i.e. los polos de $\Gamma(2s)$ que no son los polos de $\Gamma(s)$ ni de $\Gamma(s+1)$. Observe que como $2y$ es un real, no necesitamos definir una rama del logaritmo para que $(2y)^{-2s}$ sea holomorfa. Con todo esto, concluimos que el lado derecho de (1.30) es una función meromorfa que define una extensión de $S(z;s)$ a $\mathbb{H}\times\mathbb{C}$.

Por último usamos el inciso iii) de la proposición 40 para calcular $S_\pm(z;0)$. Claramente tenemos que $S_+(z;0)=0$ y así

$$S_\pm(z;0)=S_-(z;0)=\sum_{n=1}^{\infty}\hat{\phi}_{y,0}(-n)e^{-2\pi inx}=2\pi i\sum_{n=1}^{\infty}e^{-2\pi in(x+iy)}=2\pi i\sum_{n=1}^{\infty}e^{-2\pi inz}.$$

Por lo tanto sustituimos $s=0$ en (1.35) para obtener

$$S(z;0)=2\pi i\frac{(2y)^{-2\cdot 0}\Gamma(2\cdot 0)}{\Gamma(0)\Gamma(0+1)}+S_\pm(z;0)=2\pi i\sum_{n=0}^{\infty}e^{-2\pi inz}=\frac{2\pi i}{1-e^{-2\pi iz}}.$$

□

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

Proof. Fijamos $m\geq 1$ y usamos la fórmula de S para calcular

$$\sum_{r=0}^{m-1}S\left(z+\tfrac{r}{m};s\right)=\sum_{r=0}^{m-1}\sum_{n=-\infty}^{\infty}\hat{\phi}_{y,s}(n)e^{2\pi in(x+r/m)}=\sum_{n=-\infty}^{\infty}\hat{\phi}_{y,s}(n)e^{2\pi inx}\sum_{r=0}^{m-1}e^{2\pi inxr/m}.$$

Ahora,

$$\sum_{r=0}^{m-1}(e^{2\pi in/m})^r=\begin{cases}m & m\mid n\\ 0 & m\nmid n\end{cases},$$

donde el caso $m\nmid n$ se verifica porque estamos sumando varias veces todas las raices $m'-$ésimas de la unidad que da cero, donde $m'=m/(n,m)$. Entonces tenemos que

$$\sum_{r=0}^{m-1}S\left(z+\tfrac{r}{m};s\right)=m\sum_{n\in m\mathbb{Z}}\hat{\phi}_{y,s}(n)e^{2\pi inx}.$$

Sustituimos la expresión anterior en la fórmula (1.25) de $E_{1,\chi}(z,s)$:

$$\begin{aligned}E_{1,\chi}(z,s)&=2\sum_{m=1}^{\infty}\chi(m)m^{-1-2s}\sum_{r=0}^{m-1}S\left(z+\tfrac{r}{m};s\right)\\&=2\sum_{m=1}^{\infty}\sum_{n\in m\mathbb{Z}}\chi(m)m^{-2s}\hat{\phi}_{y,s}(n)e^{2\pi inx}\\&=2\sum_{n\in\mathbb{Z}}\Big(\sum_{\substack{m\mid n\\ m>0}}\chi(m)m^{-2s}\Big)\hat{\phi}_{y,s}(n)e^{2\pi inx}\qquad z\in\mathbb{H},\ \Re(s)>\tfrac{1}{2}.\end{aligned}\tag{1.36}$$

Ahora, si $s\in\mathbb{C}$ es tal que $\Re(s)>-\frac{1}{2}$ o equivalentemente $-2\Re(s)<1$, tenemos que $m^{-2\Re(s)}<m$ y así

$$\Big|\sum_{\substack{m\mid n\\ m>0}}\chi(m)m^{-2s}\Big|\leq\sum_{m\mid n}|\chi(m)|m^{-2\Re(s)}<\sum_{m\mid n}m<n^2,\qquad\Re(s)>-\tfrac{1}{2}.$$

De esto es claro que la serie del lado derecho de (1.36) converge absolutamente y uniformemente sobre cualquier subconjunto compacto Q de $\mathbb{H}\times\{\Re(s)>-\frac{1}{2}\}$. En efecto las fórmulas (1.31) y (1.32) nos dan una cota uniforme de $\hat{\phi}_{y,s}(n)$ para $(z,s)\in Q$ que decae exponencialmente en n (observe que $y^{\Re(s)}$ es una función continua de y y así está acotado para toda $(z,s)\in Q$).

Por lo tanto el lado derecho de (1.36), como función de (z,s) define una función holomorfa sobre $\mathbb{H}\times\{\Re(s)>-\frac{1}{2}\}$. Como la igualdad (1.36) es sobre el abierto $\mathbb{H}\times\{\Re(s)>\frac{1}{2}\}$, esta igualdad define una extensión holomorfa de $E_{1,\chi}(z,s)$ a $\mathbb{H}\times\{\Re(s)>-\frac{1}{2}\}$.

En la fórmula (1.36) ponemos $s=0$ y usamos la proposición 40 inciso iii) para calcular:

$$\begin{aligned}E_{1,\chi}(z,0)&=2\sum_{n\in\mathbb{Z}}\Big(\sum_{\substack{m|n\\m>0}}\chi(m)\Big)\hat{\phi}_{y,0}(n)e^{2\pi inx}\\&=4\pi i\sum_{n=-\infty}^{0}\Big(\sum_{\substack{m|n\\m>0}}\chi(m)\Big)e^{2\pi ny}e^{2\pi inx}\\&=4\pi i\sum_{n=0}^{\infty}\Big(\sum_{\substack{m|n\\m>0}}\chi(m)\Big)e^{-2\pi inz}.\end{aligned}$$

□

1.2 Curvas Algebraicas

1.2.1 Variedades Afines

En esta sección revisamos las herramientas de geometría algebraica. Repasamos las definiciones básicas de variedades y sus morfismos. Después nos enfocamos en curvas para enunciar sus propiedades que usaremos en esta tesis. Luego estudiamos dos casos particulares: curvas elítpicas sobre $\mathbb{C}$ y las curvas modulares $X_0(N)$. En esta sección fijamos un campo K que sea algebraicamente cerrado, e.g. $K=\mathbb{C}$ ó $K=\overline{\mathbb{Q}}$.

Fijamos la siguiente notación: para $n>0$ y K algebraicamente cerrado,

- $\mathbb{A}^n_K:=\{(a_1,\ldots,a_n)\mid a_i\in K\}=K^n$ es el espacio afín con la topología de Zariski. A los puntos de $\mathbb{A}^n_K$ los denotamos por $a=(a_1,\ldots,a_n)$.
- $K[x]:=K[x_1,\ldots,x_n]$ el anillo de polinomios en n variables con coeficientes en K. Si aparecen varios valores de n a la vez, usaremos la notación completa.
- $\mathcal{F}(X,K):=\{f:X\to K\}$ el anillo[12] de funciones de X a K. En particular vamos a estudiar $\mathcal{F}(\mathbb{A}^n_K,K)$ y sus subanillos.

Nota. La topología de Zariski está definido por la siguiente base de cerrados: para todo ideal $I\subseteq K[x]$ define

$$\mathbb{V}_K(I):=\{a\in\mathbb{A}^n_K\mid f(a)=0\ \ \forall f\in I\}.$$

[12]Las operaciones de $\mathcal{F}(\mathbb{A}^n_K,K)$ son las inducidas por las operaciones de K, i.e. $(f+g)(a):=f(a)+g(a)$ y $(fg)(a):=f(a)g(a)$ donde $x=(a_1,\ldots,a_n)$

Es decir, la topología de Zariski está definida por la base $\{\mathbb{A}^n_K - \mathbb{V}_K(I)\}_I$. La asignación $I \mapsto \mathbb{V}_K(I)$ nos da un mapeo de los ideales de $K[x]$ a los conjuntos cerrados de $\mathbb{A}^n_K$. Existe una operación (casi) inversa: para todo subconjunto $X \subseteq \mathbb{A}^n_K$ cerrado define

$$\mathbb{I}_K(X) := \{f \in K[x] \mid f(a) = 0 \ \ \forall a \in X\}.$$

Por el Nullstellensatz de Hillbert[13], tenemos que $\mathbb{I}_K(\mathbb{V}_K(I)) = \sqrt{I}$ donde $\sqrt{I} := \{f \in K[x] \mid f^m \in I,\ m \gg 0\}$ es el radical del ideal $I \subseteq K[x]$. Conversamente, consideraciones estrictamente topológicas nos dan $\mathbb{V}_K(\mathbb{I}_K(X)) = \overline{X}$, la cerradura topológica de X en $\mathbb{A}^n_K$. Esto nos da una biyección entre los ideales radicales de $K[x]$ (i.e. ideales I tales que $\sqrt{I} = I$) y los conjuntos cerrados de $\mathbb{A}^n_K$. Véase §1, capítulo 1 de [Hartshorne, 1977] para más detalles.

Definición 43. A los conjuntos cerrados $X \subseteq \mathbb{A}^n_K$, de la forma $X = \mathbb{V}_K(I)$ para algún ideal $I \subseteq K[x]$, los llamamos *conjuntos algebráicos afines* sobre K. A cada X le asociamos su *anillo de coordenadas* definido como el cociente

$$K[X] := \frac{K[x]}{\mathbb{I}_K(X)}$$

que es una $K-$álgebra finitamente generada por el teorema de la base de Hilbert.[14] Si además I es primo, decimos que X es una *variedad afín* sobre K y en este caso $K[X]$ es un dominio entero. Extendemos la definición de variedad a cualquier subconjunto abierto $Y \subseteq X$ definiendo $\mathbb{I}_K(Y) := \mathbb{I}_K(X)$ y $K[Y] := K[X]$.

Nota. En términos de la topología de Zariski, ser variedad afín es equivalente a ser un conjunto irreducible, es decir: Un subconjunto Y de un espacio topológico X es *irreducible* si no existen subconjuntos propios $Y_1, Y_2 \subsetneq Y$, cerrados en la topología de subespacio de Y, tales que $Y = Y_1 \cup Y_2$. Véase por ejemplo el corolario 1.4 del capítulo I de [Hartshorne, 1977]).

La asignación $X \mapsto K[X]$ le asocia una $K-$álgebra entera finitamente generada a cada variedad afín. Como en el caso de $\mathbb{V}_K(I)$, también hay un inverso a esta construcción. Si A es cualquier $K-$álgebra entera finitamente generada determina una variedad afín sobre K con anillo de coordenadas A. En efecto, existe un homomorfismo sobreyectivo $K[x] \to A$ y así $A \cong K[x]/I$ donde I es primo porque A es dominio, en particular I es radical y así $\mathbb{I}_K(\mathbb{V}_K(I)) = \sqrt{I} = I$. Por lo tanto se definimos $X = \mathbb{V}_K(I)$, obtenemos una variedad afín con anillo de coordenadas

$$K[X] = \frac{K[x]}{\mathbb{I}_K(X)} = \frac{K[x]}{I} = A.$$

Por lo tanto podemos pensar a $K[X]$ como una realización algebraica de la variedad X.

Podemos interpretar a $K[X]$ como funciones de X en K, i.e. como un subanillo de $\mathcal{F}(X, K)$. Para precisar esto primero vemos el caso $X = \mathbb{A}^n_K$. El anillo de polinomios $K[x]$ se puede identificar con el subanillo de $\mathcal{F}(\mathbb{A}^n_K, K)$ definido por

$$\left\{a \mapsto f(a) \middle| f \in K[x]\right\} \subset \mathcal{F}(\mathbb{A}^n_K, K). \tag{1.37}$$

[13]La versión del Nullstellensatz que estamos usando es: sea I un ideal de $K[x]$ con K algebraicamente cerrado, entonces si $f \in K[x]$ es tal que $f(a) = 0$ para toda $a \in \mathbb{V}_K(I)$, entonces existe un natural $r > 0$ tal que $f^r \in I$. Véase por ejemplo el capítulo IX, §1 de [Lang, 2005] o el teorema 25 de §14 de [Matsumura, 1970] para otra formulación.

[14]Simplemente dice, en lenguaje moderno, que si A es un anillo noetheriano, entonces $A[x]$ es noetheriano. Con inducción sobre n se prueba que $A[x_1, \ldots, x_n]$ es noetheriano. Por lo tanto todo cociente es noetheriano, en particular $K[X]$ para algún conjunto algebraico afín $X \subseteq \mathbb{A}^n_K$

Esto es posible porque cuando K es infinito (e.g. cuando K es algebraicamente cerrado), entonces la función $a \mapsto f(a)$ es la función $a \mapsto 0$ si y solo si $f = 0$. A las funciones en (1.37) se les llaman *funciones polinomiales* y lo denotamos por $K[\mathbb{A}^n_K]$. También es costumbre identificar a K con el subanillo de funciones constantes en $\mathcal{F}(\mathbb{A}^n_K, K)$. Similarmente con las funciones polinomiales, el anillo de coordenadas $K[X]$ de un conjunto algebraico afín $X \subseteq \mathbb{A}^n_K$ se puede identificar con un subanillo $\mathcal{F}(X, K)$. En efecto, $f, g \in K[x]$ determinan la misma función en $\mathcal{F}(X, K)$ si y solo si para todo $a \in X$ tenemos que $(f - g)(a) = f(a) - g(a) = 0$, i.e. que $f - g \in \mathbb{I}_K(X)$. Por lo tanto podemos identificar $K[X] = K[x]/\mathbb{I}_K(X)$ con el subanillo de funciones polinomiales en $\mathcal{F}(X, K)$, es decir que son restricción de funciones en $K[\mathbb{A}^n_K]$.

El anillo de coordenadas de un conjunto algebraico afín también se usa para definir *dimensión* de X: es el número natural definido por la dimensión de Krull de $K[X]$, i.e.

$$\dim_{\text{Krull}} K[X] := \sup\{N \in \mathbb{N} \mid \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_N \text{ es una cadena de ideales primos}\}.$$

En el caso particular de dimensión 1, $X \subseteq \mathbb{A}^n(K)$ es de dimensión 1 si y solo si $X = \mathbb{V}(f)$ donde $f \in K[x]$ irreducible no constante (véase la proposición 1.13 de §I.1 en [Hartshorne, 1977] para una prueba).

Ahora estudiamos una generalización de funciones polinomiales.

Definición 44. Sea X una variedad sobre K y $a \in X$. Decimos que la función $f \in \mathcal{F}(X, K)$ es *regular* en a si existe una vecindad abierta $U \subseteq X$ de a y polinomios $g, h \in K[x]$ tales que

$$f(a') = \frac{g(a')}{h(a')}, \quad h(a') \neq 0 \qquad \forall a' \in U.$$

Si f es regular en todos los puntos de un abierto $V \subseteq X$ (e.g. $V = X$), decimos que f es regular sobre V. Al conjunto de funciones racionales regulares sobre V lo denotamos $\mathcal{O}(V)$.

Nota. En palabras, f es regular en a si localmente está bien definida como cociente de polinomios. Observa que la expresión $f = g/h$ no es única al menos de que $K[X]$ sea un dominio de factorización única, donde toda expresión se puede llevar a una expresión única al imponer la condición de que g y h sean primos relativos. Además, si f es regular entonces es continua si le transferimos la topología de Zariski de $\mathbb{A}^1(K)$ a K. (cf. lema 3.1 del capítulo I de [Hartshorne, 1977]). Esto nos va a ayudar para definir morfismos entre variedades.

Como el valor de una función regular en un punto $a \in X$ solamente depende de la información local alrededor de a, podemos estudiar los gérmenes de funciones regulares alrededor de a. Más precisamente, consideremos las parejas (U, f) donde f es regular sobre $U \subseteq X$, una vecindad abierta de a. A este conjunto de parejas lo denotamos:

$$\text{Reg}_{a,X} := \{(U, f) \mid a \in U \text{ es abierto}, f \in \mathcal{F}(X, K) \text{ es regular sobre } U\}.$$

Esto no es notación estándar.

Decimos que dos parejas (U, f) y (V, g) son equivalentes si $f|_{U\cap V} = g|_{U\cap V}$.[15]

[15]El hecho que esto es efectivamente una relación de equivalencia se sigue de las siguientes dos observaciones: las funciones regulares son continuas y todo subconjunto abierto de X es denso (gracias a que X es irreducible como espacio topológico). En efecto si dos funciones regulares f y g coinciden en un abierto U, entonces son iguales porque el conjunto donde coinciden $W = \{a' \in X \mid f(a') - g(a') = 0\}$ es cerrado y contiene a U, un abierto denso, por lo tanto $W = X$ o equivalentemente $f = g$.

Definición 45. Con la notación anterior, una clase de equivalencia $[U, f]$ en $\text{Reg}_{a,X}$ se llama un *gérmen* de funciones regulares alrededor de a. Al anillo de gérmenes de funciones regulares alrededor de a lo denotamos por $\mathcal{O}_{a,X}$ y se llama *el anillo local* de a en X.

Nota. Observe que $\mathcal{O}_{a,X}$ es un anillo local con ideal maximal $\mathfrak{m}_{a,X} = \{[U, f] \mid f(a) = 0\}$. Claramente $\mathfrak{m}_{a,X}$ es un ideal. Para ver que es local, solamente debemos probar que cualquier elemento afuera de $\mathfrak{m}_{a,X}$ es una unidad.[16]. Sea $[U, f] \in \mathcal{O}_{a,X}$ tal que $f(a) \neq 0$. Como f es regular en a, es localmente un cociente de polinomios, es decir existe una vecindad U' de a tal que $f(a') = g(a')/h(a')$ para todo $a' \in U'$. Además, como $f(a) \neq 0$ implica que $g(a) \neq 0$, existe otra vecindad U'' de a tal que $g(a'') \neq 0$ para toda $a'' \in U''$. Esto quiere decir que el cociente $1/f = h/g$ está bien definido sobre la vecindad $U' \cap U''$ de a. Por lo tanto $[U' \cap U'', 1/f] \in \mathcal{O}_{X,a}$ y es el inverso de $[U, f]$.

Ahora quitamos nuestra restricción a un punto a y consideramos parejas (U, f_U) donde $U \subseteq X$ es un abierto arbitrario y $f_U : U \to K$ es regular. Similarmente al caso anterior, a este conjunto lo denotamos por Reg_X. Decimos que dos parejas $(U, f_U), (V, f_V) \in \text{Reg}_X$ son equivalentes si $f_U|_{U\cap V} = f_V|_{U\cap V}$. De esta manera:

Definición 46. Sea X una variedad sobre K, al conjunto de clases de equivalencia, definidas en el párrafo anterior, lo denotamos por $K(X)$ y lo llamamos el *campo de funciones de* X. Sus elementos se llaman *funciones racionales* de X y los denotamos por $f = [U, f_U]$, en este caso decimos que la pareja (U, f_U) representa a la función racional.

Nota. $K(X)$ es un campo gracias al mismo argumento que usamos para probar que $\mathcal{O}_{a,X}$ es un anillo local. Observa que para cada $a \in X$ tenemos contenciones naturales

$$K \hookrightarrow \mathcal{O}(X) \hookrightarrow \mathcal{O}_{a,X} \hookrightarrow K(X)$$

definidos por $f \mapsto [U, f] \mapsto [U, f]$ donde U es una vecindad de a. Por lo tanto $K(X)$ es una $K-$álgebra.

El siguiente teorema, que tomamos de [Hartshorne, 1977], relaciona la manera intrínseca de definir $\mathcal{O}(X), \mathcal{O}_{a,X}$ y $K(X)$ con el anillo de coordenadas de X que depende de las ecuaciones que lo definen:

Teorema 47. *Sea $X \subseteq \mathbb{A}^n_K$ una variedad algebraica afín. Entonces:*

(i) $K[X] \cong \mathcal{O}(X)$.

(ii) $K(X) \cong \text{Frac}(K[X])$, *el campo de cocientes de* $K[X]$.

(iii) La función

$$a \mapsto \mathfrak{m}_a := \{f \in K[X] \mid f(P) = 0\}$$

es una biyección entre los puntos de X y los ideales maximales de $K[X]$.

(iv) Para todo $a \in X$, tenemos que $\mathcal{O}_{a,X} \cong K[X]_{\mathfrak{m}_a}$, la localización de $K[X]$ con respecto del ideal maximal $\mathfrak{m}_a$.

(v) $\dim_{\text{Krull}} \mathcal{O}_{a,X} = \dim_{\text{Krull}} K[X] = \dim X$.

[16] Aquí estamos usando la equivalencia entre anillos locales y anillos tales que sus elementos no invertibles forman un ideal (necesariamente maximal). Véase la proposición 1.6 de [Atiyah and Macdonald, 1994].

Nota. Por (ii), tenemos que $K(X)$ es una extensión finitamente generada de K de grado de trascendencia $\dim X$ ya que este número coincide con el grado de trascendencia de $\mathrm{Frac}(K[X])$ sobre K [Matsumura, 1970, §14].

El teorema anterior nos permite adaptar la definición usual de suavidad en cálculo para variedades algebraicas sobre K de manera intrínseca, es decir que no depende de las ecuaciones que definen a la variedad. Recuerde que cada punto $a \in X$ tiene asociado un anillo local noetheriano $\mathcal{O} = \mathcal{O}_{a,X}$ con ideal maximal $\mathfrak{m} = \mathfrak{m}_{a,X}$. El campo residual $k = \mathcal{O}_{a,X}/\mathfrak{m}_{a,X}$ actúa sobre $\mathfrak{m}/\mathfrak{m}^2$ por multiplicación escalar, i.e. $\mathfrak{m}/\mathfrak{m}^2$ es un $k-$espacio vectorial. Con esto definimos:

Definición 48. Sea X una variedad sobre K y $a \in X$ un punto. Decimos que X es *suave* en a si su anillo local $\mathcal{O}$ es un *anillo local regular*, i.e. $\dim \mathcal{O} = \dim_k \mathfrak{m}/\mathfrak{m}^2$. Decimos que X es *suave* si es suave en todos sus puntos.

Nota. Esta definición de suavidad coincide con la noción clásica de suavidad definida por el Jacobiano. Más precisamente, sea $X \subseteq \mathbb{A}^n_K$ es una variedad afín cuyo ideal es generado por $f_1, \ldots, f_m \in K[x]$. Entonces X es suave en un punto $a \in X$ si el rango de la matriz Jacobiana

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1}(a) & \cdots & \frac{\partial f_1}{\partial x_n}(a) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1}(a) & \cdots & \frac{\partial f_m}{\partial x_n}(a) \end{pmatrix}$$

es igual a $n - \dim X$. Véase el teorema 5.1 del primer capítulo de [Hartshorne, 1977] para una prueba de esto.

Ahora definimos morfismos entre variedades y veremos que los anillos $\mathcal{O}(X)$, $\mathcal{O}_{P,X}$ y $K(X)$ son invariantes asociados a la variedad X.

Definición 49. Sean X y Y variedades sobre K Decimos que una función $\varphi : X \to Y$ es un *morfismo* de variedades sobre K si es continua con respecto de las topologías de Zariski y si para toda $V \subseteq Y$ abierto y para toda $f \in \mathcal{O}(V)$, entonces $f \circ \varphi \in \mathcal{O}(\varphi^{-1}(V))$.

Nota. La composición de morfismos es morfismo entonces, dos variedades X y Y sobre K son isomorfos si existen morfismos $\varphi : X \to Y$ y $\psi : Y \to X$ tales que $\psi \circ \varphi = \mathrm{Id}_X$ y $\varphi \circ \psi = \mathrm{Id}_Y$.

Cada morfismo $\varphi : X \to Y$ determina un morfismo de $K-$álgebras:

$$\varphi^* : K[Y] \longrightarrow K[X] \quad \text{definido por} \quad f \mapsto \varphi \circ f. \tag{1.38}$$

La asignación $\varphi \mapsto \varphi^*$ es una biyección entre el conjunto de morfismos $X \to Y$ y el conjunto de homomorfismos de $K-$álgebras $K[Y] \to K[X]$. En efecto, su inverso se puede construir de la siguiente manera:

Sea $f : K[Y] \to K[X]$ un homomorfismo de $K-$álgebras. Bajo f, las funciones coordenadas $x_i \in K[Y]$ corresponden a $x_i' := f(x_i) \in K[X]$. La función $f_* : X \to Y$ definida por $a = (a_1, \ldots, a_n) \mapsto (x_1'(a), \ldots, x_m'(a))$ es el inverso de $\varphi \mapsto \varphi^*$. Para más detalles, véase la prueba de la proposición 3.5 del capítulo I de [Hartshorne, 1977].

Esta biyección nos sugiere que $X \mapsto K[X]$ es una equivalencia de categorías. Más precisamente, denotamos por $\mathbf{VarAfin_K}$ a la categoría de variedades sobre K con los morfismos sobre K y denotamos por **K-alg**.**fg** a la categoría de $K-$álgebras finitamente generadas sin divisores de cero, junto con homomorfismos de $K-$álgebras. Entonces tenemos:

Teorema 50. *La asignación $X \mapsto K[X]$ junto con $(X \xrightarrow{\varphi} Y) \mapsto (K[Y] \xrightarrow{\varphi^*} K[X])$, es una equivalencia (contravariante) de categorías* $\mathbf{VarAfin_K} \xrightarrow{\sim} \mathbf{K\text{-}alg.fg}$. *En particular, si X y Y son variedades afines, entonces:*

$$X \cong Y \quad \iff \quad K[X] \cong K[Y].$$

Un resultado muy similar se puede probar con $K(X)$ en lugar de $K[X]$, pero requiere otro tipo de morfismo entre variedades cuya construcción es muy similar a la construcción de $K(X)$. Para definirlo sean X y Y variedades sobre K y consideramos parejas (U, φ_U) donde $U \subseteq X$ es un abierto y $\varphi_U : U \to Y$ es un morfismo de variedades sobre K. Análogamente a la construcción de $K(X)$, decimos que $(U, \varphi_U) \sim (V, \varphi_V)$ si y solo si $\varphi_U|_{U\cap V} = \varphi_V|_{U\cap V}$.

Definición 51. Sean X y Y variedades sobre K. Con la notación de arriba, una clase de equivalencia $\varphi = [U, \varphi_U]$ se llama un *mapeo racional* de X a Y y se denota por $\varphi : X \to Y$. Decimos que φ es *dominante* si la imagen de φ_U es densa en Y.[17]

Nota. La composicion de dos mapeos racionales $\varphi : X \to Y$ y $\psi : Y \to Z$ representados por (U, φ_U) y (V, ψ_V) respectivamente se define como el mapeo racional $\psi \circ \varphi : X \to Z$ representado por $(U, \psi_V|_{\varphi_U(U)\cap V} \circ \varphi_U)$. Si φ y ψ son dominantes, entonces $\psi \circ \varphi$ también lo es porque la imagen de $\psi_V|_{\varphi_U(U)\cap V} \circ \varphi_U$ es densa en Z. Por lo tanto podemos considerar a la categoría de variedades sobre K con mapeos racionales dominantes que denotamos por $\mathbf{VarAfin_K^{rac}}$. Si existen mapeos racionales dominantes $\varphi : X \to Y$ y $\psi : Y \to X$ tales que $\psi \circ \varphi = \mathrm{Id}_X$ y $\varphi \circ \psi = \mathrm{Id}_Y$, decimos que X y Y son *birracionalmente equivalentes* y lo denotamos por $X \approx Y$.

Para relacionar esta contrucción con el campo de funciones $K(X)$, tomamos un mapeo racional dominante $\varphi : X \to Y$ representado por (U, φ_U) y vamos a construir un homomorfismo $K(Y) \to K(X)$. Sea $g \in K(Y)$ representado por la pareja (V, g_V) donde $g_V : V \to K$ es regular. Primero observa que como $\varphi_U(U) \subset Y$ es denso, $\varphi_U(U) \cap V$ es no vacío, por lo tanto $\varphi_U^{-1}(V)$ es no vacío y abierto, porque φ_U es continua por ser morfismo. Otra vez por la definición de morfismo, la composición $g_V \circ \varphi_U : \varphi_U^{-1}(V) \to K$ es regular sobre un abierto de X y por lo tanto podemos definir $g \mapsto [\varphi^{-1}(V), g_V \circ \varphi_U] \in K(X)$. Esta función es un morfismo de $K-$álgebras.

Similarmente a la construcción $\varphi \mapsto \varphi^*$ de (1.38), la asignación de un morfismo de $K-$álgebras a un mapeo racional dominante es una biyección entre el conjunto de morfismos de $K-$álgebras $K(Y) \to K(X)$ y el conjunto de mapeos birracionales dominantes $X \to Y$. Por lo tanto la asignación $X \mapsto K(X)$ es un funtor a la categoría de extensiones de K finitamente generadas, que denotamos por $\mathbf{K\text{-}ext, fg}$. De esta manera tenemos un resultado similar al teorema 50:

Teorema 52. *El funtor $X \mapsto K(X)$ es una equivalencia de categorías* $\mathbf{VarAfin_K} \xrightarrow{\sim} \mathbf{K\text{-}ext.fg}$. *En particular dos variedades X y Y son birracionalmente equivalentes si y solo si $K(X)$ y $K(Y)$ son isomorfas como $K-$álgebras, i.e.*

$$X \approx Y \quad \iff \quad K(X) \cong K(Y).$$

Por otro lado, el espacio proyectivo $\mathbb{P}^n(K)$ se define como el espacio cociente de la acción $K^* \curvearrowright \mathbb{A}^n(K) - \{0\}$ que escala, i.e. consiste de clases de equivalencia $[x_0; \cdots ; x_n]$ donde no todas las x_i's son cero y tales que $[x_0; \cdots ; x_n] = [x'_0; \cdots ; x'_n]$ si y solo si existe un escalar $\lambda \in K^*$ tal

[17] Esta definición no depende de la elección de pareja (U, φ_U) para representar a φ ya que si dos morfismos de X a Y coinciden sobre un abierto, son iguales (véase el lema 4.1 del capítulo I de [Hartshorne, 1977]).

que $\lambda x_i = x_i'$ para toda i. Ahora, un polinomio $f \in K[x_0, \ldots, x_n]$ no necesariamente define una función $\mathbb{P}^n(K) \to K$, pero cuando f es *homogéneo*[18], podemos definir bien cuándo f se anula, i.e. $f[x_0, \ldots, x_n] = 0 \iff f(x_0, \ldots, x_n) = 0$.

Por lo tanto decimos que $X \subset \mathbb{P}^n(K)$ es un *conjunto algebraico proyectivo* si existe un *ideal homogéneo* $I \subseteq K[x_0, \ldots, x_n]$, i.e. generado por polinomios homogéneos, tal que X es igual a

$$\mathbb{V}_{\mathbb{P}^n(K)}(I) := \{P \in \mathbb{P}^n(K) \mid f(P) = 0, \ \ \forall f \in K[x_0, \ldots, x_n] \ \text{ homogéneo}\}.$$

Análogamente definimos para X un conjunto proyectivo su ideal asociado

$$\mathbb{I}_{\mathbb{P}^n(K)}(X) := \langle f \in K[x_0, \ldots, x_n] \ \text{ homogéneo} \mid f(P) = 0, \ \ \forall P \in X\rangle.$$

Además decimos que X es una *variedad proyectiva* si $\mathbb{I}_{\mathbb{P}^n(K)}(X)$ es un ideal primo de $K[x_0, \ldots, x_n]$. Similarmente al caso afín, $\mathbb{P}^n(K)$ tiene una topología de Zariski generado por los complementos de los conjuntos $\mathbb{V}_{\mathbb{P}^n(K)}(I)$.

Una ventaja de trabajar en $\mathbb{P}^n(K)$ es que está cubierto por espacios afines $\mathring{A}^n(K)$. Más precisamente consideremos el conjunto algebraico proyectivo $\mathbb{V}_{\mathbb{P}^n(K)}(x_i)$, i.e. el conjunto de puntos $[x_0, \ldots, x_n]$ tales que $x_i = 0$, su complemento $U_i := \mathbb{P}^n(K) - \mathbb{V}_{\mathbb{P}^n(K)}(x_i)$ es un conjunto abierto en la topología de Zariski y además la función

$$\varphi_i : U_i \longrightarrow \mathbb{A}^n(K) \quad \text{definida por} \quad [x_0, \ldots, x_n] \mapsto \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

es un homeomorfismo donde $U_i \subset \mathbb{P}^n(K)$ tiene la topología inducida por la topología de Zariski del espacio proyectivo (cf. la proposición 2.2 de §2 del capítulo I de [Hartshorne, 1977]). Claramente $\{U_i\}_{i=0,\ldots,0}$ es una cubierta abierta de $\mathbb{P}^n(K)$, es decir $\mathbb{P}^n(K) = \cup U_i$, entonces $\{X \cap U_i\}$ es una cubierta de X, donde cada $X \cap U_i$ es homeomorfo a su imagen en $\mathbb{A}^n(K)$ bajo φ_i. Como $X \cap U_i$ es cerrado en U_i, su imagen es cerrado, i.e. es una conjunto algebraico que denotamos $X_i := \varphi_i(X \cap U_i)$. Las parejas $(X \cap U_i, \varphi)$ se llaman cartas afines de la variedad X.

Esto nos permite asociarle variedades afines a una variedad proyectiva. El converso también es cierto, es decir a podemos asociar una variedad proyectiva a cualquier variedad afín. Sea $X \subseteq \mathbb{A}^n(K)$ y toma la cerradura topológica de $\varphi_i^{-1}(X)$ en $\mathbb{P}^n(K)$; a este cerrado lo denotamos por $\overline{X}$ y lo llamamos la *proyectivización* de X. Con esta notación, podemos precisar la relación entre variedades afines y proyectivas con:

Proposición 53. *Para toda variedad proyectiva $X \subseteq \mathbb{P}^n(K)$ los conjuntos algebraicos afines $X_i \neq \emptyset$ son variedades cuya proyectivizaciones son X, i.e. $\overline{X_i} = X$. Por el contrario, para toda variedad afín $X \subset \mathbb{A}^n(K)$ existe una variedad proyectiva $\overline{X} \subseteq \mathbb{P}^n(K)$, tal que $X = (\overline{X})_i$ para alguna i.*

Proof. Esto es la proposición 2.3 y su corolario en §2 del capítulo I de [Hartshorne, 1977]. □

Nota. Los diferentes anillos de coordenadas $K[X_i]$ son isomorfas como $K-$álgebras y en general las diferentes X_i's son birracionalmente equivalentes, entonces módulo equivalencia birracional, podemos denotar $X \cap \mathbb{A}^n(K) := X_i$. La proposición anterior se reescribe como $\overline{X \cap \mathbb{A}^n(K)} = X$ (resp. $\overline{X} \cap \mathbb{A}^n(K) = X$) cuando X es una variedad proyectiva (resp. afín). La asociación $X \mapsto X \cap \mathbb{A}^n(K)$ nos permite definir la dimensión de una variedad proyectiva X como la dimensión

[18] Decimos que un polinomio $f \in K[x_0, \ldots, x_n]$ es homogéneo de grado d si todos sus monomios son de grado d, o equivalentemente $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, f_n)$ para toda $\lambda \in K$.

de $X \cap \mathbb{A}^n(K)$. Hacemos lo mismo con el campo de funciones, es decir definimos el campo de funciones de la variedad proyectiva X como $K(X \cap \mathbb{A}^n(K))$; recuerde que si cambiamos de carta afín obtenemos $K-$álgebras isomorfas.

Ahora, discutimos los morfismos entre variedades proyectivas. Sean $X, X \subseteq \mathbb{P}^n(K)$ variedades proyectivas y $f_0, \ldots, f_n \in K(X)$

1.2.2 El teorema de Riemann-Roch

Teorema 54. *(Riemann-Roch) Sea $\mathcal{C}$ una curva definida sobre cualquier campo y sea K su divisor canónico. Entonces existe un entero g, el género de $\mathcal{C}$ tal que para todo divisor $D \in \mathrm{Div}(\mathcal{C})$ se cumple:*

$$\dim \mathcal{L}(D) - \dim \mathcal{L}(K - D) = \deg D - g + 1.$$

La prueba de Riemann-Roch se puede hacer con el teorema de dualidad de Serre, e.g. en el capítulo IV de [Hartshorne, 1977] o en [Serre, 1959]

Corolario 55. *Con las hipótesis del teorema de Riemann-Roch tenemos:*

(i) $\dim \mathcal{L}(K) = g$.

(ii) $\deg K = 2g - 2$

(iii) $\deg D > 2g - 2 \quad \Longrightarrow \quad \dim \mathcal{L}(D) = \deg D - g + 1$

1.2.3 Curvas modulares

El modelo racional de $X_0(N)$

Teorema 56. *Para toda curva modular $X_0(N)$ existe una única (módulo isomorfismo) curva proyectiva suave sobre $\mathbb{Q}$, que denotamos por $X_0(N)_{\mathbb{Q}}$, y un isomorfismo $\varphi_N : X_0(N) \to X_0(N)_{\mathbb{Q}}(\mathbb{C})$ sobre $\mathbb{C}$ entre los $\mathbb{C}-$puntos tal que el morfismo inducido en campo de funciones, $\varphi_N^* : \mathbb{C}(X_0(N)_{\mathbb{Q}}) \to \mathbb{C}(X_0(N))$, cumple que $\varphi_N^*(\mathbb{Q}(X_0(N)_{\mathbb{Q}})) = \mathbb{Q}(j, j_N)$.*

Espacios moduli

En esta sección vemos como las curvas modulares parametrizan clases de isomorfismos entre curvas elípticas que preservan cierta información de torsión de las curvas elípticas.

El siguiente paso es estudiar la categoría de curvas elípticas con un subgrupo cíclico de orden 15 distinguido. Más precisamente, los objetos son parejas (E', C') donde $E'/\mathbb{C}$ es una curva elíptica con un subgrupo cíclico C' de $E(\overline{\mathbb{Q}})$ de orden $N = 15$. Los isomorfismos de esta categoría son isomorfismos $\varphi : E' \to E''$ tales que $\varphi(C') = C''$ que definen una relación de equivalencia sobre estas parejas que denotamos por $(E', C') \sim (E'', C'')$. Al conjunto de clases de equivalencias lo denotamos $S_0(N) = \{[E', C']\}$. Si queremos restringir las curvas elípticas a curvas sobre algún subcampo K de $\mathbb{C}$, denotamos por $S_0(N)(K)$ al conjunto de clases de equivalencias $[E', C']$ donde E' está definida sobre K, el isomorfismo $E' \to E''$ está definida sobre K y $C' \subset E'(K)$. Observe que $S_0(N)(\mathbb{C}) = S_0(N)$.

Nota. En general, podemos identificar $S_0(N)(K)$ con otro conjunto de clases de equivalencia. En este caso los objetos son isogenias $\varphi : E \to E'$ definidas sobre K con núcleo cíclico de orden N; a éstas se les llaman $N-$*isogenias*. Un isomorfismo entre dos $N-$isogenias $\varphi_1 : E_1 \to E_1'$ y $\varphi_2 : E_2 \to E_2'$ es una pareja de isomorfismos $E_1 \cong E_2$ y $E_1' \cong E_2'$, cada uno definido sobre K, tales que el siguiente diagrama conmuta:

$$\begin{array}{ccc} E_1 & \xrightarrow{\sim} & E_2 \\ {\scriptstyle\varphi_1}\downarrow & & \downarrow{\scriptstyle\varphi_2} \\ E_1' & \xrightarrow{\sim} & E_2' \end{array} \tag{1.39}$$

A la clase de isomorfismo de $N-$isogenias, lo denotamos $[E \xrightarrow{\varphi} E']$. Al conjunto de clases de isomorfismo de isogenias lo denotamos por $\mathrm{Isog}_N(K)$. De esta manera podemos identificar $S_0(N)(K)$ con $\mathrm{Isog}_N(K)$. Para esto consideramos la siguiente función:

$$\Phi_{N,K} : \mathrm{Isog}_N(K) \longrightarrow S_0(N)(K) \quad \text{definido por} \quad [E \xrightarrow{\varphi} E'] \mapsto [E, \ker\varphi] \tag{1.40}$$

La función $\Phi_{N,K}$ es claramente bien definida por la conmutatividad del diagrama (1.39).

Para construir su inverso, recuerde que para todo subgrupo finito C de E, existe una única curva elíptica, denotada por E/C, y una isogenia $E \to E/C$ con núcleo C (cf. teorema 63), i.e. una $N-$isogenia. Además, como E está definida sobre K y $C \subset E(K)$, la curva E/C y la isogenia están definidas sobre K. Esta asignación sugiere que el inverso de $\Phi_{N,K}$ es la función $[E, C] \mapsto [E \to E/C]$. En efecto, la unicidad de la curva E/C garantiza que está bien definida y claramente es el inverso de $\Phi_{N,K}$. Por lo tanto $\Phi_{N,K}$ es una biyección.

Este teorema es nuevo en la sección de curvase elipticas

Ahora hacemos una primera reducción para estudiar $S_0(N)$. Gracias al teorema de uniformización (cf. el teorema 74), para toda curva elíptica $E/\mathbb{C}$ existe un $\tau \in \mathbb{H}$ tal que $E \cong \mathbb{C}/(\tau\mathbb{Z} \oplus \mathbb{Z})$ como grupos de Lie; denotamos $\Lambda_\tau := \tau\mathbb{Z} \oplus \mathbb{Z}$ y $E_\tau := \mathbb{C}/\Lambda_\tau$. Con esta notación tenemos el siguiente lema:

Lema 57. *Todo elemento $[E, C] \in S_0(N)$ es de la forma $[E_\tau, \langle N^{-1} + \Lambda_\tau\rangle]$ para alguna $\tau \in \mathbb{H}$. Además, la función $\Psi_N : S_0(N) \to Y_0(N)$ definido por $[E_\tau, \langle N^{-1} + \Lambda_\tau\rangle] \mapsto \tau\Gamma_0(N) \in Y_0(N)$ es una biyección.*

Proof. Sea $[E, C] \in S_0(N)$ y sea $Q \in C$ un generador, en particular Q es de orden N. Por el teorema de uniformización $E_\tau \cong E$ para alguna τ. Bajo este isomorfismo, Q corresponde a un punto de E_τ que denotamos por

$$Q = z_0 + \Lambda_\tau \qquad (z_0 \in \mathbb{C}).$$

Como Q es de orden N, entonces $Nz_0 \in \Lambda_\tau$ lo cual implica que existen $a, b \in \mathbb{Z}$ tales que $Nz_0 = a\tau + b$. Como $\{1, \tau\}$ es una $\mathbb{R}-$base de $\mathbb{C}$, existen $\lambda, \mu \in \mathbb{R}$ tales que $z_0 = \lambda\tau + \mu$. Si igualamos ambas expresiones de z_0, obtenemos que $N\lambda = a$ y $N\mu = b$ y por lo tanto $\lambda, \mu \in \mathbb{Q}$. De otra manera:

$$Q = \frac{\alpha\tau + \beta}{\gamma} + \Lambda_\tau \qquad (\alpha, \beta, \gamma \in \mathbb{Z}).$$

Otra vez por el orden de Q, multiplicamos la ecuación anterior por N y obtenemos: $N(\alpha\tau+\beta)/\gamma \in \Lambda_\tau$ y así $N\alpha/\gamma, N\beta/\gamma \in \mathbb{Z}$. Sin pérdida de generalidad podemos tomar $(\alpha, \beta, \gamma) = 1$, entonces podemos concluir que $\gamma \mid N$. Por otro lado, si $\gamma < N$ entonces $\gamma Q = \alpha\tau + \beta + \Lambda_\tau = \Lambda_\tau$ lo cual

contradice que Q tiene orden N. Por lo tanto $\gamma = N$ y podemos asumir que existen $c, d \in \mathbb{Z}$ tales que

$$Q = \frac{c\tau + d}{N} + \Lambda_\tau \qquad (c, d, N) = 1.$$

Observe que si $t, t' \in \mathbb{Z}$ entonces la ecuación

$$\frac{(c + tN)\tau + (d + t'N)}{N} + \Lambda_\tau = \frac{c\tau + d}{N} + t\tau + t' + \Lambda_\tau = \frac{c\tau + d}{N} + \Lambda_\tau = Q$$

implica que la elección de c y d depende solamente de sus clases módulo N.

Por las hipótesis sobre c, d y N, existen $a, b, k \in \mathbb{Z}$ tales que $ad - bc + kN = 1$ es decir, si denotamos

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}),$$

entonces bajo la proyección $\pi : M_2(\mathbb{Z}) \twoheadrightarrow M_2(\mathbb{Z}/N\mathbb{Z})$, tenemos que $\pi(\sigma) \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Como la restricción $\pi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ es sobreyectiva, toma

$$\sigma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

tal que $\pi(\sigma') = \pi(\sigma)$. Por construcción, $c \equiv c' \pmod N$ y $d \equiv d' \pmod N$ entonces $Q = (c'\tau + d')/N + \Lambda_\tau$.

Sea $\tau' \in \mathbb{H}$ tal que

$$\tau' = \sigma'\tau = \frac{a'\tau + b'}{c'\tau + d'} \tag{1.41}$$

y denotamos al denominador por $m = c'\tau + d'$. Entonces $m\tau' = (a'\tau + b')$ y así

$$m\Lambda_{\tau'} = m(\tau'\mathbb{Z} \oplus \mathbb{Z}) = m\tau'\mathbb{Z} \oplus m\mathbb{Z} = (a'\tau + b')\mathbb{Z} \oplus (c'\tau + d')\mathbb{Z}. \tag{1.42}$$

Es conocido que dos retículas $\omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ y $\omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$, tales que $\Im(\omega_1/\omega_2), \Im(\omega_1'/\omega_2') > 0$, son iguales si $\omega_1/\omega_2, \omega_1'/\omega_2' \in \mathbb{H}$ están en la misma órbita de la acción $\mathrm{PSL}_2(\mathbb{Z}) \curvearrowright \mathbb{H}$.[19] En este caso tenemos que $(a'\tau + b')\mathbb{Z} \oplus (c'\tau + d')\mathbb{Z} = \tau\mathbb{Z} \oplus \mathbb{Z}$ porque $(a'\tau + b')/(c'\tau + d') = \tau' = \sigma'(\tau)$ y así $\tau/1$ y $(a'\tau' + b')/(c'\tau' + d')$ están en la misma órbita. De (1.42) concluimos que $m\Lambda_{\tau'} = \Lambda_\tau$ y que

$$m\left(\frac{1}{N} + \Lambda_{\tau'}\right) = \frac{c'\tau + d'}{N} + \Lambda_\tau = Q.$$

Por lo tanto el homomorfismo $E_{\tau'} \to E_\tau$ definido por $z + \Lambda_{\tau'} \mapsto mz + \Lambda_\tau$ es un isomorfismo. Si lo componemos con el isomorfismo $E_\tau \cong E$ obtenemos un isomorfismo $f : E_{\tau'} \to E$ donde $f(N^{-1} + \Lambda_{\tau'}) = Q$. De esta manera $f\big(\langle N^{-1} + \Lambda_{\tau'}\rangle\big) = \langle Q\rangle = C$. Concluimos que $[E, C] = [E_{\tau'}, \langle N^{-1} + \Lambda_{\tau'}\rangle]$ para alguna $\tau' \in \mathbb{H}$.

No sé si agregar una parte de retículas a la sección de curvas elípticas para justificar este isomorfismo

Ahora demostramos la segunda parte del lema. Tenemos que probar que la función $\Psi_N : [E_\tau, \langle N^{-1} + \Lambda_\tau\rangle] \mapsto \tau\Gamma_0(N)$ cumple tres cosas:

[19] Más precisamente, si $\mathcal{R}$ es el espacio de retículas, $\mathbb{C}^*$ actúa por homotecias. Entonces $\omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z} \mapsto \omega_1/\omega_2$ es una biyección $\mathcal{R}/\mathbb{C}^* \to \mathbb{H}/\mathrm{PSL}_2(\mathbb{Z})$ (cf. la proposición 3 de §2 del capítulo VII de [Serre, 1973]). En particular tenemos que

$$\omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z} = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z} \quad \iff \quad \omega_1' = a\omega_1 + b\omega_2,\ \ \omega_2' = c\omega_1 + d\omega_2 \quad \text{donde } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

i) Ψ_N está bien definida.

Si $[E_\tau, \langle N^{-1} + \Lambda_\tau\rangle] = [E_{\tau'}, \langle N^{-1} + \Lambda_{\tau'}\rangle]$, entonces $\mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda_{\tau'}$ y por lo tanto existe un $m \in \mathbb{C}^*$ tal que $m\Lambda_\tau = \Lambda_{\tau'}$ y tal que $m\langle N^{-1} + \Lambda_\tau\rangle = \langle N^{-1} + \Lambda_{\tau'}\rangle$ (véase la nota de pie 19). Como $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$, entonces la igualdad $m\Lambda_\tau = m\tau\mathbb{Z} \oplus m\mathbb{Z} = \tau'\mathbb{Z} \oplus \mathbb{Z}$ nos dice que existe un

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

tal que

$$m\tau = a\tau' + b \quad , \quad m = c\tau' + d$$

o en particular $\sigma\tau' = \tau$; esto es otra vez por la nota de pie 19.

Por otro lado sabemos que el isomorfismo $E_\tau \cong E_{\tau'}$ manda $N^{-1} + \Lambda_\tau$ en $\langle N^{-1} + \Lambda_{\tau'}\rangle$, es decir

$$m\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{c\tau' + d}{N} + \Lambda_{\tau'} = \frac{k}{N} + \Lambda_{\tau'} \quad (1 \leq k < N)$$

donde $(k, N) = 1$ porque $k/N + \Lambda_{\tau'}$ es necesariamente de orden N. La ecuación anterior implica que

$$\frac{c}{N}\tau' + \frac{d-k}{N} \in \Lambda_{\tau'} \quad \Longrightarrow \quad N \mid c, \;\; N \mid d - k.$$

En particular $c \equiv 0 \pmod{N}$. Además, si δ fuese un factor común de N y d, entonces $\delta \mid d - k$ implica que $\delta \mid k$ y así $\delta \mid (N, k) = 1$. Por lo tanto $(N, d) = 1$ y así deducimos que $d \equiv 1 \pmod{N}$. Con esto concluimos que $\sigma \in \Gamma_0(N)$. Como $\sigma\tau' = \tau$, tenemos que $\tau\Gamma_0(N) = \tau'\Gamma_0(N)$ cuando $[E_\tau, \langle N^{-1} + \Lambda_\tau\rangle] = [E_{\tau'}, \langle N^{-1} + \Lambda_{\tau'}\rangle]$ y por lo tanto la función $[E_\tau, \langle N^{-1} + \Lambda_\tau\rangle] \mapsto \tau\Gamma_0(N)$ está bien definida.

ii) Ψ_N es inyectiva.

Sean $\tau, \tau' \in \mathbb{H}$ tales que $\tau\Gamma_0(N) = \tau'\Gamma_0(N)$, por ejemplo $\tau' = \sigma'\tau$ donde $\sigma' \in \Gamma_0(N)$ y es de la forma (1.41). De manera análoga a (1.42) y al párrafo que le sigue, concluimos que $m\Lambda_{\tau'} = \Lambda_\tau$, donde $m = c'\tau + d'$, y que

$$m\left(\frac{1}{N} + \Lambda_{\tau'}\right) = \frac{c'\tau + d'}{N} + \Lambda_\tau.$$

De esta manera $E_\tau = \mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda_{\tau'} = E_{\tau'}$ donde el isomorfismo está dado por $z + \Lambda_{\tau'} \mapsto mz + \Lambda_\tau$. Además, como $\sigma' \in \Gamma_0(N)$, entonces $N \mid c'$ y así $c' = Nc$ para alguna $c \in \mathbb{Z}$. Por lo tanto

$$m\left(\frac{1}{N} + \Lambda_{\tau'}\right) = c\tau + \frac{d'}{N} + \Lambda_\tau = \frac{d'}{N} + \Lambda_\tau,$$

donde, como $(N, d') = 1$, $d'/N + \Lambda_\tau$ es un generador del subgrupo cíclico $\langle N^{-1} + \Lambda_\tau\rangle$. Por lo tanto el isomorfismo $z + \Lambda_{\tau'} \mapsto mz + \Lambda_\tau$ manda al subgrupo $\langle \frac{1}{N} + \Lambda_{\tau'}\rangle$ en el subgrupo $\langle N^{-1} + \Lambda_\tau\rangle$. Por lo tanto $[E_\tau, \langle N^{-1} + \Lambda_\tau\rangle] = [E_{\tau'}, \langle N^{-1} + \Lambda_{\tau'}\rangle]$ y Ψ_N es inyectiva.

iii) Ψ_N es sobre.

Esto es claro porque $\tau\Gamma_0(N)$ viene de la curva elíptica E_τ con subgrupo cíclico fijo $\langle N^{-1} + \Lambda_\tau\rangle$, i.e. $\Psi_N[E_\tau, \langle N^{-1} + \Lambda_\tau\rangle] = \tau\Gamma_0(N)$ y Ψ_N es sobre.

□

Nota. Recuerde que $S_0(N)$ se puede identificar con $\mathrm{Isog}_N(\mathbb{C})$, i.e. clases de isomorfismo de isogenias con núcleo cíclico de orden N. Las clases $[E_\tau, \langle N^{-1} + \Lambda_\tau\rangle]$ corresponden a la clase $[E_\tau \xrightarrow{\varphi} E_{N\tau}]$ donde la isogenia φ es multiplicar por N. En efecto, el núcleo de φ consiste de puntos $z + \Lambda_\tau$ tales que $Nz \in \Lambda_{N\tau}$, es decir $Nz = a + bN\tau$ para algunas $a, b \in \mathbb{Z}$. Como $\{1, \tau\}$ es $\mathbb{R}-$base de $\mathbb{C}$, sabemos que existen $\lambda, \mu \in \mathbb{R}$ tales que $z = \lambda + \mu\tau$ y por lo tanto $N\lambda = a$ y $\mu = b$. Esto quiere decir que

$$z + \Lambda_\tau = \left(\frac{a}{N} + b\tau\right) + \Lambda_\tau = \frac{a}{N} + \Lambda_\tau \in \langle N^{-1} + \Lambda_\tau\rangle$$

y por lo tanto $\ker\varphi \subseteq \langle N^{-1} + \Lambda_\tau\rangle$. Como claramente $N^{-1} + \Lambda_\tau \in \ker\varphi$, tenemos la otra contención y podemos concluir que $\ker\varphi = \langle N^{-1} + \Lambda_\tau\rangle$. Todo esto, junto con el lema 57, nos produce la identificación de los tres conjuntos:

$$\begin{array}{ccccc} \mathrm{Isog}_N(\mathbb{C}) & \xleftarrow{\quad\Phi_{N,\mathbb{C}}\quad} & S_0(N) & \xleftarrow{\quad\Psi_N\quad} & Y_0(N) \\ \big[E_\tau \xrightarrow{\cdot N} E_{N\tau}\big] & \longleftrightarrow & \big[E_\tau, \langle N^{-1} + \Lambda_\tau\rangle\big] & \longleftrightarrow & \tau\Gamma_0(N) \end{array}.$$

Ahora, para $K \subseteq \mathbb{C}$, consideremos la función

$$\Delta_{N,K} : S_0(N)(K) \longrightarrow \mathbb{A}^2_K \quad \text{definido por} \quad [E, C] \mapsto \big(j(E), j(E/C)\big),$$

donde E/C es la única curva elíptica asociada a una isogenia de $E \to E/C$ con núcleo C (véase el teorema 63). Observe que $\Delta_{N,K}$ está bien definida porque si $[E, C] = [E', C']$, mediante un isomorfismo $f : E \to E'$, entonces $j(E) = j(E')$.[20] Además la composición $E \xrightarrow{f} E' \longrightarrow E'/C'$ es una isogenia con núcleo C porque $f(C) = C' = \ker(E' \to E'/C)$. Por la unicidad de E/C, necesariamente tenemos que $E/C \cong E'/C'$ y por lo tanto $j(E/C) = j(E'/C')$. Esto prueba que $[E, C] \mapsto (j(E), j(E/C))$ está bien definido.

También podemos probar que $\Delta_{N,K}$ es inyectiva. Supongamos que $[E, C], [E', C'] \in S_0(N)(K)$ tales que

$$\Delta_{N,K}[E, C] = (j(E), j(E/C)) = (j(E'), j(E'/C')) = \Delta_{N,K}[E', C'],$$

es decir, que $j(E) \neq j(E')$ o $j(E/C) \neq j(E'/C')$. Para esto supongamos que $j(E) = j(E')$. Como $K \subseteq \mathbb{C}$, E y E' definen curvas sobre $\mathbb{C}$ que son isomorfas sobre $\mathbb{C}$, i.e. hay un isomorfismo $g : E(\mathbb{C}) \to E'(\mathbb{C})$ definido sobre $\mathbb{C}$. Ahora, la isogenia $E(\mathbb{C}) \xrightarrow{f} E'(\mathbb{C}) \longrightarrow E'(\mathbb{C})/C'$ tiene núcleo C. Por la unicidad de la curva elíptica $E(\mathbb{C})/C$, tenemos que $E(\mathbb{C})/C \cong E'(\mathbb{C})/C'$ sobre $\mathbb{C}$ o equivalentemente $j(E)$

Por contradicción, supongamos que $[E, C] = [E', C']$. Esto significa que $E \cong E'$ y así $j(E) = j(E')$ (véase el pie de página [20])

y por lo tanto $[E, C] \neq [E', C']$. Ahora supongamos que $j(E) = j(E')$, observe que en este caso $j(E/C) \neq j(E/C)$. Si consideramos E y E' sobre $\mathbb{C}$, entonces son isomorfas sobre $\mathbb{C}$; sea $f : E \to E'$

[20] Más precisamente, E y E' tienen ecuaciones de Weierstrass y si $E \cong E'$, entonces sus ecuaciones de Weierstrass difieren en un cambio de variable

$$X = u^2X' + r, \quad Y = u^3Y' + su^2X' + t \qquad u \in K^*,\ r, s, t \in K,$$

que no altera el $j-$invariante de las ecuaciones, es decir $j(E) = j(E')$. Equivalentemente tenemos que $j(E) \neq j(E')$ implica $E \ncong E'$.

un isomorfismo sobre $\mathbb{C}$. Si $f(C) = C'$, entonces el núcleo de la isogenia $E \xrightarrow{f} E' \longrightarrow E'/C'$ es C y tendríamos como antes: $E/C \cong E'/C'$ lo cual contradice $j(E/C) \neq j(E/C)$. Por lo tanto $f(C) \neq C'$ para todo isomorfismo $f : E \to E'$ sobre $\mathbb{C}$, en particular $[E, C] \neq [E', C']$ porque de lo contrario habría un isomorfismo $g : E \to E'$ sobre K que induce un isomorfismo $\mathbb{C}$ que satisface

Con esto en mente consideremos la función:

$$\Delta_{N,K} : \mathrm{Isog}_N(K) \longrightarrow \mathbb{A}^2(K) = K \times K \quad \text{definido por} \quad [E \to E'] \mapsto (j(E), j(E')).$$

La función está bien definida porque si dos isogenias $E_1 \to E_1'$ y $E_2 \to E_2'$ son isomorfas sobre K, entonces hay isomorfismos $E_1 \cong E_2$ y $E_1' \cong E_2'$ definidos sobre K lo cual implica que $j(E_1) = j(E_2) \in K$ y $j(E_1') = j(E_2') \in K$. También es fácil ver que $\Delta_{N,K}$ es inyectivo ya que si $j(E_1) \neq j(E_2)$ entonces las curvas E_1 y E_2 no pueden ser isomorfas sobre K. Por lo tanto si $(j(E_1), j(E_1')) \neq (j(E_2), j(E_2'))$ entonces $[E_1 \to E_1'] \neq [E_2 \to E_2']$ y así $\Delta_{N,K}$ es inyectivo. Lo que nos falta hacer es calcular la imagen de $\Delta_{N,K}$.

Observe que cuando $K = \mathbb{C}$ tenemos que $\Delta_{N,\mathbb{C}}$ actúa como $[E_\tau \to E_{N\tau}] \mapsto (j(E_\tau), j(E_{N\tau}))$. En este caso tenemos que $j(E_{N\tau}) = j(N\tau) = j_N(\tau)$ y por lo tanto $[E_\tau \to E_{N\tau}] \mapsto (j(\tau), j_N(\tau))$. Recuerde que j y j_N satisfacen la ecuación modular, i.e. $F(j, j_N) = 0$ para algún polinomio $F(X, Y) \in \mathbb{Q}[X, Y]$. Más precisamente, como $\mathbb{Q}(j, j_N)$ es de grado de trascendencia 1, j_N es algebraico sobre $\mathbb{Q}(j)$ y F es el polinomio mínimo de j_N sobre $\mathbb{Q}(j)$. Por lo tanto la imagen de $\Delta_{N,\mathbb{C}}$ está contenida en los ceros del polinomio $F(X, Y)$, i.e.

$$\Delta_{N,\mathbb{C}}[E_\tau \to E_{N\tau}] = (j(\tau), j_N(\tau)) \in \{(X, Y) \in \mathbb{C} \times \mathbb{C} \mid F(X, Y) = 0\} = \mathcal{C}(\mathbb{C}),$$

donde $\mathcal{C}$ es la curva sobre $\mathbb{Q}$ definida como los ceros de $F(X, Y)$. Es decir que la imagen de $\Delta_{N,\mathbb{C}}$ está contenida en $\mathcal{C}(\mathbb{C})$. Ahora este argumento implica el caso $K \subset \mathbb{C}$ arbitrario, en efecto, si $[E \to E'] \in \mathrm{Isog}_N(K)$, entonces $j(E), j(E') \in K$ y por lo tanto $\Delta_{N,K}[E \to E'] \in \mathcal{C}(K) \subseteq \mathcal{C}(\mathbb{C})$.

Ahora, cuando $K = \mathbb{Q}$ podemos usar el modelo racional de la curva modular $X_0(N)$ (cf. el teorema 56), que denotamos por $(X_0^{\mathbb{Q}}(N), \varphi_N)$, donde $X_0^{\mathbb{Q}}(N)$ es una curva proyectiva suave sobre $\mathbb{Q}$ y $\varphi_N : X_0(N) \to X_0^{\mathbb{Q}}(N)(\mathbb{C})$ es un isomorfismo sobre $\mathbb{C}$ tal que que el isomorfismo inducido en los campos de funciones $\varphi_N^* : \mathbb{C}(X_0^{\mathbb{Q}}(N)) \to \mathbb{C}(X_0(N)) = \mathbb{C}(j, j_N)$ se restringe a un isomorfismo $\varphi_N^* : \mathbb{Q}(X_0^{\mathbb{Q}}(N)) \to \mathbb{Q}(j, j_N)$. Los puntos afines de $X_0^{\mathbb{Q}}(N)$ son los ceros del polinomio mínimo de j_N sobre $\mathbb{Q}(j)$, visto como polinomio en $\mathbb{Q}[X, Y]$, i.e. $X_0^{\mathbb{Q}}(N)(K) = \mathcal{C}(K)$.

Además, $Y_0(N)$ también tiene un modelo racional $(Y_0^{\mathbb{Q}}(N), \varphi_N)$ y se obtiene del modelo de $X_0(N)$ quitándole una cantidad finita de puntos que corresponden a las cúspides de $X_0(N)$. Más precisamente, si $\pi_N : X_0(N) \to X_0(1)$ es la proyección natural inducida por la función $\tau\Gamma_0(N) \mapsto \tau\mathrm{SL}_2(\mathbb{Z})$, obtenemos un morfismo $\pi_{N,\mathbb{Q}}$ entre los modelos $X_0^{\mathbb{Q}}(N)$ y $X_0^{\mathbb{Q}}(1)$ al completar el siguiente diagrama:

$$\begin{array}{ccc} X_0(N) & \xrightarrow{\varphi_N} & X_0^{\mathbb{Q}}(N)(\mathbb{C}) \\ \downarrow{\scriptstyle \pi_N} & & \vdots{\scriptstyle \pi_{N,\mathbb{Q}}} \\ X_0(1) & \xrightarrow{\varphi_1} & X_0^{\mathbb{Q}}(1)(\mathbb{C}) \end{array} .$$

El $j-$invariante induce un isomorfismo $j : X_0(1) \to \mathbb{P}^1(\mathbb{C})$ donde la cúspide $\infty\mathrm{SL}_2(\mathbb{Z}) \in X_0(1)$ es el único punto tal que $j(\infty\mathrm{SL}_2(\mathbb{Z})) = \infty = [1, 0] \in \mathbb{P}^1(\mathbb{Q})$. Bajo la proyección natural $\pi_N : X_0(N) \to X_0(1)$, las cúspides de $X_0(N)$ corresponden a la única cúspide de $X_0(1)$. Estos dos hechos implican

que la imagen inversa de ∞ bajo $j \circ \pi_N$ es el conjunto de cúspides de $X_0(N)$, i.e.

$$\pi_N^{-1}(\infty \mathrm{SL}_2(\mathbb{Z})) = \pi_N^{-1}(j^{-1}(\infty)) = \{\tau\Gamma_0(N) \in X_0(N) \mid \tau \mathrm{SL}_2(\mathbb{Z}) = \infty \mathrm{SL}_2(\mathbb{Z})\}$$
$$\therefore \quad \pi_N^{-1}(\infty \mathrm{SL}_2(\mathbb{Z})) = \{\text{cúspides de } X_0(N)\}$$

Por lo tanto definimos las cúspides de $X_0^{\mathbb{Q}}(N)$ como $\varphi_N(\pi_N^{-1}(\infty \mathrm{SL}_2(\mathbb{Z})))$ y definimos $Y_0^{\mathbb{Q}}(N)$ como la variedad cuasialgebraica $X_0^{\mathbb{Q}}(N) - \varphi_N(\pi_N^{-1}(\infty \mathrm{SL}_2(\mathbb{Z})))$. En particular los puntos afines de la curva $Y_0^{\mathbb{Q}}(N)$ satisfacen el mismo polinomio que los puntos afines de $X_0^{\mathbb{Q}}(N)$.

Ahora los puntos racionales de $Y_0^{\mathbb{Q}}(N)$ son los puntos racionales $X_0^{\mathbb{Q}}(N)(\mathbb{Q})$ menos una cantidad finita de puntos racionales correspondientes a las cúspides de $X_0(N)$ (cf. la nota después del teorema 56). Afirmamos que la imagen de $\Delta_{N,\mathbb{Q}}$ es $Y_0^{\mathbb{Q}}(N)(\mathbb{Q})$. Esto lo enunciamos y probamos de manera más precisa como un corolario del lema 57:

agregué una nota en la sección del modela racional de $X_0(N)$

Corolario 58. *La función $\Theta : S_0(N)(\mathbb{Q}) \to Y_0^{\mathbb{Q}}(N)(\mathbb{Q})$ definida por $[E, C] \mapsto (j(E), j(E/C))$ es una biyección, es decir las clases de isomorfismo de curvas elípticas con subgrupo cíclico fijo de orden N están en biyección con los puntos racionales de $X_0(N)$ no cuspidales.*

Proof. Primero descomponemos a Θ como la composición del inverso de $\Phi_{N,K}$ (cf. (1.40)) con $\Delta_{N,\mathbb{Q}}$, i.e.

$$\begin{array}{ccccc} \Theta & S_0(N)(\mathbb{Q}) & \xrightarrow{\Phi_{N,\mathbb{Q}}^{-1}} & \mathrm{Isog}_N(\mathbb{Q}) & \xrightarrow{\Delta_{N,\mathbb{Q}}} & X_0^{\mathbb{Q}}(N)(\mathbb{Q}) \\ & [E, C] & \longmapsto & [E, E/C] & \longmapsto & (j(E), j(E/C)) \end{array}.$$

Solamente nos falta probar que la imagen de $\Delta_{N,\mathbb{Q}}$ es $Y_0^{\mathbb{Q}}(N)(\mathbb{Q})$.

Supongamos que $[E \to E'] \in \mathrm{Isog}_N(\mathbb{Q})$ es tal que $\Delta_{N,\mathbb{Q}}[E \to E'] = (j(E), j(E')) \in \varphi_N(\pi_N^{-1}(\infty \mathrm{SL}_2(\mathbb{Z})))$. Entonces

$$\varphi_N^{-1}(j(E), j(E')) \in \pi_N^{-1}(\infty \mathrm{SL}_2(\mathbb{Z}))$$

□

1.3 Curvas elípticas

En esta sección repasamos algunas definiciones y resultados que vamos a requerir acerca de las curvas elítpicas. No demostramos todas las propiedades para mantener esta sección breve, pero habrá referencias para las pruebas omitidas.

1.3.1 Definiciones preliminares

Definición 59. Una *curva elíptica* $E = (E, O)$ es una curva proyectiva suave de género 1 con un punto distinguido $O \in E$. Decimos que E *está definido sobre* un campo K, si E está definido sobre K como variedad proyectiva; esto lo denotamos por E/K. Una función no constante $\varphi : E \to E'$ entre curvas elípticas sobre K es una *isogenia* si φ es un morfismo de variedades sobre K tal que $\varphi(O) = O'$.

A cada curva elíptica se le puede asociar una ecuación de la forma

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

donde, si E está definido sobre K, $a_i \in K$. De hecho, la homogenización de esta ecuación es el polinomio que define la imagen de E bajo un encaje $E \hookrightarrow \mathbb{P}^2(K)$,[21] es decir E se puede encajar como una curva cúbica suave en $\mathbb{P}^2(K)$ con ecuación

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3. \tag{1.43}$$

Más precisamente tenemos el siguiente teorema: este teorema es nuevo

Teorema 60. *Sea (E, O) una curva elíptica sobre K y sea $K(E)$ su campo de funciones de E. Entonces existen $x, y \in K(E)$ tales que x (resp. y) tiene un polo de orden 2 (resp. 3) en 0 y tales que $K(E) = K(x, y)$ y tal que la función racional*

$$\varphi : E(\overline{K}) \to \mathbb{P}^2(\overline{K}) \quad \text{definido por} \quad \varphi(P) = [x(P), y(P), 1]$$

induce un isomorfismo de E a la curva $\mathcal{C}$ sobre K, definida por una ecuación de Weierstrass

$$y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{1.44}$$

donde $a_i \in K$ y $\varphi(O) = [0, 1, 0]$.

Además, cualesquiera dos ecuaciones de Weierstrass que definen una curva elíptica, están relacionadas por el un cambio de variable de la forma:

$$X = u^2X' + r, \quad Y = u^3Y' + su^2X' + t,$$

donde $u \in K^*$ y $r, s, t \in K$.

Proof. Solamente comentamos sobre la primera parte de la prueba, que es una aplicación estándar del teorema de Riemann-Roch, y nos referimos a la fuente original [Silverman, 2009, III.3.1] para la prueba completa del teorema.

Consideramos los divisores de E de la forma nO que tienen grado $n > 0$. Como E es de género 1, el teorema de Riemann-Roch nos dice que $\dim \mathcal{L}(nO) = n$. De esta manera $\dim \mathcal{L}(2O) = 2$ y como la función constante $1 \in \mathcal{L}(2O)$, podemos encontrar un $x\mathcal{L}(2O)$ tal que $\{1, x\}$ es una $K-$base de $\mathcal{L}(2O)$; observe que x necesariamente tiene un polo de orden 2 en O porque si el polo fuera de orden 1, $\{1, x\}$ no genera a $\mathcal{L}(2O)$. Por otro lado podemos extender el conjunto linealmente independiente $\{1, x\} \in \mathcal{L}(3O)$ a una base $\{1, x, y\}$; similarmente y tiene un polo de orden 3 en O.

Por último, $\{1, x, y, x^2, xy, y^2, x^3\} \subset \mathcal{L}(6O)$ es un conjunto de 7 elementos en un espacio de dimensión 6 y por lo tanto existe una combinación lineal no trivial

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0, \qquad A_i \in K \text{ no todas } = 0 \tag{1.45}$$

Observe que si $A_6 \neq 0$ entonces A_7x^3 sería el único término de (1.45) con un polo de orden 6, el más alto de los órdenes, por lo tanto la suma del lado izquierdo tendría que ser una función meromorfa con un polo de orden 6, no la constante 0. De manera análoga concluimos que $A_7 \neq 0$.

Después de hacer el cambio de variable

$$x \mapsto -A_6A_7x, \quad y \mapsto A_6A_7^2y \tag{1.46}$$

[21] El espacio proyectivo de dimensión n sobre K se define como el espacio cociente $(K^{n+1} - \{0\})/K^*$ donde la acción $K^* \curvearrowright (K^{n+1} - \{0\})$ es por multiplicación escalar $(\lambda, v) \mapsto \lambda v$.

a (1.45) y cancelar el denominador $A_6^3A_7^4$ de la ecuación que surge, obtenemos la ecuación de Weierstrass:

$$y^2\underbrace{-\frac{A_5}{A_6A_7}}_{a_1}xy\underbrace{-\frac{A_3}{A_6^2A_7^2}}_{a_3}y = x^3\underbrace{-\frac{A_4}{A_6^2A_7^3}}_{a_2}x^2 + \underbrace{\frac{A_2}{A_6^2A_7^3}}_{a_4}x\underbrace{-\frac{A_0}{A_6^2A_7^3}}_{a_6}$$

El siguiente paso es probar que φ es un isomorfismo de curvas sobre su imagen que, por la ecuación anterior, cae dentro de la variedad proyectiva definida por los ceros de (1.44), pero aquí dejamos la exposición y referimos al lector a [Silverman, 2009].

Solamente comentamos que si a priori tenemos funciones $x, y \in K(E)$ con polos de orden 2 y 3 respectivamente y ningún otro polo ni cero, entonces $\{1, x\}$ y $\{1, x, y\}$ son bases de $\mathcal{L}(2O)$ y $\mathcal{L}(3O)$ respectivamente y la prueba procede idénticamente. Por lo tanto si de antemano conocemos a x y a y y satisfacen una relación algebraica de la forma (1.44), entonces esa relación algebraica define una curva elíptica isomorfa a E. Este método lo usaremos en la sección 2.2. □

La ecuación 1.44 asociada a E/K se llama la *ecuación de Weierstrass generalizada* de E. Si la característica de K es distinto de 2 el cambio de variable

$$X' = X, \quad Y' = \frac{1}{2}(Y - a_1X - a_3)$$

transforma la ecuación de Weierstrass a la forma:

$$Y'^2 = 4X'^3 + b_2X'^2 + b_4X' + b_6, \tag{1.47}$$

donde

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

Si además la característica de K es distinto de 3 podemos simplificar la ecuación aun más con el cambio de variable

$$X = \frac{x - 3b_2}{36}, \quad Y = \frac{Y'}{108},$$

que nos da la *ecuación de Weierstrass simplificada* de E:

$$Y^2 = X^3 + Ax + B,$$

donde los coeficientes están definidos por $A = -27c_4$ y $B = -54c_6$ con:

$$c_4 = b_2^2 - 24b_4, \qquad c_6 - b_2^3 + 36b_2b_4 - 216b_6.$$

Definición 61. Sea E una curva elíptica sobre K con una ecuación de Weierstrass simplificada $Y^2 = X^3 + AX + B$ con $A, B \in K$. El *discriminante* (denotado por Δ) y el *j-invariante* (denotado por $j(E)$) de la curva E se definen como:

$$\Delta = -16(4A^3 + 27B^2) \qquad j(E) = -1728\frac{64A^3}{\Delta}.$$

El j-invariante obtiene su nombre gracias al siguiente teorema importante:

Teorema 62. *Sean E y E' curvas elípticas definidas sobre un campo K algebraicamente cerrado. Entonces*

$$E \cong E' \quad \iff \quad j(E) = j(E').$$

(cf. [Silverman, 2009, §3.1, proposición 1.4] o [Hartshorne, 1977, capítulo IV, teorema 4.1] para una prueba usando herramientas de geometría algebraica)

Los puntos de E forman un grupo abeliano (cf. [Silverman, 2009, §3.2]). Para definir la operación geometricamente nos basamos en el celebrado teorema de Bézout[22] que, en nuestro caso, dice que la cantidad de puntos, contando multiplicidad, en la intersección de $E \subset \mathbb{P}^2$ con una recta $L \subset \mathbb{P}^2$ es tres.

Antes de elaborar este argumento, primero consideremos un ecuación de Weierstrass de la forma 1.47 escrita sin tanta notación como:

$$E : Y^2 = 4X^3 + aX^2 + bX + c. \tag{1.48}$$

Si homogenizamos esta ecuación con la variable Z e intersectamos con la recta al infinito definida por $Z = 0$, obtenemos la ecuación $X^3 = 0$ que tiene una única solución $[0, 1, 0] \in \mathbb{P}^2(K)$ de multiplicidad tres. Por el teorema de Bézout, esto quiere decir que la curva E intersecta a la recta al infinito en solamente en $O = [0, 1, 0]$; el punto O va a ser el nuetro de la operación de grupo de E.

Con esto en mente podemos considerar la parte afín de E y agregarle el punto O al infinito. Entonces sean P y Q puntos sobre la curva afín definida por la ecuación 1.48. Sus coordenadas las denotamos por $P = (x(P), y(P))$ y $Q = (x(Q), y(Q))$. Ahora tomamos L la recta en el plano afín que contiene a P y a Q; si $P = Q$ tomamos la recta tangente a $P = Q$. Por el teorema de Bezhout hay un tercer punto de intersección que puede ser O ó un tercer punto R en la curva afín.

Si el tercer punto de intersección es O, definimos $P + Q = O$ o de otra manera $-P := Q$. En este caso la recta L es vertical y por lo tanto

$$x(-P) = x(P), \qquad y(-P) = -y(P), \tag{1.49}$$

que se deduce de la ecuación afín que define a E.

Si el tercer punto de intersección es un punto afín R, definimos $P + Q = -R$ donde $-R$ es el punto construido arriba, i.e. el tercer punto sobre la recta que une R y O. Véase la figura 1.4 para una ilustración de este proceso sobre la curva elíptica definida por $y^2 = x^3 + 17$.

Para calcular las coordenadas de $P+Q$ en téminos de las coordenadas de P y Q, sea $y = \lambda x + \mu$ la ecuación de la recta L. Como pasa por P y Q, su pendiente y su intersección con el eje y son respectivamente:

$$\lambda = \frac{y(Q) - y(P)}{x(Q) - x(P)}, \qquad \mu = y(P) - \lambda x(P) = y(Q) - \lambda x(Q).$$

Si sustituimos $y = \lambda x + \mu$ en la ecuación de Weierstrass (1.48) obtenemos:

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\mu)x + (c - \mu^2).$$

Por otro lado, como P, Q y $P + Q$ están sobre L, las coordenadas $x(P), x(Q)$ y $x(P + Q)$ son raices a la ecuación cúbica anterior. Por lo tanto el polinomio cúbico mónico se factoriza como $(x - x(P))(x - x(Q))(x - x(P + Q))$. Al igualar los coeficientes de ambas expresiones obtenemos el siguiente sistema de ecuaciones:

$$x(P) + x(Q) + x(P + Q) = \lambda^2 - a, \tag{1.50}$$

$$x(P)x(Q) + x(P)x(P + Q) + x(Q)x(P + Q) = b - 2\lambda\mu,$$

$$x(P)x(Q)x(P + Q) = \mu^2 - c, \tag{1.51}$$

[22]Este teorema es famoso y se encuentra en muchos textos sobre curvas, por ejemplo en §5.3 de [Fulton, 2008]

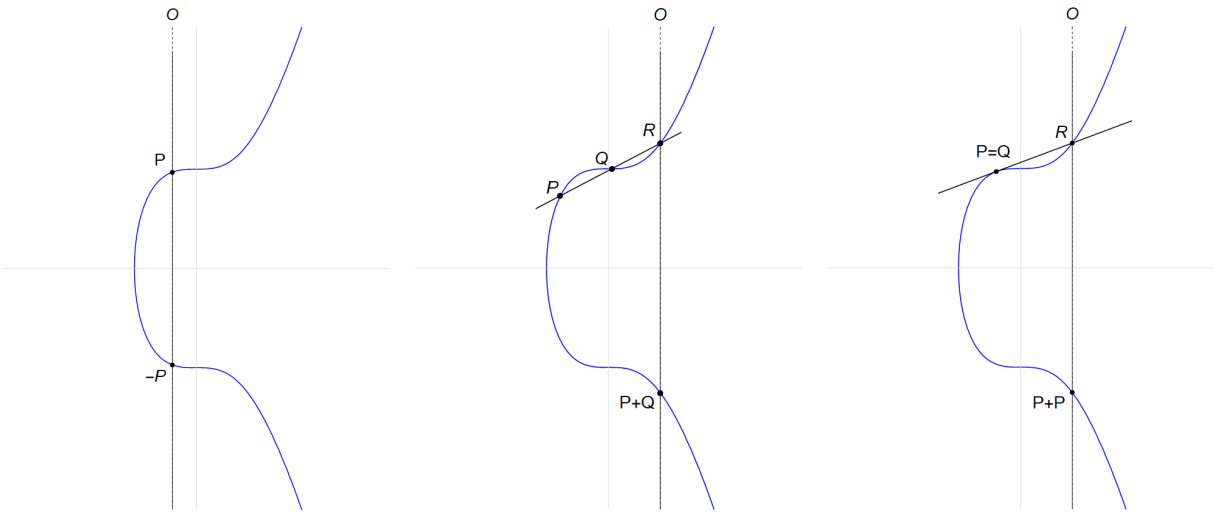


Figure 1.4: Construcción geométrica de la suma de puntos P y Q sobre una curva elíptica según si $P+Q=O$, $P\neq Q$ y $P=Q$ respectivamente.

donde (1.50) nos dice que

$$x(P+Q)=\left(\frac{y(P)-y(Q)}{x(P)-x(Q)}\right)^2-a-x(P)-x(Q)\quad\text{cuando}\quad P\neq Q. \tag{1.52}$$

La fórmula (1.51) la usaremos en la sección 2.2. Cuando $P=Q$, tenemos la fórmula de duplicación:

$$x(2P)=\frac{x^4-2bx^2-8cx+b^2-4ac}{4x^3+4ax^2+4bx+4c}. \tag{1.53}$$

La construcción geométrica de la suma implica inmediatamente que O es el neutro de la operación. Por otro lado, probar que la operación es asociativa y conmutativa es tedioso porque involucra muchas cálculos que no ilustran la teoría. Nos referimos a la sección III.2 de [Silverman, 2009] para las pruebas.

Las isogenias resultan estar estrechamente relacionadas con la estructura de grupo de las curvas elípticas:

Teorema 63. *Sea $\varphi: E\to E'$ una isogenia de curvas elípticas, entonces cumple:*

i) Para todos $P,Q\in E$, tenemos $\varphi(P+Q)=\varphi(P)+\varphi(Q)$, es decir φ es un homomorfismo de grupos.

ii) El núcleo $\ker\varphi$ es un subgrupo finito de E.

iii) Conversamente, para todo subgrupo finito C de E existe una única curva elíptica, denotada por E/C, y una isogenia $\varphi: E\to E/C$ con $\ker\varphi=C$.

Proof. La prueba de las tres partes son III.4.8, III.4.9 y III.4.12 de [Silverman, 2009] respectivamente. Solamente mencionamos un comentario adicional que hace Silverman: si E está definido sobre K y C es $\mathrm{Gal}(\overline{K}/K)-$invariante, entonces E/C y φ se pueden definir sobre K. □

Nota. Hay una manera de definir una ecuación de E/C, en términos de las coordenadas de los puntos de C. En 1971, Jaques Vélu calculó las ecuaciones que definen la curva elíptica E/C. Más precisamente, Vélu definió los generadores del campo de funciones de E/C como:

$$X(P) := x(P) + \sum_{Q \in C - \{O\}} x(P+Q) - x(Q), \qquad Y(P) := y(P) + \sum_{Q \in C - \{O\}} y(P+Q) - y(Q).$$

Véase [Vélu, 1971] para más detalles.

Nota. La existencia de la isogenia dual junto con la existencia de la isogenia $E \to E/C$ del teorema 63, nos implica que el rango del grupo de puntos racionales $E(\mathbb{Q})$ es invariante bajo isogenias:

Sean E y E' curvas elípticas sobre $\mathbb{Q}$, denotamos por $G = E(\mathbb{Q})$ (resp. $G' = E(\mathbb{Q})$) a su grupos de puntos racionales. Si una isogenia $\varphi : G \to G'$ está definida sobre $\mathbb{Q}$, entonces φ se restringe a un homomorfismo de grupos $\varphi : G \to G'$. Por otro lado, el teorema de Mordell-Weil nos dice que G y G' son finitamente generados y (gracias al teorema de estructura de grupoes abelianos finitamente generados):

$$G \cong G_{\text{tor}} \oplus \mathbb{Z}^r, \qquad G' \cong G'_{\text{tor}} \oplus \mathbb{Z}^{r'}$$

donde r (resp. r') es el rango de E (resp. E'). Por el inciso ii), $\ker \varphi$ es finito y así $\ker \varphi \subseteq G_{\text{tor}}$. Por lo tanto φ se factoriza a través de un homomorfismo $\bar{\varphi}$ inyectivo:

$$\begin{array}{ccc} G & \xrightarrow{\quad\varphi\quad} & G' \\ \downarrow & \nearrow_{\bar{\varphi}} & \\ G/G_{\text{tor}} \cong \mathbb{Z}^r & & \end{array}$$

Como G/G_{tor} es libre y $\bar{\varphi}$ es inyectivo, la imagen $\varphi(G/G_{\text{tor}}) \subseteq \mathbb{Z}^{r'} \subseteq G'$ es libre de rango al menos r porque si $\{g_1, \ldots, g_n\}$ es una base de G/G_{tor}, entonces $\{\bar{\varphi}(g_1), \ldots, \bar{\varphi}(g_n)\}$ es linealmente independiente. Por lo tanto $r \leq r'$. Hemos probado que si existe una isogenia $\varphi : E \to E'$ entonces $r \leq r'$. Por lo tanto la existencia de la isogenia dual nos da la otra desigualdad para concluir

$$\exists \varphi : E \longrightarrow E' \quad \text{una isogenia sobre } \mathbb{Q} \quad \Longrightarrow \quad \text{rango de } E \;=\; \text{rango de } E'.$$

Otra manera de definir la suma de E es con divisores:

Definición 64. Un *divisor* D de E es un elemento del grupo libre abeliano generado por los puntos de E, es decir D es una suma formal de la forma:

$$D = \sum_{P \in E} n_p(P)$$

donde $n_P \in \mathbb{Z}$ y $n_P = 0$ para casi toda $P \in E$. Aquí estamos escribiendo (P) como el divisor asociado al punto P (i.e. donde $n_Q = 0$ para toda $Q \neq P$ y $n_P = 1$). Al conjunto de todos los divisores de E lo denotamos $\text{Div}(E)$.

Por ejemplo, si f es una función racional de E, es decir un elemento de $K(E)$ distinto de cero, entonces podemos definir un divisor:

$$\text{div}(f) := \sum_{P \in E} \nu_P(f)(P)$$

donde ν_P es la valoración asociada a $K[E]_P$, la localización de $K[E]$ (el anillo de coordenadas de E) en el ideal maximal $\mathfrak{m}_P = \{f \in K[E] \mid f(P) = 0\}$. Recuerda que como E es suave, $K[E]_P$ es un anillo de valoración discreto.[23] De esta manera, para un $f \in K[E]_P$ la valoración $\nu_P(f)$ se define como el único entero n tal que $f \in \mathfrak{m}_P^n$ pero $f \notin \mathfrak{m}_P^{n+1}$.

Definición 65. Un divisor D de E es *principal* si existe una función racional $f \in K(E)$ distinto de cero tal que $D = \text{div}(f)$. Además hay una relación de equivalencia sobre $\text{Div}(E)$: decimos que D y D' son *linealmente equivalentes*, i.e. $D \sim D'$, si $D - D'$ es un divisor principal. El conjunto de clases de equivalencia es un grupo abeliano, se llama el *grupo de Picard* de E y se denota por $\text{Pic}(E)$.

Observa que el conjunto de divisores principales es un subgrupo de $\text{Div}(E)$ y $\text{Pic}(E)$ es el grupo cociente con el subgrupo de divisores principales. Enunciamos una caracterización de ser divisor principal:

Proposición 66. *Sea E una curva elíptica y $D = \sum n_P(P)$ un divisor de E. Entonces D es principal si y solo si $\sum n_P = 0$ y $\sum [n_p]P = O$ (la segunda suma es en E).*

(cf. [Silverman, 2009, capítulo III, §3, corolario 3.5])

Nota. La función $D \mapsto \sum n_P$ es importante, entonces le damos un nombre:

$$\deg : \text{Div}(E) \to \mathbb{Z} \quad \text{definido por} \quad \deg\left(\sum_{P \in E} n_P(P)\right) = \sum_{P \in E} n_P.$$

Observa que deg es aditiva, i.e. $\deg(D + D') = \deg(D) + \deg(D')$ para todas $D, D' \in \text{Div}(E)$.

Ahora regresamos a la operación algebraica de E. Para $P, Q \in E$ se puede probar que $P + Q$ es el único punto $R \in E$ tal que $(P) + (Q) \sim (R) + (O)$.

Como E es un grupo abeliano, E es un $\mathbb{Z}$-módulo, es decir hay multiplicación por $N \in \mathbb{Z}$. Más precisamente, existen los morfismos de multiplicación:

$$[N] : E \longrightarrow E \quad \text{definido por} \quad [N]P = \underbrace{P + \cdots + P}_{N \text{ veces}} \quad (N > 0).$$

Si $N < 0$ definimos $[N]P := -\big([|N|]P\big)$ y si $N = 0$ definimos $[0]P = O$. La múltiplicación por $N \in \mathbb{Z}$ nos permite estudiar el grupo de torsión de E.

Definición 67. Al subgrupo de elementos de E/K de orden N lo denotamos por:

$$E[N] = \ker[N] = \{P \in E(K) \mid [N]P = O\}.$$

El grupo de torsión de E es simplemente la unión de todas las $E[n]$. De la misma manera, definimos

$$E[N](\overline{K}) = \{P \in E(\overline{K}) \mid [N]P = O\}.$$

[23] Por definición, un punto x en una variedad X es no-singular si el anillo local $\mathcal{O}_{x,X}$ es un anillo *regular* (i.e. el $(\mathcal{O}_{x,X}/\mathfrak{m}_{x,X})$-espacio vectorial $\mathfrak{m}_{x,X}/\mathfrak{m}_{x,X}^2$ es de dimensión $\dim(\mathcal{O}_{x,X})$). Como las curvas elípticas son de dimensión 1, ser regular es equivalente a ser un anillo de valoración discreta (cf. [Atiyah and Macdonald, 1994, §9,proposición 9.2]).

La estructura de $E[N]$ es relativamente sencilla:

Proposición 68. *Sea E una curva elíptica sobre K y sea $c = \mathrm{char}(K)$, entonces:*

$$E[N] \cong \frac{\mathbb{Z}}{N\mathbb{Z}} \times \frac{\mathbb{Z}}{N\mathbb{Z}}$$

si $c = 0$ o si $c \nmid N$ cuando $c > 0$.

Proof. Nada más probamos el caso cuando $K \subseteq \mathbb{C}$. Por el teorema de uniformización (teorema 74), existe una latiz tal que $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ pero este cociente es isomorfo a $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$. Por lo tanto $E[N]$ es un subgrupo de $E[N](\mathbb{C}) = \{P \in E(\mathbb{C}) \mid [N]P = O\}$ que a su vez es un subgrupo (cuyos elementos son de orden N) de $\mathbb{R}/\mathbb{Z}\times\mathbb{R}/\mathbb{Z}$. El único subgrupo que cumple esto es $\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$. □

En particular, si ℓ es un número primo, entonces $[\ell] : E \to E$ se restringe a un morfismo de grupos $[\ell] : E[\ell^{m+1}] \to E[\ell^m]$ para toda $m > 1$. La familia de morfismos

$$\cdots \longrightarrow E[\ell^{m+2}] \xrightarrow{[\ell]} E[\ell^{m+1}] \xrightarrow{[\ell]} E[\ell^m] \xrightarrow{[\ell]} \cdots \xrightarrow{[\ell]} E[\ell]$$

es un sistema inverso. Por lo tanto existe su límite inverso:

Definición 69. Sea E/K una curva elíptica y ℓ un número primo distinto de la característica de K. El *módulo de Tate ℓ-ádico* de E se define como:

$$T_\ell(E) = \varprojlim_m E[\ell^m]$$

Observa que $\mathbb{Z}_\ell$, los enteros ℓ-ádicos, son el límite inverso de los cocientes $\mathbb{Z}/\ell^m\mathbb{Z}$, entonces:

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell \quad (\mathrm{char}(K) \neq \ell).$$

En particular $T_\ell(E)$ es un $\mathbb{Z}_\ell-$módulo libre de rango 2. Si elegimos una $\mathbb{Z}_\ell$-base, entonces todos los $v \in T_\ell(E)$ se pueden expresar como $v = (v_1, v_2) \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Entonces el determinante $\det : T_\ell(E) \times T_\ell(E) \to \mathbb{Z}_\ell$, definido por

$$\det(v, v') := \det \begin{pmatrix} v_1 & v_1' \\ v_2 & v_2' \end{pmatrix} = v_1 v_2' - v_1' v_2$$

es una función bilineal no-degenerada y alternante sobre el módulo de Tate (y es independiente de la elección de la $\mathbb{Z}_\ell-$base). Hay otra función bilineal no-degenerada alternante sobre $T_\ell(E)$ que resulta más útil que el determinante: el emparejamiento de Weil. Para poder definirlo, necesitamos regresar a $E[m]$, construir ahí el emparejamiento de Weil y después pasar al límite inverso.

Sean $P, Q \in E[m]$ (donde posiblemente $P = Q$). Elige $g \in \overline{K}(E)$ tal que:

$$\mathrm{div}(g) = [m]^*(Q) - [m]^*(O)$$

donde

$$[m]^* : \mathrm{Div}(E) \to \mathrm{Div}(E) \quad \text{se define en generadores como} \quad (R) \mapsto \sum_{S \in [m]^{-1}(R)} e_{[m]}(S)(S)$$

donde $e_{[m]}(R)$ es el índice de ramificación de $[m] : E \to E$ en $R \in E$. Con esto definimos el emparejamiento de Weil como:

$$e_m : E[m] \times E[m] \to \mu_m \quad \text{definido por} \quad e_m(P,Q) = \frac{g(X+P)}{g(X)}$$

donde $\mu_m \subset \mathbb{C}$ es el grupo de raices m-ésimas de la unidad y $X \in E$ es un punto elegido de tal manera que g está bien definido en $X+P$ y en X. La función e_m está bien definida y no depende de la elección de g ni de X (cf. [Silverman, 2009, capítulo III, §8]). La función e_m cumple las siguientes propiedades:

Proposición 70. *El emparejamiento de Weil e_m es una función bilineal, alternante, no-degenerada, invariante bajo la acción del grupo de Galois* $\mathrm{Gal}(\overline{K}|K)$ *y cumple:*

$$e_{mm'}(P,Q) = e_m\big([m']P, Q\big) \tag{1.54}$$

cf. [Silverman, 2009, capítulo III, proposición 8.1]).

Ahora fijamos un primo ℓ (distinto de la característica de K). Recuerde que los grupos μ_{ℓ^n}, junto con los morfismos $\mu_{\ell^{n+1}} \to \mu_{\ell^n}$ (definidos por $\zeta \mapsto \zeta^\ell$) forman un sistema inverso: definimos

$$T_\ell(\mu) = \varprojlim_n \mu_{\ell^n}.$$

Para ver que podemos tomar límites inversos de ambos lados de $e_{\ell^n} : E[\ell^n] \times E[\ell^n] \to \mu_{\ell^n}$, debemos probar que el diagrama

$$\begin{array}{ccc} E[\ell^{n+1}] \times E[\ell^{n+1}] & \xrightarrow{[\ell]\times[\ell]} & E[\ell^n] \times E[\ell^n] \\ \Big\downarrow{\scriptstyle e_{\ell^{n+1}}} & & \Big\downarrow{\scriptstyle e_{\ell^n}} \\ \mu_{\ell^{n+1}} & \xrightarrow[\hat{}\ell]{} & \mu_{\ell^n} \end{array}$$

es conmutativo: sean $P, Q \in E[\ell^{n+1}]$, entonces

$$\big(e_{\ell^{n+1}}(P,Q)\big)^\ell = e_{\ell^{n+1}}(P,[\ell]Q) = e_{\ell^n}([\ell]P,[\ell]Q),$$

donde la primera igualdad es por la linealidad en la segunda variable (escrita multiplicativamente) y la segunda igualdad es por la fórmula (1.54); esto prueba la conmutatividad del diagrama anterior.

Por lo tanto e_{ℓ^n} pasa al límite y obtenemos una función:

$$e_\ell : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$$

que hereda las propiedades de las e_{ℓ^n}, es decir e_ℓ es bilineal, no-degenerada, alternante e invariante bajo la acción del grupo de Galois G_K.

La ventaja de usar módulos de Tate y el aparejamiento de Weil, es que podemos calcular los grados de una isogenia. Sea $\varphi : E \to E$ una isogenia. Como φ es además un homomorfismo de grupos, induce un homomorfismo $\varphi_{\ell^n} : E[\ell^n] \to E[\ell^n]$ y pasando al límite inverso obtenemos una función $\mathbb{Z}_\ell$ lineal $\varphi_\ell : T_\ell(E) \to T_\ell(E)$. En general tenemos una función $\mathrm{End}(E) \to \mathrm{End}(T_\ell(E))$. Con esta notación tenemos:

Proposición 71. *Sea $\varphi \in \mathrm{End}(E)$ y $\varphi_\ell \in \mathrm{End}(T_\ell(E))$ el morfismo inducido, entonces*

$$\det \varphi_\ell = \deg \varphi \quad \text{y} \quad \mathrm{tr}\varphi_\ell = 1 + \deg \varphi - \deg(1-\varphi)$$

Proof. cf. [Silverman, 2009, capítulo III, §8, proposición 8.6] □

1.3.2 Curvas elípticas sobre $\mathbb{C}$

En el caso "geométrico" ($K = \mathbb{C}$), las curvas elípticas también se pueden describir usando latices. Un subgrupo aditivo $\Lambda \subset \mathbb{C}$ es una *retícula* si $\Lambda \cong \mathbb{Z}z_1 + \mathbb{Z}z_2$ donde z_1 y z_2 son $\mathbb{R}$-linealmente independiente o equivalentement $\mathrm{Im}\,(z_1/z_2) \neq 0$. El cociente $\mathbb{C}/\Lambda$ es una superficie de Riemann compacta y como es de esperar, el anillo de funciones meromorfas sobre $\mathbb{C}/\Lambda$ nos dice mucho sobre su estructura como variedad. Recuerda que como grupo aditivos:

$$\frac{\mathbb{C}}{\Lambda} \cong \frac{\mathbb{R} \oplus \mathbb{R}}{\mathbb{Z} \oplus \mathbb{Z}} \cong \frac{\mathbb{R}}{\mathbb{Z}} \times \frac{\mathbb{R}}{\mathbb{Z}}$$

Definición 72. Una función meromorfa $f : \mathbb{C} \to \mathbb{C}$ es *elíptica* (con respecto de Λ) si es Λ-periódica, es decir

$$f(z + \lambda) = f(z) \qquad \forall \lambda \in \Lambda$$

Al conjunto de funciones elípticas lo denotamos $\mathbb{C}(\Lambda)$. Observa que una función elíptica define una función meromorfa sobre $\mathbb{C}/\Lambda$

La función elíptica más importante para clasificar curvas elípticas con latices es la función $\wp$ de Weierstrass (asociada a Λ) definida por:

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right).$$

La función $\wp$ de Weierstrass es una función meromorfa cuyos polos (todos de residuo 0) son exactamente de los puntos de la retícula (cf. [Apostol, 1990, §1.6, teorema 1.10] o [Ahlfors, 1979, capítulo 7, §3]). Por lo tanto induce una función meromorfa sobre $\mathbb{C}/\Lambda$.

La importancia de $\wp$ es que, junto con su derivada, genera a todas las funciones elípticas. Más precisamente, si escibimos $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$ como la $\mathbb{C}$-subálgebra de $\mathbb{C}(\Lambda)$ generada por $\wp_\Lambda$ y su derivada $\wp_\Lambda$, entonces tenemos que:

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp_\Lambda, \wp'_\Lambda),$$

(cf. [Silverman, 2009, capítlo VI, teorema 3.2]).

Además $\wp := \wp_\Lambda$ satisface la ecuación diferencial

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3$$

donde $g_2 = g_2(\Lambda)$ y $g_3 = g_3(\Lambda)$ son complejos que dependen de la retícula Λ. Esta ecuación polinomial se parece a la fórmula de Weierstrass simplificada; esto no es una coincidencia:

Teorema 73. *Sea $\Lambda \subset \mathbb{C}$ una retícula y sean $g_2 = g_2(\Lambda)$ y $g_3 = g_3(\Lambda)$ los coeficientes de la ecuación diferencial que cumple $\wp_\Lambda$. Entonces la curva $E/\mathbb{C}$ definida por $y^2 = 4x^3 - g_2x - g3$ es elíptica (i.e. suave) y $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ como variedades complejas bajo la función*

$$z + \Lambda \mapsto [\wp_\Lambda(z), \wp'_\Lambda(z), 1] \in \mathbb{P}^2(\mathbb{C})$$

donde estamos identificando a $E(\mathbb{Q})$ con su encaje en $\mathbb{P}^2(\mathbb{C})$. (cf. [Silverman, 2009, capítulo VI, proposición 3.6])

Este teorema le asocia a cada retícula Λ una curva elíptica $E/\mathbb{C}$. El resultado inverso es el teorema de uniformización:

Teorema 74. *Sean $A, B \in \mathbb{C}$ tales que $4A^3 - 27B^2 \neq 0$, entonces existe una retícula $\Lambda \subset \mathbb{C}$ tal que $g_2(\Lambda) = A$ y $g_3(\Lambda) = B$. En particular para cada curva elíptica $E : y^2 = x^3 + Ax + B$ existe una retícula Λ tal que $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ como variedades complejas. Además, existe un $\tau \mathrm{SL}_2(\mathbb{Z}) \in \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ tal que $\Lambda \cong \mathbb{Z}\tau \oplus \mathbb{Z}$ y por lo tanto $E(\mathbb{C}) \cong \mathbb{C}/(\tau\mathbb{Z} \oplus \mathbb{Z})$.*

Los isomorfismos en los teoremas 73 y 74 también son homomorfismos de grupo (i.e. de grupos de Lie)

1.3.3 Curvas elípticas sobre campos finitos

Para esta sección fijamos un número primo impar p y fijamos una potencia $q = p^n$ de p. De manera usual, denotamos al campo de Galois de orden q por $\mathbb{F}_q$. También fijamos una curva elíptica E definida sobre $\mathbb{F}_q$. Vamos a estar interesados en calcular la cantidad de puntos en $E(\mathbb{F}_q)$.

Un resultado famoso, debido a Hasse, dice que $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$ (cf. [Silverman, 2009, capítulo V, teorema 1.1]). En esta sección calcularemos $\#E(\mathbb{F}_q)$ usando la traza del mapeo de Frobenius que está definido para cualquier curva elíptica sobre un campo finito.

El mapeo de Frobenius usual $\varphi : \mathbb{F}_q \to \mathbb{F}_q$, definido por $x \mapsto x^q$, induce un automorfismo de E (que denotamos igual) definido en coordenadas afines por $P = (x, y) \mapsto (x^q, y^q)$. Con esto tenemos:

Teorema 75. *Sea $E/\mathbb{F}_q$ una curva elíptica, $\varphi : E \to E$ el mapeo de Frobenius de orden q y escribe $a_q(E) := q + 1 - \#E(\mathbb{F}_q)$. Entonces el morfismo inducido $\varphi_\ell : T_\ell(E) \to T_\ell(E)$ en los módulos de Tate ($\ell \neq p$) tiene polinomio característico $T^2 - a_q(E)T + q$. En particular el mapeo de Frobenius satisface $\varphi^2 - a_q(E)\varphi + q = 0 \in \mathrm{End}(E)$.*

Proof. Como el grupo absoluto de Galois $G_{\mathbb{F}_q}$ es generado topológicamente por el mapeo de Frobenius de orden q sobre $\overline{\mathbb{F}}_q$, entonces $P \in E(\mathbb{F}_q)$ si y solamente si $\varphi(P) = \varphi(x, y) = (x^q, y^q) = (x, y) = P$ o equivalentemente $E(\mathbb{F}_q) = \ker(1 - \varphi)$.

Ahora como $p \nmid 1$, la isogenia $1 - \varphi$ es separable (cf. [Silverman, 2009, capítulo III, corolario 5.5]) y las isogenias separables cumplen que $\#\ker\varphi = \deg\varphi$ (cf. [Silverman, 2009, capítulo III, teorema 4.10.c]), tenemos que

$$\#E(\mathbb{F}_q) = \#\ker(1 - \varphi) = \deg(1 - \varphi). \tag{1.55}$$

Nota. Como $\deg\varphi = q$ y $\deg : \mathrm{End}(E) \to \mathbb{Z}$ es una forma cuadrática positiva definida, la desigualdad de Hasse mencionada anteriormente se sigue de la fórmula anterior después de aplicar una versión adecuada de la desigualdad de Cauchy-Schwarz para deg.

Luego aplicamos la proposición 71 a 1.55 y tenemos que $\det\varphi_\ell = \deg\varphi = q$ y

$$\mathrm{tr}\varphi_\ell = 1 + \deg\varphi - \deg(1 - \varphi) = 1 + q - \#E(\mathbb{F}_q) = a_q(E).$$

Por lo tanto el polinomio característico de φ_ℓ es $T^2 - a_q(E)T + q$.

Por el teorema de Cayley-Hamilton, $\varphi_\ell^2 - a_q(E)\varphi_\ell + q = 0$. Volvemos a aplicar la proposición 71 para concluir que:

$$\deg(\varphi^2 - a_q(E)\varphi + q) = \det(\varphi_\ell^2 - a_q(E)\varphi_\ell + q) = 0.$$

La única isogenia de grado cero es $[0] \in \mathrm{End}(E)$ y acabamos. □

Curvas elípticas sobre campos finitas también surgen de curvas elípticas definidas sobre $\mathbb{Q}$ o en general sobre campos locales (i.e. localmente compactos con respecto de una topología no discreta, por ejemplo cualquier extensión finita de $\mathbb{Q}_p$ para algún primo p).

Sea $E/\mathbb{Q}$ una curva elíptica con una ecuación $y^2 = ax^3 + bx^2 + cx + d$ y sea p primo. Entonces bajo el cambio de coordenadas $x = ux' + v$, $y = wy'$ (para algunas $u, v, w \in \mathbb{Q}$) la nueva curva elíptica E' definida por

$$(y')^2 = aw^{-2}(ux' + v)^3 + bw^{-2}(ux' + v)^2 + cw^{-2}(ux' + v) + dw^{-2} = a'(x')^3 + b'(x')^2 + c'x' + d'$$

es isomorfa a E y los números $u, v, w \in \mathbb{Q}$ se pueden tomar de tal manera que los denominadores de los nuevos coeficientes sean primos relativos con p, ie $a', b', c', d' \in \mathbb{Z}_{(p)}$ (la localización de $\mathbb{Z}$ en el ideal primo $p\mathbb{Z}$).

El anillo $\mathbb{Z}_{(p)}$ tiene un morfismo de reducción módulo p:

$$\mathbb{Z}_{(p)} \xrightarrow{\bmod p} \tfrac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} \cong \tfrac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p.$$

Por lo tanto si tomamos el polinomio $y^2 - ax^3 - bx^2 - cx - d \in \mathbb{Z}_{(p)}[x, y]$ que define E (después de un cambio de coordenadas adecuado) podemos aplicar la reducción módulo p a cada coeficiente, i.e. aplicar el morfismo $\mathbb{Z}_{(p)}[x, y] \twoheadrightarrow \mathbb{F}_p[x, y]$ para obtener un polinomio con coeficientes en $\mathbb{F}_p$. En ciertos casos, este procedimiento produce una curva elíptica E_p definida sobre un campo finito. Veamos bajo qué condiciones sucede esto.

Definición 76. Sea $E/\mathbb{Q}$ una cuva elíptica y p un primo impar.

1. E tiene *buena reducción* módulo p si existe un cambio de variable tal que la nueva ecuación que define a E cumple $y^2 - ax^3 - bx^2 - cx - d \in \mathbb{Z}_{(p)}[x, y]$ y además $a \in \mathbb{Z}^*_{(p)}$, de tal manera que la curva elíptica $E_p/\mathbb{F}_p$ es suave (o equivalentemente que la ecuación $y^2 = ax^3 + bx^2 + cx + d \pmod p$ tiene tres raices diferentes).

2. E tiene *reducción multiplicativa* módulo p si existe un cambio de variable tal que la nueva ecuación que define a E cumple $y^2 - ax^3 - bx^2 - cx - d \in \mathbb{Z}_{(p)}[x, y]$ y además $a \in \mathbb{Z}^*_{(p)}$, de tal manera que la ecuación $y^2 = ax^3 + bx^2 + cx + d \pmod p$ tiene una raiz de multiplicidad dos y otra raiz simple.

3. E tiene *reducción aditiva* módulo p si existe un cambio de variable tal que la nueva ecuación que define a E cumple $y^2 - ax^3 - bx^2 - cx - d \in \mathbb{Z}_{(p)}[x, y]$ y además $a \in \mathbb{Z}^*_{(p)}$, de tal manera que la ecuación $y^2 = ax^3 + bx^2 + cx + d \pmod p$ tiene una raiz de multiplicidad tres.

Decimos que E tiene *reducción mala* si satisface 2 o 3. Si E tiene reducción multiplicativa, decimos que la reducción es *partida* si las direcciones de las tangentes en el nodo son elementos de $\mathbb{F}_p$ y decimos que es *no-partida* en otro caso.

Definición 77. Una curva elíptica $E/\mathbb{Q}$ es semiestable en un primo p si tiene reducción buena en p o reducción multiplicativa partida en p. Decimos que E es *semiestable* si es semiestable en todo primo.

1.4 Representaciones de Galois

1.4.1 Definiciones Preliminares

En esta sección vamos a fijar la siguiente notación: ℓ y p siempre son números primos, $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ es el grupo de Galois absoluto de $\mathbb{Q}$ (muchos resultados de esta sección se pueden generalizar a cualquier grupo de Galois $G_{L|K} = \mathrm{Gal}(L \mid K)$) que, con la topología de Krull [Neukirch, 1999, capítulo IV, §1], es un grupo topológico compacto y Hausdorff, de hecho:

$$G_{\mathbb{Q}} = \varprojlim_{K} \mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$$

donde K corre sobre todas las extensiones de Galois de $\mathbb{Q}$. En particular $G_{\mathbb{Q}}$ es un grupo profinito, i.e. admite una base local del $1 \in G_{\mathbb{Q}}$ de los subgrupos normales abiertos $\mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$ (donde $K/\mathbb{Q}$ es finito y de Galois).

Definición 78. Sea A un anillo topológico. Una *representación de Galois* es un homomorfismo $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(A)$ de grupos topológicos. Decimos que dos representaciones de Galois ρ y ρ' son isomorfas, denotado por $\rho \cong \rho'$, si existe una matriz $M \in \mathrm{GL}_n(A)$ tal que $\rho(\sigma) = M\rho'(\sigma)M^{-1}$ para toda $\sigma \in G_{\mathbb{Q}}$. Decimos que ρ es *impar* si $\det \rho(\mathfrak{c}) = -1$ donde $\mathfrak{c} \in G_{\mathbb{Q}}$ es la conjugación compleja.

Nota. Como $G_{\mathbb{Q}}$ es compacto, ρ satisface muchas de las mismas propiedades de las representaciones de grupos finitos como el lema de Schur [Serre, 1977a, parte I, §4].

Nosotros vamos a estar interesados en tres casos de representaciones de Galois:

1. A es una extensión de campos finita sobre $\mathbb{Q}_\ell$. Recuerde que todo campo de esta forma se obtiene al completar un campo numérico $K|\mathbb{Q}$ con respecto de un valor absoluto $|*|_\lambda$ que está canónicamente asociado a un ideal primo $\lambda \subset \mathcal{O}_K$ sobre ℓ. Esta completación, denotada por K_λ, también se puede obtener como el campo de cocientes del límite inverso $\mathcal{O}_{K,\lambda} := \varprojlim_n \mathcal{O}_K/\lambda^n$, donde $\mathcal{O}_K$ es el anillo de enteros de K.

2. A es un *anillo de coeficientes*. Un anillo de coeficientes es un anillo local completo noetheriano con campo residual k finito. A es naturalmente un anillo topológico con la topología $\mathfrak{m}$-ádica donde $\mathfrak{m}$ es el ideal maximal de A. Una base para esta topología es la familia de abiertos $\{a + \mathfrak{m}^N \mid a \in A, N > 0\}$. Además, como A es completo, tenemos que $A \cong \varprojlim A/\mathfrak{m}^N$. De esta manera, la topología $\mathfrak{m}$-ádica de A induce una topología profinita en $\mathrm{GL}_n(A)$ dado por el isomorfismo $\mathrm{GL}_n(A) \cong \varprojlim \mathrm{GL}_n(A/\mathfrak{m}^N)$. En este caso, A casi siempre va a ser una extensión finita de la completación de $\mathbb{Q}_\ell$ con respecto de un ideal primo sobre ℓ o su anillo de enteros.

3. A es una extensión finita de $\mathbb{F}_\ell$. En este caso, a A y a $\mathrm{GL}_n(A)$ les damos la topología discreta.

El caso cuando $A = K$ es una extensión finita de $\mathbb{Q}_\ell$, la representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ es isomorfa a una representación cuya imagen cae dentro de $\mathrm{GL}_n(\mathcal{O}_K)$ donde $\mathcal{O}_K$ es el anillo de enteros de K. Más precisamente tenemos la siguiente proposición:

Proposición 79. *Sea K una extensión finita de $\mathbb{Q}_\ell$ con anillo de enteros $\mathcal{O}_K$ y $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ una representación de Galois. Si denotamos a la inclusión $\mathrm{GL}_n(\mathcal{O}_K) \hookrightarrow \mathrm{GL}_n(K)$ por i, entonces existe una representación de Galois $\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathcal{O}_K)$ tal que $\rho \cong i \circ \rho'$.*

Proof. Esto se sigue esencialmente de que $\rho(G_{\mathbb{Q}})$ es compacto en $\mathrm{GL}_n(K)$ que podemos conjugar para que esté contenido en el compacto $\mathrm{GL}_n(\mathcal{O}_K)$. Como $\mathcal{O}_K$ es un dominio de ideales principales, el rango de la imagen es la adecuada. Véase la proposición 9.3.5 de [Diamond and Shurman, 2005] para más detalles. □

En otras palabras, siempre que tengamos una representación de Galois $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$, podemos asumir (módulo isomorfismo) que la imagen de ρ está contenido en $\mathrm{GL}_n(\mathcal{O}_K)$.

En este trabajo vamos a trabajar con tres propiedades que pueden o no cumplir las representaciones de Galois: la irreducibilidad, la ramificación en primos y la modularidad. El propósito de esta sección es discutir estas propiedades. Empezamos con la más sencilla.

Definición 80. Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ una representación de Galois donde K es un campo finito o una extensión finita de $\mathbb{Q}_\ell$. Decimos que ρ es *irreducible* si el $K-$espacio vectorial K^n tiene exactamente dos subespacios $G_{\mathbb{Q}}-$invariantes: 0 y K^n. Además decimos que es *absolutamente irreducible* si para toda extensión finita K' de K, la representación $\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_n(K')$ definida por la composición $G_{\mathbb{Q}} \xrightarrow{\rho} \mathrm{GL}_n(K) \hookrightarrow \mathrm{GL}_n(K')$ es irreducible.

Como veremos más adelante (c.f. la proposición 86), la irreducibilidad y la irreducibilidad absoluta coinciden en dimensión 2 y caracterísitca diferente de 2 junto con una hipótesis adicional sobre el determinante de la representación, pero las representaciones que aparecen en este trabajo cumplen esa condición. Esta equivalencia se usará en la sección 2.1.

Las segunda propiedad esencial de las representaciones de Galois que estudiaremos es la ramificación, pero para poder discutirla necesitamos estudiar la estructura $G_{\mathbb{Q}}$ con más cuidado. Como $G_{\mathbb{Q}}$ es profinito, primero estudiamos los grupos de Galois de extensiones finitas.

Para cualquier extensión finita de Galois $K \mid \mathbb{Q}$ con anillo de enteros $\mathcal{O}_K$, si $\mathfrak{P} \subset \mathcal{O}_K$ es un ideal primo sobre p (i.e. $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$) entonces el grupo de descomposición de $\mathfrak{P} \mid p$ se define como

$$D_{p,\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(K \mid \mathbb{Q}) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Hay un epimorfismo natural $D_{p,\mathfrak{P}} \twoheadrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{P} \mid \mathbb{F}_p)$ definida por $\sigma \mapsto \big(x + \mathfrak{P} \mapsto \sigma(x) + \mathfrak{P}\big)$. El nucleo de este morfismo, denotado por $I_{p,\mathfrak{P}}$, es el *grupo de inercia*. Entonces tenemos el isomorfismo:

$$\frac{D_{p,\mathfrak{P}}}{I_{p,\mathfrak{P}}} \cong \mathrm{Gal}(\mathcal{O}_K/\mathfrak{P} \mid \mathbb{F}_p). \tag{1.56}$$

El grupo de Galois $\mathrm{Gal}(\mathcal{O}_K/\mathfrak{P} \mid \mathbb{F}_p)$ es generado por el automorfismo de Frobenius definido por $x \mapsto x^p$. A cualquier preimagen $\sigma \in D_{p,\mathfrak{P}}$ de φ_p bajo $D_{p,\mathfrak{P}} \twoheadrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{P} \mid \mathbb{F}_p)$ se le llama un *elemento de Frobenius* sobre p. Entonces σ está bien definido módulo el grupo de inercia $I_{p,\mathfrak{P}}$.

En el caso de la extensión $\overline{\mathbb{Q}} \mid \mathbb{Q}$, si $\mathfrak{p} \subset \overline{\mathbb{Z}}$ es un ideal maximal de la cerradura entera de $\mathbb{Z}$ en $\overline{\mathbb{Q}}$, entonces definimos el grupo de descomposición de $\mathfrak{p}$ como:

$$D_{\mathfrak{p}} := \{\sigma \in G_{\mathbb{Q}} \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Este grupo de descomposición es el límite inverso de los grupos de descomposición de las subextensiones finitas de Galois, es decir

$$D_{\mathfrak{p}} \cong \varprojlim_{K} D_{p,\mathfrak{p}\cap\mathcal{O}_K}$$

donde $K \subset \overline{\mathbb{Q}}$ corre sobre todas las subextensiones finitas de Galois y $\mathcal{O}_K$ es el anillo de enteros de K, además p es el número primo que cumple $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. En efecto, el isomorfismo está

dado por $\sigma \mapsto \{\sigma|_K\}_K$ donde estamos identificando a $\varprojlim D_{p,\mathfrak{p}\cap\mathcal{O}_K}$ como subconjunto del producto $\prod_K \mathrm{Gal}(K \mid \mathbb{Q})$.

Ahora, como $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, entonces la inclusión $\mathbb{Z} \hookrightarrow \overline{\mathbb{Z}}$ induce la inclusión $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \overline{\mathbb{Z}}/\mathfrak{p}$. Por lo tanto $\overline{\mathbb{Z}}/\mathfrak{p}$ es una extensión (de campos) de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. De hecho es la cerradura algebraica de $\mathbb{F}_p$ porque cualquier elemento $\alpha + \mathfrak{p} \in \overline{\mathbb{Z}}/\mathfrak{p}$ satisface un polinomio mónico con coeficientes en $\mathbb{F}_p$ que es la reducción módulo p del polinomio mónico que satisface $\alpha \in \overline{\mathbb{Z}}$ y porque cualquier extensión algebraica propia de $\overline{\mathbb{Z}}/\mathfrak{p}$ induciría una extensión entera de $\overline{\mathbb{Z}}$ en $\overline{\mathbb{Q}}$ y esto no puede suceder porque $\overline{\mathbb{Z}}$ es la cerradura entera de $\mathbb{Z}$ en $\overline{\mathbb{Q}}$. Por lo tanto tenemos un isomorfismo $\overline{\mathbb{Z}}/\mathfrak{p} \cong \overline{\mathbb{F}}_p$ y gracias a esto identificamos $\overline{\mathbb{Z}}/\mathfrak{p}$ con $\overline{\mathbb{F}}_p$. Por lo tanto obtenemos un epimorfismo $\overline{\mathbb{Z}} \twoheadrightarrow \overline{\mathbb{F}}_p$ con nucleo $\mathfrak{p}$.

De esta manera, cualquier $\sigma \in D_\mathfrak{p}$ induce un homomorfismo $\tilde{\sigma}$ definido por el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \overline{\mathbb{Z}} & \xrightarrow{\sigma} & \overline{\mathbb{Z}} \\ \downarrow & & \downarrow \\ \overline{\mathbb{F}}_p & \xrightarrow{\tilde{\sigma}} & \overline{\mathbb{F}}_p \end{array}$$

Más precisamente hay un homomorfismo $D_\mathfrak{p} \to G_{\mathbb{F}_p}$ definido por $\sigma \mapsto \tilde{\sigma}$ donde $\tilde{\sigma}(\alpha+\mathfrak{p}) = \sigma(\alpha)+\mathfrak{p}$.

El nucleo de $D_\mathfrak{p} \to G_{\mathbb{F}_p}$ se llama el grupo de inercia de $\mathfrak{p}$ y se denota por $I_\mathfrak{p}$. Análogamente al caso de $D_\mathfrak{p}$, el grupo de inercia de $\mathfrak{p}$ es el límite inverso de los grupos de inercia $I_{p,\mathfrak{p}\cap\mathcal{O}_K}$ donde K corre sobre todas las subextensiones finitas de Galois, i.e.

$$I_\mathfrak{p} \cong \varprojlim_K I_{p,\mathfrak{p}\cap\mathcal{O}_K}$$

donde $\mathcal{O}_K$ es el anillo de enteros de K.

Recuerde que $G_{\mathbb{F}_p} \cong \widehat{\mathbb{Z}}$, la completación profinita[2] de $\mathbb{Z}$ (c.f. [Neukirch, 1999, capítulo IV, §2, ejemplo 5]). Entonces el *automorfismo de Frobenius* $\varphi_p : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ definido por $\varphi_p(x) = x^p$ corresponde al elemento $1 \in \widehat{\mathbb{Z}}$ y el subgrupo generado por φ_p corresponde al subgrupo denso $\mathbb{Z} \subset \widehat{\mathbb{Z}}$. A cualquier preimagen de φ_p en $D_\mathfrak{p}$ bajo el homomorfismo $D_\mathfrak{p} \to G_{\mathbb{F}_p}$ se le llama un *elemento de Frobenius absoluto sobre p.*

Con todo esto podemos definir la ramificación:

Definición 81. Sea $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(A)$ una representación de Galois. Entonces ρ es *no-ramificado* en p si cumple $I_\mathfrak{p} \subseteq \ker\rho$ para algún (y por lo tanto todo, ver la siguiente nota) ideal maximal $\mathfrak{p} \subset \overline{\mathbb{Z}}$ sobre p. En general decimos que ρ es *no-ramificado casi donde sea* si ρ es no-ramificado para todo primo p salvo posiblemente un conjunto finito de números primos.

Nota. Si elegimos otro ideal primo $\mathfrak{p}'$ sobre p, entonces existe un $\sigma \in G_\mathbb{Q}$ tal que $\sigma(\mathfrak{p}) = \mathfrak{p}'$ (esto es porque $G_\mathbb{Q}$ actúa transitivamente sobre el conjunto de ideales primos sobre p). De esta manera $\sigma D_\mathfrak{p}\sigma^{-1} = D_{\sigma(\mathfrak{p})} = D_{\mathfrak{p}'}$ y en particular los grupos de inercia, $I_\mathfrak{p}$ y $I_\mathfrak{p}$, son conjugados. Por lo tanto, como $\ker\rho$ es un subgrupo normal, $I_\mathfrak{p} \subseteq \ker\rho$ si y solamente si $I_{\mathfrak{p}'} \subseteq \ker\rho$. Es decir la definición anterior no depende del ideal primo $\mathfrak{p}$ sobre p.

Nota. Si $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(\mathbb{C})$ es una representación compleja, entonces se factoriza a través de una representación $\rho' : \mathrm{Gal}(K_\rho \mid \mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ donde K_ρ es una extensión finita igual al campo fijo

[2]Formalmente $\widehat{\mathbb{Z}}$ se define como el límite inverso $\widehat{\mathbb{Z}} = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})$ donde el sistema proyectivo se define con el orden de divisibilidad, más precisamente, cuando $n \mid m$ entonces usamos la proyección módulo n y así la familia de morfismos $\{\mathbb{Z}/m\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}\}_{n|m}$ forman un sistema proyectivo; su límite inverso es $\widehat{\mathbb{Z}}$

de $\ker\rho \subset G_{\mathbb{Q}}$. Esto se sigue de que cualquier representación $\sigma : G \to \mathrm{GL}_2(\mathbb{C})$ tiene imagen finita cuando G es compacto, en efecto la representación inducida $\bar{\sigma} : G/\ker\sigma \to \mathrm{GL}_n(\mathbb{C})$ es un homeomorfismo a su imagen $\sigma(G)$. Pero éste es compacto en $\mathrm{GL}_n(\mathbb{C})$, por lo tanto es de Lie. Por lo tanto $\sigma(G)$ es totalmente disconexo y de Lie y concluimos que $G/\ker\sigma \cong \sigma(G)$ es finito. Como cualquier representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ tiene imagen finita, ρ es no-ramificado en p si y solamente si K_ρ es no ramificado en p[2].

Ejemplo 82. Sea $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ un caracter de Dirichlet primitivo. Sabemos que $\mathrm{Gal}(\mathbb{Q}(\mu_N)|\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^*$ y es la imagen de la proyección $\pi : G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_n) \mid \mathbb{Q})$ definida por la restricción $\sigma \mapsto \sigma|_{\mathbb{Q}(\mu_N)}$. Juntamos estos comentarios en el siguiente diagrama:

$$G_{\mathbb{Q}} \xrightarrow{\pi} \mathrm{Gal}(\mathbb{Q}(\mu_N) \mid \mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/N\mathbb{Z})^* \xrightarrow{\chi} \mathbb{C}^*$$
$$\rho_\chi$$

Por lo tanto obtenemos una representación ρ_χ asociado a χ. Afirmamos que ρ_χ es no-ramificado cuando $p \nmid N$. En efecto, $\ker\rho_\chi = \ker\pi$ y así su campo fijo es $\mathbb{Q}(\mu_N)$ donde la ramificación de primos es bien conocido: p es no-ramificado cuando $p \nmid N$.

Ahora estudiemos más a fondo qué sucede cuando ρ es no-ramificado en un primo p. En este caso elige un ideal primo $\mathfrak{p} \subset \overline{\mathbb{Z}}$ sobre p y un elemento de Frobenius absoluto $\sigma \in D_{\mathfrak{p}} \subset G_{\mathbb{Q}}$. Resulta que el valor $\rho(\sigma)$ es independiente de la elección de σ. En efecto, si σ' es otro elemento de Frobenius absoluto entonces $\sigma' = \sigma\tau$ para alguna $\tau \in I_{\mathfrak{p}}$ y así $\rho(\sigma') = \rho(\sigma\tau) = \rho(\sigma)$ ya que $I_{\mathfrak{p}} \subseteq \ker\rho$ por hipótesis.

Ahora, si elegimos otro ideal maximal $\mathfrak{p}'$ sobre p, entonces $\tau D_{\mathfrak{p}}\tau^{-1} = D_{\mathfrak{p}'}$ para alguna $\tau \in G_{\mathbb{Q}}$ y así cualquier elemento de Frobenius absoluto $\sigma' \in D_{\mathfrak{p}'}$ es de la forma $\tau\sigma\tau^{-1}$ donde $\sigma \in D_{\mathfrak{p}}$ es un elemento de Frobenius absoluto. Por lo tanto cambiar de ideal maximal sobre p conjuga al elemento de Frobenius absoluto. Esto quiere decir que el valor $\rho(\sigma)$ cambia por conjugación (por $\rho(\tau)$ en este caso). Por lo tanto la clase de conjugación $[\sigma] = \{\tau\sigma\tau^{-1} \mid \tau \in G_{\mathbb{Q}}\}$ de un elemento de Frobenius absoluto no depende de la elección de $\mathfrak{p}$, solamente de p. Este hecho nos sugiere la siguiente definición:

Definición 83. Sea p un número primo y sea $\sigma \in D_{\mathfrak{p}} \subset G_{\mathbb{Q}}$ un elemento de Frobenius absoluto para algún ideal maximal $\mathfrak{p} \subset \overline{\mathbb{Z}}$ sobre p. La clase de conjugación $[\sigma] \subset G_{\mathbb{Q}}$ se llama la *clase de conjugación de Frobenius* sobre p y se denota por Frob_p.

Recuerde que el polinomio característico de la matriz $\rho(\sigma)$ (para alguna $\sigma \in \mathrm{Frob}_p$) es invariante bajo conjugación. Por lo tanto el polinomio característico

$$\det(\rho(\mathrm{Frob}_p) - T\mathrm{Id}) := \det(\rho(\sigma) - T\mathrm{Id}) \quad \text{para alguna } \sigma \in \mathrm{Frob}_p$$

está bien definido y lo denotamos por $f_{\rho,p}$. Similarmente la traza $\mathrm{tr}\rho(\mathrm{Frob}_p)$ está bien definido.

Los primeros ejemplos de representaciones de Galois son los caracteres ciclotómicos y sus propiedades de ramificación son sencillas.

El grupo de Galois $G_{\mathbb{Q}}$ actúa sobre $\mu_N \subset \overline{\mathbb{Q}}$ de manera natural, entonces hay un homomorfismo de grupos $G_{\mathbb{Q}} \to \mathrm{Aut}(\mu_N)$. Recuerde que $\mathrm{Aut}(\mu_N) \cong (\mathbb{Z}/N\mathbb{Z})^*$, bajo el isomorfismo $f \mapsto n$ donde

[2]i.e. la factorización del ideal $p\mathcal{O}_\rho$ del anillo de enteros de K_ρ es un producto lineal de ideales primos distintos, todos con índice de ramificación 1.

n es el entero que cumple $f(\zeta) = \zeta^n$ para alguna raiz primitiva de la unidad $\zeta \in \mu_N$ (observe que este isomorfismo no es canónico). Por lo tanto obtenemos una representación

$$\bar{\chi}_N : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_1(\mathbb{Z}/N\mathbb{Z}) = (\mathbb{Z}/N\mathbb{Z})^*,$$

que llamamos el *caracter ciclotómico módulo* N. Esta representación cumple:

Proposición 84. *El caracter ciclotómico módulo N cumple y es caracterizado por las siguientes dos propiedades*

i) $\bar{\chi}_N$ *es no-ramificada en todo primo* $q \nmid N$.

ii) $\bar{\chi}_N(\mathrm{Frob}_q) \equiv q \pmod{N}$ *para toda* $q \nmid N$.

Proof. c.f. [Kato et al., 2011, §5.2 proposición 5.12 y §8.1 teorema 8.7] □

Ahora, si fijamos un número primo ℓ, tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} & & (\mathbb{Z}/\ell^{n+1}\mathbb{Z})^* \\ & \overset{\bar{\chi}_{\ell^{n+1}}}{\nearrow} & \big\downarrow \bmod \ell^n \\ G_{\mathbb{Q}} & \xrightarrow[\bar{\chi}_{\ell^n}]{} & (\mathbb{Z}/\ell^n\mathbb{Z})^* \end{array}$$

Entonces podemos pasar al límite inverso. Sabemos que $\varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^* \cong \mathbb{Z}_\ell^*$, entonces si denotamos por χ_ℓ al morfismo inducido por la propiedad universal del límite inverso, obtenemos una representación

$$\chi_\ell : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_\ell^*.$$

La representación χ_ℓ se llama el *caracter ciclotómico ℓ-ádico*. Similarmente a $\bar{\chi}_N$, la representación χ_ℓ cumple:

Proposición 85. *Para todo primo ℓ, el caracter ciclotómico χ_ℓ cumple, y es caracterizado por, las siguientes propiedades:*

i) χ_ℓ *es no-ramificada para todo primo q distinto de ℓ.*

ii) $\chi_\ell(\mathrm{Frob}_q) = q$ *cuando* $q \neq \ell$.

Proof. Las propiedades de $\bar{\chi}_{\ell^n}$ de la proposición 84 se preservan al pasar al límite inverso. □

esta nota nueva es una generalizacion de la nota despues del teorema de Eichler-Shimura que cambie de lugar aqui. La proposicion que sigue tambien es nuevo y se usa en Langlands-Tunnell

Nota. En general los caracteres ciclotómicos los vamos a usar para imponer condiciones sobre el determinante de las representaciones de Galois. Más precisamente vamos a pedir, o demostrar, que el determinante de una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(A)$, definido por la composición

$$\det \rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_n(A) \xrightarrow{\det} A^*$$

sea igual a algún caracter ciclotómico. Pero inmediatamente vemos que A no necesariamente es $(\mathbb{Z}/N\mathbb{Z})^*$ o $\mathbb{Z}_\ell^*$, entonces las igualdades $\det \rho = \bar{\chi}_N$ o $\det \rho = \chi_\ell$ no están bien definidas. Por suerte hay una manera natural de corregir esta discrepancia.

Cuando A es una extensión finita de $\mathbb{Q}_\ell$ (resp. su anillo de enteros), tenemos $\mathbb{Z}_\ell \subset \mathbb{Q}_\ell$ (resp. $\mathbb{Z}_\ell \subset A$) así tenemos una inclusión natural $\mathbb{Z}_\ell^* \hookrightarrow A^*$. Por lo tanto si componemos χ_ℓ con esta

inclusión obtenemos la representación $\chi_\ell : G_\mathbb{Q} \to A^*$ que denotamos con el mismo símbolo. De esta manera la igualdad $\det\rho = \chi_\ell$ tiene sentido. De manera similar, si A es una extensión finita de $\mathbb{F}_p$, componemos el caracter ciclotómico $\bar{\chi}_p$ con la inclusión $\mathbb{F}_p^* \hookrightarrow A^*$ para obtener el caracter $\bar{\chi}_p : G_\mathbb{Q} \to A^*$ que sí se puede comparar con $\det\rho$.

En palabras, cuando decimos que $\det\rho$ es igual a un caracter ciclotómico, estamos componiendo el caracter ciclotómico con una inclusión adecuada para que la igualdad tenga sentido.

Con estas consideraciones sobre los caracteres ciclotómicos, estamos en posición para enunciar y probar la equivalencia de la irreducibilidad y la irreducibilidad absoluta de las representaciones de Galois de dimensión 2:

Proposición 86. *Sea $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(K)$ una representación de Galois con K una extensión finita de $\mathbb{F}_\ell$ (resp. $\mathbb{Q}_\ell$) donde $\ell \neq 2$. Si ρ es irreducible y $\det\rho = \bar{\chi}_\ell$ (resp. $\det\rho = \chi_\ell$) entonces ρ es absolutamente irreducible.*

Proof. Sea $\mathfrak{c} \in G_\mathbb{Q}$ la conjugación compleja. Claramente $\rho(\mathfrak{c})^2 = \mathrm{Id}$ y así sus valores propios satisfacen la ecuación $T^2 - 1 = 0$. Como $\ell \neq 2$, los dos valores propios 1 y -1 son distintos y $\det(\mathfrak{c}) = -1$.

Ahora supongamos que ρ no es absolutamente irreducible. Entonces existe una extensión finita L de K tal que la composición $G_\mathbb{Q} \xrightarrow{\rho} \mathrm{GL}_2(K) \hookrightarrow \mathrm{GL}_2(L)$ no es irreducible. Como estamos en dimensión 2, esto significa que existe un subespacio $V \subset L^2$ de dimensión 1 que es $G_\mathbb{Q}-$invariante. Gracias a la dimensión de V, éste tiene que ser un eigenespacio de $\rho(\mathfrak{c})$ porque no hay ningún otro subespacio de dimensión 1 que sea estable bajo la acción de $\rho(\mathfrak{c})$.

Ahora, $\rho(\mathfrak{c})$ está definido sobre K, i.e. las entradas de $\rho(\mathfrak{c})$ son elementos de K. De esta manera, un generador de V, cuyas coordenadas están en L, tiene un múltiplo cuyas coordenadas están en K. Por lo tanto induce el subespacio $V \cap K^2 \subset K^2$ de dimensión 1 que es $G_\mathbb{Q}-$estable. Esto contradice la irreducibilidad de ρ. Por lo tanto concluimos que ρ es absolutamente irreducible. □

1.4.2 Representaciones asociadas a curvas elípticas

Sea E una curva elíptica sobre $\mathbb{Q}$ y $E[N] \subset E(\overline{\mathbb{Q}})$ sus puntos de orden N. Observa que el grupo de Galois absoluto $G_\mathbb{Q}$ actúa sobre $E(\overline{\mathbb{Q}})$ y en particular actúa sobre $E[N]$. Esta acción está bien definida porque la acción de $G_\mathbb{Q}$ conmuta con la suma de E. En efecto, si P y Q son dos puntos de E, entonces las coordenadas de $P + Q$ son funciones racionales en las coordenadas de P y Q [Silverman, 2009, §III.2, Group Law Algorithm]. Por lo tanto, como el neutro tiene coordenadas racionales,

$$O = O^\sigma = ([N]P)^\sigma = (P + \cdots + P)^\sigma = P^\sigma + \cdots + P^\sigma = [N]P^\sigma$$

y así $P^\sigma \in E[N]$ siempre que $P \in E[N]$. De esta manera cada σ induce un automorfismo de $E[N]$, es decir, tenemos una representación $G_\mathbb{Q} \to \mathrm{Aut}(E[N])$. Por otro lado, sabemos que $E[N] \cong (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ (c.f. la proposición 68 de la sección 1.3.1), entonces $\mathrm{Aut}(E[N])$ es simplemente $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Así definimos:

Definición 87. La representación de Galois de los puntos de N-torsión de una curva elíptica $E/\mathbb{Q}$ se denota por

$$\bar{\rho}_{E,N} : G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

Cuando $N = p$ es primo, podemos determinar la ramificación de $\bar{\rho}_{E,p}$ en los primos donde E tiene buena reducción y calcular su polinomio característico.

Proposición 88. *Sea p un primo y sea E una curva elíptica sobre Q con buena reducción en un primo q distinto de p. Entonces,*

i) $\bar{\rho}_{E,p}$ es no-ramificado en q y en particular, $\bar{\rho}_{E,p}$ es no-ramificado casi donde sea.

ii) El polinomio característico de $\bar{\rho}_{E,p}$ cumple

$$\det(\bar{\rho}_{E,p}(\mathrm{Frob}_q) - T\mathrm{Id}) \equiv q - a_q(E)T + T^2 \pmod{p},$$

donde $a_q(E) = q + 1 - \#E(\mathbb{F}_q)$ (compare con el teorema 75).

Proof. (c.f. [Saito, 2013a, §3.3, proposición 3.15]) □

Como en el caso del caracter ciclotómico módulo N, podemos pasar al límite inverso. Más precisamente, si fijamos un primo ℓ y tomamos $n \geq 1$ arbitrario, tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccccc} & & \mathrm{GL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) & \xrightarrow{\cong} & \mathrm{Aut}(E[\ell^{n+1}]) \\ & \overset{\bar{\rho}_{E,\ell^{n+1}}}{\nearrow} & \downarrow \text{mod } \ell^n & & \vdots \\ G_{\mathbb{Q}} & \xrightarrow[\bar{\rho}_{E,\ell^n}]{} & \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) & \xrightarrow{\cong} & \mathrm{Aut}(E[\ell^n]) \end{array}$$

Por lo tanto, como en el caso del caracter ciclotómico ℓ-ádico, existe naturalmente una representación de $G_{\mathbb{Q}}$ en $\varprojlim \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \cong \varprojlim \mathrm{Aut}(E[\ell^n]) = \mathrm{Aut}(T_\ell(E))$, es decir, tenemos:

Definición 89. Sea E una curva elíptica sobre $\mathbb{Q}$, entonces la *representación de Galois ℓ-ádica* asociada a E, es la representación

$$\rho_{E,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \cong \mathrm{Aut}(T_\ell(E))$$

Esta representación cumple casi las mismas propiedades que $\bar{\rho}_{E,p}$. La siguiente proposición sobre $\rho_{E,\ell}$ se obtiene esencialmente aplicando el el límite inverso a la proposición 88.

Proposición 90. *Sea ℓ un primo fijo y sea E una curva elíptica sobre $\mathbb{Q}$, entonces*

i) $\rho_{E,\ell}$ es no-ramificado en q para todo primo distinto de ℓ donde E tenga buena reducción. En particular, $\rho_{E,\ell}$ es no-ramificado casi donde sea.

ii) El polinomio característico de $\rho_{E,\ell}$ es

$$\det(\rho_{E,\ell}(\mathrm{Frob}_q) - T\mathrm{Id}) = q - a_q(E)T + T^2 \qquad (\forall q \neq \ell).$$

Del polinomio característico de $\rho_{E,\ell}(\mathrm{Frob}_q)$ podemos leer el determinante y la traza de $\rho_{E,\ell}(\mathrm{Frob}_q)$. En particular, el caracter $\det \rho_{E,\ell} : G_{\mathbb{Q}} \to \mathbb{Z}_\ell^*$ obtenido de la composición $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell) \xrightarrow{\det} \mathbb{Z}_\ell^*$, cumple que $\det \rho_{E,\ell}(\mathrm{Frob}_q) = q$ para toda q distinta de ℓ; cumple la mitad de las propiedades que caracterizan al caracter ciclotómico ℓ-ádico. Por otro lado, como toda curva elíptica sobre $\mathbb{Q}$ solamente tiene una cantidad finita de primos donde hay reducción mala, entonces $\rho_{E,\ell}$ es no-ramificado casi donde sea. Entonces, como consecuencia de las proposiciones 84, 85, 88 y 90, tenemos el siguiente corolario:

Corolario 91. *Sea E una curva elíptica sobre $\mathbb{Q}$ y sean p y ℓ primos fijos. Entonces:*

1. $\det \bar{\rho}_{E,p} = \bar{\chi}_p$ *y* $\mathrm{tr}\bar{\rho}_{E,p}(\mathrm{Frob}_q) \equiv a_q(E) \pmod{p}$ *para todo primo q distinto de p.*

2. $\det \rho_{E,\ell} = \chi_\ell$ *y* $\mathrm{tr}\rho_{E,\ell}(\mathrm{Frob}_q) = a_q(E)$ *para todo primo q distinto de p.*

1.4.3 La modularidad de representaciones de Galois

En esta sección estudiamos las representaciones de Galois que surgen de las formas modulares. Como en la sección 1.1, denotamos por $S_2(\Gamma_0(N))$ al espacio de formas cuspidales de peso 2 y sea $f \in S_2(\Gamma_0(N))$ una forma primitiva (véase la definición 32). Recuerde que el campo numérico de f, denotado por K_f, es la extensión finita de $\mathbb{Q}$ generada por los valores propios de f bajo los operadores de Hecke (c.f. la proposición 34). Denotamos por $\mathcal{O}_f$ al anillo de enteros de K_f.

Gracias al trabajo de Eichler y Shimura, cada forma primitiva de peso 2 tiene asociado una representación de Galois:

Teorema 92. *(Eichler-Shimura) Sea $f \in S_2^{\text{new}}(\Gamma_0(N))$ una forma primitiva y ℓ un número primo. Para todo ideal primo $\lambda \subset \mathcal{O}_f$ sobre ℓ escribimos $K_{f,\lambda}$ como la completación de K_f con respecto del valor absoluto asociado a λ. Bajo estas condiciones, existe una representación de Galois*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(K_{f,\lambda})$$

que satisface las siguientes propiedades:

i) $\rho_{f,\lambda}$ *es no-ramificado en q para todo primo $q \nmid N\ell$.*

ii) $\det \rho_{f,\lambda} = \chi_\ell$ *el caracter ciclotómico $\ell-$ádico (esta iguladad se justifica en la nota después de la proposición 85).*

iii) $\mathrm{tr}(\rho_{f,\lambda}(\mathrm{Frob}_q)) = a_q(f)$ *para todo primo $q \nmid N\ell$.*

Proof. Esto es el teorema 9.5.4 en §9.5 de [Diamond and Shurman, 2005], ó véase §7.6 de [Shimura, 1994]. □

Este teorema tiene una generalización a otros pesos distintos de 2 (c.f. el teorema 9.6.5 de [Diamond and Shurman, 2005]). El teorema anterior para pesos mayores que 2 es debido a Deligne [Deligne, 1971] y para peso 1 es debido a Deligne y Serre [Deligne and Serre, 1974]. Aunque en este trabajo solamente nos enfocaremos en peso 2 para definir modularidad, el artículo de Deligne y Serre volverá a aparecer en la sección 2.1 para la prueba de la modularidad de $\bar{\rho}_{E,3}$.

Las representaciones de Galois asociadas a formas primitivas nos determinan una clase muy importante de representaciones. Para definirla, necesitamos separar en casos según qué anillo topológico A tomamos:

Definición 93. Sea ℓ un primo y sea $A = K$ una extensión finita de $\mathbb{Q}_\ell$. Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(K)$ una representación de Galois no-ramificada casi donde sea. Decimos que ρ es *modular* si existe una forma primitiva $f \in S_2^{\text{new}}(\Gamma_0(N))$ y un ideal primo $\lambda \subset \mathcal{O}_f$ sobre ℓ tales que $K_{f,\lambda} \hookrightarrow K$ y $\rho \cong \rho_{f,\lambda}$ (donde estamos identificando $\rho_{f,\lambda}$ con la composición $G_{\mathbb{Q}} \xrightarrow{\rho_{f,\lambda}} \mathrm{GL}_2(K_{f,\lambda}) \hookrightarrow \mathrm{GL}_2(K)$).

aqui empieza lo nuevo——————————————————

agregue dos proposiciones que prueban una condicion suficiente para establecer la modularidad de $\rho_{E,\ell}$

Esta definición es difícil de aplicar, entonces queremos una condición suficiente para modularidad que sea más práctico de verificar. Primero enunciamos una condición suficiente para determinar cuando dos representaciones son isomorfas y luego la aplicamos a las representaciones $\rho_{E,\ell}$ que vimos en la sección anterior.

Proposición 94. *Sea K una extensión finita de $\mathbb{Q}_\ell$ y $\rho, \rho' : G_\mathbb{Q} \to \mathrm{GL}_n(K)$ dos representaciones de Galois que son no-ramificadas casi donde sea. Entonces:*

$$\rho \text{ es irreducible y } \operatorname{tr}\rho(\mathrm{Frob}_q) = \operatorname{tr}\rho'(\mathrm{Frob}_q) \text{ para casi todo primo } q \quad \Longrightarrow \quad \rho \cong \rho'.$$

Proof. Esto es la proposición 3.4 de §3.1 en [Saito, 2013b]. □

Corolario 95. *Sea E una curva elíptica sobre $\mathbb{Q}$ tal que $\rho_{E,\ell} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}_\ell) \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell)$ es irreducible para algún primo $\ell \neq 2$ (donde E necesariamente tiene buena reducción). Si existe una forma primitiva $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ tal que $a_q(f) = a_q(E)$ para casi todo primo q, entonces $\rho_{E,\ell}$ es modular.*

Proof. Por la proposición 90 y el Teorema 92, las representaciones $\rho_{E,\ell}$ y $\rho_{f,\ell}$ son no-ramificadas casi donde sea (esto es independiente del ideal primo $\lambda \subset \mathcal{O}_f$). Si componemos $\rho_{E,\ell}$ con la inclusión $i : \mathrm{GL}_2(\mathbb{Z}_\ell) \hookrightarrow \mathrm{GL}_2(K_{f,\lambda})$, esta nueva representación sigue siendo no-ramificada casi donde sea porque $\ker\rho_{E,\ell} \subseteq \ker(i \circ \rho_{E,\ell})$. Además sigue siendo irreducible porque la proposición 86 nos dice que $\rho_{E,\ell}$ es absolutamente irreducible.

Por lo tanto, para aplicar la proposición anterior a $\rho_{E,\ell}$ y $\rho_{f,\ell}$ solamente nos falta verificar que $\operatorname{tr}\rho_{E,\ell}(\mathrm{Frob}_q) = \operatorname{tr}\rho_{f,\ell}(\mathrm{Frob}_q)$ para casi todo primo q, pero esto es inmediato de las fórmulas para $\operatorname{tr}\rho_{E,\ell}(\mathrm{Frob}_q)$ y de $\operatorname{tr}\rho_{f,\ell}(\mathrm{Frob}_q)$ que aparecen en el corolario 91 y el teorema 92 respectivamente. Con esto aplicamos la proposición 94 para concluir que $\rho_{E,\ell} \cong \rho_{f,\ell}$ y que $\rho_{E,\ell}$ es modular. □

Necesito que $a_q(f) \in \mathbb{Q}$????

aqui termina lo nuevo————————————————

Para definir modularidad para representaciones sobre extensiones finitas de $\mathbb{F}_\ell$, retomamos la representación de Galois $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(A)$, donde A es una extensión finita de $\mathbb{Q}_\ell$. Bajo estas condiciones, ρ se factoriza a través de la inclusión $\mathrm{GL}_n(\mathcal{O}_A) \hookrightarrow \mathrm{GL}_n(A)$ donde $\mathcal{O}_A$ es el anillo de enteros de A; esto es exactamente la proposición 79. Más precisamente, existe una representación de Galois $\rho' : G_\mathbb{Q} \to \mathrm{GL}_n(\mathcal{O}_A)$ tal que ρ es isomorfa a la composición

$$G_\mathbb{Q} \xrightarrow{\rho'} \mathrm{GL}_n(\mathcal{O}_A) \hookrightarrow \mathrm{GL}_n(A).$$

Por lo tanto, en el caso $A = K_{f,\lambda}$ para alguna forma primitiva $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ y un ideal primo $\lambda \subset \mathcal{O}_f$ sobre ℓ, cada representación de Galois $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(K_{f,\lambda})$ tiene asociada una representación $\rho' : G_\mathbb{Q} \to \mathrm{GL}_n(\mathcal{O}_{f,\lambda})$ donde $\mathcal{O}_{f,\lambda}$ es el anillo de enteros de $K_{f,\lambda}$. Definimos la representación $\bar\rho_{f,\lambda} : G_\mathbb{Q} \to \mathrm{GL}_n(\mathcal{O}_{f,\lambda}/\mathfrak{m}_{f,\lambda})$ obtenida por la composición de ρ' con la proyección módulo $\mathfrak{m}_{f,\lambda} = \lambda\mathcal{O}_{f,\lambda}$. Resumimos estos dos párrafos con el siguiente diagrama conmutativo:

$$\begin{array}{ccccc} & & & & \mathrm{GL}_n(K_{f,\lambda}) \\ & \overset{\rho_{f,\lambda}}{\nearrow} & & & \uparrow \\ G_\mathbb{Q} & & \xrightarrow{\rho'} & \mathrm{GL}_n(\mathcal{O}_{f,\lambda}) & \xrightarrow{\bmod \mathfrak{m}_{f,\lambda}} \mathrm{GL}_n(\mathcal{O}_{f,\lambda}/\mathfrak{m}_{f,\lambda}). \\ & \searrow & & \overset{\exists\,\bar\rho_{f,\lambda}}{\nearrow} & \end{array} \tag{1.57}$$

Recuerde que $\mathcal{O}_{f,\lambda}/\mathfrak{m}_{f,\lambda}$ es una extensión finita de $\mathbb{F}_\ell$. Por lo tanto la asignación $\rho_{f,\lambda} \mapsto \bar\rho_{f,\lambda}$ asocia a cada representación $\rho_{f,\lambda} : G_\mathbb{Q} \to \mathrm{GL}_2(K_{f,\lambda})$ una representación $\bar\rho_{f,\lambda} : G_\mathbb{Q} \to \mathrm{GL}_2(F)$ donde F es una extensión finita de $\mathbb{F}_\ell$.

Ahora definimos la modularidad de representaciones de Galois sobre $\bar{\mathbb{F}}_\ell$.

Definición 96. Una representación de Galois $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$ es *modular* si existe una forma primitiva $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ y un ideal primo $\lambda \subset \mathcal{O}_f$ sobre ℓ tales que $\rho \cong \bar{\rho}_{f,\lambda}$.

Nota. Si F es una extensión finita de $\mathbb{F}_\ell$, entonces $F \subset \bar{\mathbb{F}}_\ell$. Así podemos extender la definición anterior a la representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$ simplemente considerando la composición $G_{\mathbb{Q}} \xrightarrow{\rho} \mathrm{GL}_2(F) \hookrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$. Conversamente, si tenemos una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$, la imagen de ρ es finito por ser un subconjunto compacto del espacio discreto $\bar{\mathbb{F}}_\ell$ (ya que $G_{\mathbb{Q}}$ es compacto y ρ es continua). Por lo tanto la imagen de ρ está contenido en $\mathrm{GL}_2(F)$ para alguna extensión finita F de $\mathbb{F}_\ell$, es decir, ρ se factoriza a través de la inclusión $\mathrm{GL}_2(F) \hookrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$. En conclusión, una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$ induce una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$ donde $[F : \mathbb{F}_\ell] < \infty$ y vice versa. Por lo tanto la definición anterior realmente es una definición de modularidad de representaciones sobre extensiones finitas de $\mathbb{F}_\ell$.

Como con la definición 93, esta última definición de modularidad no es práctica, pero también tenemos un resultado análogo al corolario 95 para establecer una condición suficiente para la modularidad de una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$.

Proposición 97. *Sea E una curva elíptica sobre $\mathbb{Q}$ tal que su representación de Galois $\bar{\rho}_{E,p}$ asociada a sus puntos de $p-$torsión es irreducible. Si existe una forma primitiva $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ y un ideal primo $\mathfrak{P} \subset \mathcal{O}_f$ sobre p tales que*

$$a_q(E) \equiv a_q(f) \pmod{\mathfrak{P}}$$

para casi todo primo q, entonces $\bar{\rho}_{E,p}$ es modular.

esta proposici y la nota tambien son nuevas

Nota. La prueba de la proposición anterior es muy similar a la prueba del corolario 95 pero se basa en una versión distinta de de la proposición 94. Esa versión viene en la misma proposición de [Saito, 2013a] citada en la prueba y de hecho no requiere la hipótesis sobre la ramificación como lo pide la proposición 94.

La modularidad de una curva elíptica está codificada en la modularidad de las representaciones ℓ-ádicas asociadas a la curva:

Teorema 98. *Sea $E/\mathbb{Q}$ una curva elíptica. Entonces las siguientes afirmaciones son equivalentes:*

1. *E es modular.*
2. *$\rho_{E,\ell}$ es modular para todo primo ℓ.*
3. *Existe un primo ℓ tal que $\rho_{E,\ell}$ es modular.*

Proof. c.f. [Saito, 2013a, §3.4, proposición 3.23] □

Este teorema es un paso fundamental en la prueba de STW semiestable (véase la segunda figura de la introducción).

Chapter 2

El teorema de modularidad

2.1 El teorema de Langlands-Tunnel y la modularidad de $\bar{\rho}_{E,3}$

Sea E una curva elíptica sobre $\mathbb{Q}$ y sea $\bar{\rho}_{E,3}$ la representación asociada a sus puntos de 3−torsión (c.f. la sección 1.4). En esta sección, probamos cómo la modularidad de $\bar{\rho}_{E,3}$ se sigue de un teorema celebrado de Langlands [Langlands, 1980] y Tunnel [Tunnell, 1981]. La versión de su teorema que vamos a usar es:

Teorema 99. *(Langlands-Tunnell) Sea $\sigma : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ una representación continua, impar, irreducible y tal que $\sigma(G_{\mathbb{Q}})/\{\pm 1\} \subset \mathrm{PGL}_2(\mathbb{C})$ es un subgrupo soluble. Entonces existe una forma primitiva $g \in S_1^{\mathrm{new}}(\Gamma_0(N), \chi)$ (para algún entero N y un caracter χ módulo N) tal que para casi todo primo q se tiene*

$$a_q(g) = \mathrm{tr}(\sigma(\mathrm{Frob}_q)).$$

La prueba de este teorema se divide en tres casos: cuando $\sigma(G_{\mathbb{Q}})$ es isomorfo a S_4 (las simetrías del octahedro), A_4 (las simetrías del tetrahedro) y D_{2n} (el grupo dihédrico). La prueba en el caso dihédrico es debido a los trabajos de Hecke y Maass. El caso tetrahédrico es debido a Langlands y el caso octahédrico lo empezó Langlands en [Langlands, 1980] y lo terminó Tunnell en [Tunnell, 1981].

El teorema de Langlands-Tunnell es un caso particular de la conjetura de reciprocidad de Langlands porque establece una correspondencia biyectiva entre formas primitivas de peso 1 y representaciones irreducibles automorfas de peso 1 sobre $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$ (véase la sección §2.5 del capítulo de Stephen Gelbart de [Gelbart, 1997] para más detalles).

El propósito de esta sección es probar el siguiente teorema:

Teorema 100. *Sea E una curva elíptica sobre $\mathbb{Q}$. Si $\bar{\rho}_{E,3} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$ es irreducible, entonces $\bar{\rho}_{E,3}$ es modular.*

La prueba de este teorema se divide en cuatro pasos que en seguida desciribimos a grandes rasgos:

1. Levantamos la representación $\bar{\rho}_{E,3}$ a una representación $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ que sea impar, con imagen en $\mathrm{PGL}_2(\mathbb{C})$ soluble e irreducible;

2. Aplicamos el teorema de Langlands-Tunnell para obtener una forma primitiva de peso 1 asociada al levantamiento de $\bar{\rho}_{E,3}$;

3. Multiplicamos la forma primitiva por una serie de Eisenstein de peso 1 para obtener una forma cuspidal de peso 2 que, aunque no es una eigenforma, sí es una eigenforma módulo algún ideal del campo numérico de la forma primitiva del paso anterior y que contiene a $(3) \subset \mathbb{Z}$;

4. Aplicamos el lema de levantamiento de Deligne-Serre (c.f. lema 101) para obtener una genuina eigenforma asociada a $\bar{\rho}_{E,3}$ y así concluir que $\bar{\rho}_{E,3}$ es modular.

Proof. El primer paso de la demostración es levantar la representación $\bar{\rho}_{E,3}$ a una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ que sea irreducible, impar y soluble.

Primero observamos que el ideal primo $(1+\sqrt{-2}) \subset \mathbb{Z}[\sqrt{-2}]$ contiene al ideal primo $(3) \subset \mathbb{Z}$ cuya factorización en $\mathbb{Q}(\sqrt{-2})$ es $(3) = (1+\sqrt{-2})(1-\sqrt{-2})$. Con la *identidad fundamental*[1] para la factorización de ideales primos en extensiones de campos deducimos inmediatamente que el grado inercial de $(1+\sqrt{-2})$ sobre (3) es

$$\left[\frac{\mathbb{Z}[\sqrt{-2}]}{(1+\sqrt{-2})} : \frac{\mathbb{Z}}{3\mathbb{Z}}\right] = 1$$

y por lo tanto

$$\frac{\mathbb{Z}[\sqrt{-2}]}{(1+\sqrt{-2})} \cong \mathbb{F}_3.$$

Con esta expresión para $\mathbb{F}_3$ queremos definir un homomorfismo inyectivo $\Psi : \mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}])$. Para esto tomamos

$$A = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

como unos generadores de $\mathrm{GL}_2(\mathbb{F}_3)$. Se puede verificar directamente las siguientes relaciones:

checar que esa es la única relación.

$$A^3 = \mathrm{Id} \quad \text{y} \quad B^8 = \mathrm{Id}.$$

Además, estos exponentes son los enteros mínimos positivos que satisfacen estas relaciones.

Como A tiene orden tres y B tiene orden ocho, entonces la intersección $\langle A \rangle \cap \langle B \rangle = \{\mathrm{Id}\}$. Por lo tanto $\langle A \rangle \langle B \rangle = \{A^n B^m \mid 1 \leq n \leq 3, 1 \leq m \leq 8\}$ tiene 24 elementos y así $\langle A, B \rangle$ tiene al menos 24 elementos. Como $\langle A, B \rangle$ no es abeliano, tiene más de 24 elementos (e.g. $BA \in \langle A, B \rangle - \langle A \rangle \langle B \rangle$) y así, por ser subgrupo de $\mathrm{GL}_2(\mathbb{F}_3)$ que tiene 48 elementos (cf. la sección 1.1.2), $\langle A, B \rangle$ tiene 48 elementos. Por lo tanto que A y B efectivamente generan a $\mathrm{GL}_2(\mathbb{F}_3)$.

[1] La identidad fundamental es una relación numérica entre la factorización de ideales en una extensión finita de dominios de Dedekind con el grado de la extensión de sus campos de cocientes. Más precisamente, fijamos $\mathcal{O}$ un dominio de Dedekind con campo de cocientes K y sea L una extensión separable de K de grado n con $\mathcal{O}'$ la cerradura integral de $\mathcal{O}$ en L. Sea $\mathfrak{p} \subset \mathcal{O}$ un ideal primo cuya extensión en $\mathcal{O}'$ se factoriza en potencias de ideales primos como $\mathfrak{p}\mathcal{O}' = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Además escribimos $f_i := [\mathcal{O}'/\mathfrak{P}_i : \mathcal{O}/\mathfrak{p}]$ como el grado inercial de $\mathfrak{P}_i$ sobre $\mathfrak{p}$.

La identidad fundamental dice que $e_1 f_1 + \cdots + e_r f_r = n$. Si además la extensión L/K es de Galois (como el caso $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$ del texto) tenemos que $e := e_1 = \cdots = e_r$ y $f := f_1 = \cdots = f_r$ y la identidad fundamental se reduce a $n = efr$. El caso general es la proposición 8.2 de la sección 1.8 de [Neukirch, 1999], el caso cuando la extensión es de Galois viene en §1.9.

Ahora, definimos Ψ sobre los generadores como

$$\Psi(A) := A \quad , \quad \Psi(B) := \begin{pmatrix} 1 & -1 \\ -\sqrt{-2} & -1+\sqrt{-2} \end{pmatrix}.$$

Observe que

$$\Psi(B)^4 = \begin{pmatrix} 1 & -1 \\ -\sqrt{-2} & -1+\sqrt{-2} \end{pmatrix}^4 = \begin{pmatrix} 1+\sqrt{-2} & -\sqrt{-2} \\ 2 & -1-\sqrt{-2} \end{pmatrix}^2 = -\mathrm{Id}.$$

Esto implica que Ψ preserva las relaciones de los generadores de $\mathrm{GL}_2(\mathbb{F}_3)$ y así Ψ es un homorfismo de grupos.

La proyección natural $\mathbb{Z}[\sqrt{-2}] \twoheadrightarrow \mathbb{F}_3$ induce un epimorfismo $\nu : \mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}]) \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_3)$. De su definición se puede verificar que Ψ es una sección de ν y cabe en el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathrm{GL}_2(\mathbb{F}_3) & \xrightarrow{\Psi} & \mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}]) \\ & \searrow^{\mathrm{Id}} & \downarrow \nu \\ & & \mathrm{GL}_2(\mathbb{F}_3) \end{array} \tag{2.1}$$

Gracias a la conmutatividad de este diagrama podemos calcular la traza y el determinante de la representación Ψ. Si $C \in \mathrm{GL}_2(\mathbb{F}_3)$, tenemos que

$$\mathrm{tr}\big(\Psi(C)\big) \equiv \mathrm{tr}(C) \pmod{1+\sqrt{-2}}. \tag{2.2}$$

Para el determinante de Ψ tenemos la congruencia más fuerte

$$\det\big(\Psi(C)\big) \equiv \det(C) \pmod{3}, \tag{2.3}$$

que se verifica sobre los generadores y se extiende a todo $\mathrm{GL}_2(\mathbb{F}_3)$ por multiplicatividad del determinante.

Como $\mathbb{Z}[\sqrt{-2}] \subseteq \mathbb{C}$, consideramos la composición $\mathrm{GL}_2(\mathbb{F}_3) \xrightarrow{\Psi} \mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}]) \hookrightarrow \mathrm{GL}_2(\mathbb{C})$ que también denotamos por Ψ. Con esta notación definimos:

$$\rho := \Psi \circ \bar{\rho}_{E,3} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{C}).$$

Para poder aplicar el Teorema de Langlands-Tunnell necesitamos probar que ρ cumple cuatro cosas:

i) ρ es continua.

Como $\mathrm{GL}_2(\mathbb{F}_3)$ tiene la topología discreta por lo tanto Ψ es automáticamente continua. Como $\bar{\rho}_{E,3}$ también es continua, concluimos que ρ también lo es.

ii) ρ es impar.

Sea $\mathfrak{c} \in G_{\mathbb{Q}}$ la conjugación compleja. Claramente $\mathfrak{c}^2 = 1$ lo cual implica que $\rho(\mathfrak{c})^2 = \mathrm{Id}$ y así $\det(\rho(\mathfrak{c}))$ satisface la ecuación $x^2 - 1 = 0$. Por lo tanto $\det(\rho(\mathfrak{c})) = \pm 1$.

Por otro lado, (2.3) nos dice que

$$\det\big(\rho(\mathfrak{c})\big) = \det\big(\Psi\big(\bar{\rho}_{E,3}(\mathfrak{c})\big)\big) \equiv \det\big(\bar{\rho}_{E,3}(\mathfrak{c})\big) \pmod{3},$$

pero por el corolario 91 sabemos que $\det \bar{\rho}_{E,3} = \bar{\chi}_3$, el caracter ciclotómico módulo 3. Como $\bar{\chi}_3$ es el caracter inducido por la acción de $G_{\mathbb{Q}}$ sobre $\mathbb{Q}(e^{2\pi i/3})$ tenemos que $\bar{\chi}_3(\mathfrak{c})$ actúa como conjugación compleja y así $\bar{\chi}_3(\mathfrak{c}) = -1 \in (\mathbb{Z}/3\mathbb{Z})^*$. Por lo tanto

$$\det\big(\rho(\mathfrak{c})\big) \equiv \bar{\chi}_3(\mathfrak{c}) = -1 \pmod 3.$$

Como ya teníamos que $\det(\rho(\mathfrak{c})) = \pm 1$, la congruencia anterior implica que $\det(\rho(\mathfrak{c})) = -1$ porque $1 \not\equiv -1 \pmod 3$. Por lo tanto ρ es impar.

iii) ρ es soluble.

Primero afirmamos que

$$\mathrm{PGL}_2(\mathbb{F}_3) := \frac{\mathrm{GL}_2(\mathbb{F}_3)}{\{\mathrm{Id}, -\mathrm{Id}\}} \cong S_4 \tag{2.4}$$

donde S_4 es el grupo de permutaciones de un conjunto de cuatro elementos.

La acción natural $\mathrm{GL}_2(\mathbb{F}_3) \curvearrowright \mathbb{P}^1(\mathbb{F}_3)$ no es fiel pues las matrices escalares actúan trivialmente, es decir el núcleo de esta acción contiene a $\{\mathrm{Id}, -\mathrm{Id}\}$ (aquí, los únicos escalares son 1 y -1).

Ahora probamos que no hay otras matrices en el núcleo. Supongamos que $A = (a_{ij}) \in \mathrm{GL}_2(\mathbb{F}_3)$ fija a todos los elementos $[x, y] \in \mathbb{P}^1(\mathbb{F}_3)$. En particular fija a la base $\{(1, 0), (0, 1)\}$ de $\mathbb{F}_3 \times \mathbb{F}_3$. De esta manera obtenemos las siguientes fórmulas:

$$[1, 0] = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = [a_1, a_3],$$
$$[0, 1] = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = [a_2, a_4].$$

Éstas implican que $a_3 = 0 = a_2$ y $|a_1| = 1 = |a_4|$. Supongamos que a_1 y a_4 tienen signo distinto, i.e. $a_4 = -a_1$. Con la fórmula del determinante deducimos que $1 = \det A = -a_1^2$, pero esto es imposible porque $-1 \in \mathbb{F}_3$ no es un cuadrado. Por lo tanto $a_1 = \pm 1 = a_4$ y así $A = \pm\mathrm{Id}$.

Hemos probado que el núcleo de la acción $\mathrm{GL}_2(\mathbb{F}_3) \curvearrowright \mathbb{P}^1(\mathbb{F}_3)$ es $\{\pm\mathrm{Id}\}$. Por lo tanto desciende a una acción fiel $\mathrm{PGL}_2(\mathbb{F}_3) \curvearrowright \mathbb{P}^1(\mathbb{F}_3)$. Equivalentemente, hay una homomorfismo inyectivo $\mathrm{PGL}_2(\mathbb{F}_3) \hookrightarrow S_4$ porque $\mathbb{P}^1(\mathbb{F}_3)$ tiene 4 elementos: los tres de $\mathbb{F}_3$ y un punto al infinito. Por otro lado $\mathrm{GL}_2(\mathbb{F}_3)$ tiene 48 elementos, entonces $\mathrm{PGL}_2(\mathbb{F}_3)$ tiene $48/2 = 24 = 4!$ elementos. Por lo tanto la inclusión $\mathrm{PGL}_2(\mathbb{F}_3) \hookrightarrow S_4$ es en realidad un isomorfismo.

Una vez establecido (2.4), vamos a ver que la imagen de ρ en $\mathrm{PGL}_2(\mathbb{C})$ es soluble. Como Ψ es inyectivo, podemos hacer la identificación $\mathrm{GL}_2(\mathbb{F}_3) \cong \Psi(\mathrm{GL}_2(\mathbb{F}_3)) \subset \mathrm{GL}_2(\mathbb{C})$. Por otro lado tenemos que

$$\Psi(\mathrm{GL}_2(\mathbb{F}_3)) \cap \{\lambda\mathrm{Id}\}_{\lambda\in\mathbb{C}} = \{\pm\mathrm{Id}\}.$$

En efecto, si $\lambda\mathrm{Id} \in \Psi(\mathrm{GL}_2(\mathbb{F}_3))$ entonces λ es una raíz de la unidad porque $\Psi(\mathrm{GL}_2(\mathbb{F}_3))$ es un grupo de orden finito y como $\Psi(\mathrm{GL}_2(\mathbb{F}_3)) \subset \mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}])$, esto implica que $\lambda = \pm 1$ porque $\mathbb{Z}[\sqrt{-2}]$ no contiene otras raíces de la unidad.

Por lo tanto tenemos la inclusión

$$\mathrm{PGL}_2(\mathbb{F}_3) \cong \frac{\Psi(\mathrm{GL}_2(\mathbb{F}_3))}{\{\pm\mathrm{Id}\}} \subset \frac{\mathrm{GL}_2(\mathbb{C})}{\{\lambda\mathrm{Id}\}_{\lambda\in\mathbb{C}}} = \mathrm{PGL}_2(\mathbb{C}).$$

Como $\rho = \Psi \circ \bar{\rho}_{E,3}$, entonces $\rho(G_{\mathbb{Q}})$ es un subgrupo de $\Psi(\mathrm{GL}_2(\mathbb{F}_3))$. De esta manera $\rho(G_{\mathbb{Q}})/\{\pm 1\}$ es isomorfa a un subgrupo de $\mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$, que es un grupo soluble[2]. Por lo tanto la imagen de $\rho(G_{\mathbb{Q}})$ en $\mathrm{PGL}_2(\mathbb{C})$ es soluble.

iv) ρ es irreducible.

Supongamos que ρ es una representación reducible. Como $G_{\mathbb{Q}}$ es compacto y ρ es una representación de dimensión 2, ρ se descompone como suma de representaciones irreducibles de dimensión 1[3] Esto implica que $\rho(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\mathbb{C})$ es un subgrupo abeliano. En efecto, si escribimos $\rho = \rho_1 \oplus \rho_2$, entonces después de elegir una base adecuada, tenemos

$$\rho(s) = \begin{pmatrix} \rho_1(s) & 0 \\ 0 & \rho_2(s) \end{pmatrix} \qquad \forall s \in G_{\mathbb{Q}}.$$

De aquí es claro ver que $\rho(G_{\mathbb{Q}}) \subset \mathrm{GL}_2(\mathbb{C})$ es abeliano. Además como $\Psi : \mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{GL}_2(\mathbb{C})$ es inyectivo, tenemos que $\bar{\rho}_{E,3}(G_{\mathbb{Q}}) \cong \Psi(\bar{\rho}_{E,3}(G_{\mathbb{Q}})) = \rho(G_{\mathbb{Q}})$. Por lo tanto $\bar{\rho}_{E,3}(G_{\mathbb{Q}})$ es un subgrupo abeliano de $\mathrm{GL}_2(\mathbb{F}_3)$.

Ahora sea $S_0 := \rho(s_0) \in \bar{\rho}_{E,3}(G_{\mathbb{Q}})$ arbitrario. Sea λ un valor propio del endomorfismo $S_0 : \mathbb{F}_3 \times \mathbb{F}_3 \to \mathbb{F}_3 \times \mathbb{F}_3$ que podemos tomar en alguna extensión finita F de $\mathbb{F}_3$. Si consideramos a S_0 como elemento de $\mathrm{GL}_2(F)$ bajo la inclusión $\mathrm{GL}_2(\mathbb{F}_3) \subset \mathrm{GL}_2(F)$, podemos definir el endomorfismo $S_1 := S_0 - \lambda \mathrm{Id}$ de $F \times F$ y denotamos por W a su núcleo. Como λ es valor propio de S_0, entonces $W \neq 0$.

Por otro lado, para toda $s \in G_{\mathbb{Q}}$ tenemos que:

$$\begin{aligned} \bar{\rho}_{E,3}(s) \circ S_1 &= \bar{\rho}_{E,3}(s)(S_0 - \lambda \mathrm{Id}) = \bar{\rho}_{E,3}(s)S_0 - \bar{\rho}_{E,3}(s)\lambda \mathrm{Id} \\ &\overset{*}{=} S_0 \bar{\rho}_{E,3}(s) - \lambda \bar{\rho}_{E,3}(s) = (S_0 - \lambda \mathrm{Id})\bar{\rho}_{E,3}(s) \\ &= S_1 \circ \bar{\rho}_{E,3}(s), \end{aligned}$$

donde el paso (*) se sigue de que $\bar{\rho}_{E,3}(G_{\mathbb{Q}})$ es abeliano y que las matrices escalares conmutan con todas las matrices. Esta igualdad nos permite deducir que para toda $x \in W$:

$$S_1\big(\bar{\rho}_{E,3}(s)(x)\big) = \bar{\rho}_{E,3}(s)\big(S_1(x)\big) = \bar{\rho}_{E,3}(s)(0) = 0,$$

lo cual implica que $\bar{\rho}_{E,3}(s)(x) \in W$ para toda $s \in G_{\mathbb{Q}}$. Por lo tanto $W \subseteq F \times F$ es un subespacio $G_{\mathbb{Q}}-$estable bajo la representación $G_{\mathbb{Q}} \xrightarrow{\bar{\rho}_{E,3}} \mathrm{GL}_2(\mathbb{F}_3) \hookrightarrow \mathrm{GL}_2(F)$.

Ahora, como $\bar{\rho}_{E,3}$ es irreducible por hipótesis, la proposición 86 implica que $\bar{\rho}_{E,3}$ es absolutamente irreducible. En particular la representación $G_{\mathbb{Q}} \xrightarrow{\bar{\rho}_{E,3}} \mathrm{GL}_2(\mathbb{F}_3) \hookrightarrow \mathrm{GL}_2(F)$ es irreducible. Como el subespacio invariante $W = \ker S_1$ es distinto de 0, necesariamente tenmos que $W = F \times F$, i.e. $S_0 - \lambda \mathrm{Id} = 0$ o equivalentemente $\bar{\rho}_{E,3}(s_0) = \lambda \mathrm{Id}$. La elección de

[2]En efecto, $\{1\} \triangleleft \mathbb{F}_2 \times \mathbb{F}_2 \triangleleft A_4 \triangleleft S_4$ es una serie normal cuyos cocientes son abelianos.

[3]Toda representación de un grupo finito en un espacio vectorial de dimensión finita se descompone como suma directa de representaciones irreducibles. La prueba de este hecho es una aplicación elemental de inducción sobre la dimensión del espacio vectorial (c.f. [Serre, 1977a, §1.4]). Hay dos maneras de generalizar este hecho a ρ: observar que ρ se factoriza a través del cociente finito $G_{\mathbb{Q}}/\mathrm{Gal}(K_\rho|\mathbb{Q})$ (véase la nota anterior al ejemplo 82) o usar la compacidad de $G_{\mathbb{Q}}$ y la existencia de su medida de Haar para generalizar la demostración a grupos compactos no necesariamente finitos (c.f. [Serre, 1977a, §4.3]).

$s_0 \in G_{\mathbb{Q}}$ fue arbitraria, entonces podemos tomar $s_0 = \mathfrak{c}$ la conjugación compleja. Esto produce una contradicción porque $\bar{\rho}_{E,3}(\mathfrak{c})$ no puede ser una matriz escalar porque tiene valores propios distintos como habíamos establecido cuando vimos que ρ era impar. La contradicción surge de asumir que ρ era reducible, entonces concluimos que ρ es irreducible.

Después de probar estas cuatro propiedades, podemos aplicar el Teorema de Langlands-Tunnell a la representación ρ: existe una forma primitiva $g \in S_1^{\text{new}}(\Gamma_0(N), \chi)$ para alguna $N \in \mathbb{N}$ y algún caracter $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$, con serie de Fourier

$$g(z) = \sum_{n=1}^{\infty} a_n(g) e^{2\pi i n z},$$

cuyos coeficientes cumplen que, para casi todo primo q,

$$a_q(g) = \operatorname{tr}\big(\rho(\operatorname{Frob}_q)\big). \tag{2.5}$$

Recuerde que los coeficientes de Fourier de g están contenidos en su campo numérico $K_g := \mathbb{Q}(\{a_n(g), \chi(n)\}_{n\geq 1})$ que es una extensión finita de $\mathbb{Q}$. Denotamos por $\mathcal{O}_g$ al anillo de enteros de K_g. De hecho sucede algo más fuerte, los coeficientes de Fourier son enteros de K_g, i.e. $a_n(g) \in \mathcal{O}_g$ (véase la nota después de la proposición 34). Por lo tanto podemos calcular la traza y el determinante de ρ módulo algún ideal primo de $\mathcal{O}_g$ que contenga al ideal $(1+\sqrt{-2})$ (véase la congruencia (2.2)).

Sea $\mathfrak{P} \subset \mathcal{O}_g$ un ideal primo que contiene al ideal $(1+\sqrt{-2})$. Para casi todo primo q tenemos:

$$\begin{aligned} a_q(g) &= \operatorname{tr}\big(\rho(\operatorname{Frob}_q)\big) = \operatorname{tr}\big(\Psi(\bar{\rho}_{E,3}(\operatorname{Frob}_q))\big) \\ &\overset{2.2}{\equiv} \operatorname{tr}\big(\bar{\rho}_{E,3}(\operatorname{Frob}_q)\big) \pmod{1+\sqrt{-2}} \\ \therefore\quad a_q(g) &\equiv \operatorname{tr}\big(\bar{\rho}_{E,3}(\operatorname{Frob}_q)\big) \pmod{\mathfrak{P}}, \end{aligned} \tag{2.6}$$

porque $(1+\sqrt{-2}) \subseteq \mathfrak{P}$.

A primera vista parece que tenemos las condiciones suficientes de la proposición 97 para concluir que $\bar{\rho}_{E,3}$ es modular. Pero bajo mejor inspección observamos que el peso de la forma primitiva g es 1, en lugar de 2. Entonces el siguiente paso es subir el peso de g a 2 multiplicándola por una serie de Eisenstein.

En particular tomamos la serie de Eisenstein $E_{1,\psi}$ de peso 1 definida por

$$E_{1,\psi}(z) = 1 + 6\sum_{n=1}^{\infty}\sum_{d|n} \psi(d) e^{2\pi i n z},$$

donde ψ es el caracter de Dirichlet impar módulo 3, i.e. el símbolo de Legendre:

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

La razón por la cual tomamos a esta serie de Eisenstein en particular es que cumple las siguientes dos propiedades, la segunda siendo trivial:

$$E_{1,\psi} \in M_1(\Gamma_0(3), \psi) \quad \text{y} \quad a_n(E_{1,\psi}) \equiv \begin{cases} 1 \pmod 3 & n = 0 \\ 0 \pmod 3 & n > 0 \end{cases}. \tag{2.7}$$

El hecho que $E_{1,\psi}$ es modular no es trivial (véase el ejercicio 9.6.4 de [Diamond and Shurman, 2005]). Otra manera de probar la modularidad de $E_{1,\psi}$ es viendo que $E_{1,\psi}$ es la transformada de Mellin inversa de $\zeta(s)\zeta(s,\psi)$ [Wiles, 1995].

Recuerde que $M(\Gamma_0(N)) = \bigoplus M_k(\Gamma_0(N))$ es un anillo graduado por el peso y contiene al ideal $S(\Gamma_0(N)) = \bigoplus S_k(\Gamma_0(N))$ (c.f. la proposición 17.iii). Como $E_{1,\psi} \in M_1(\Gamma_0(3),\psi) \subset M_1(\Gamma_0(3N))$ (véase los primeros tres párrafos de la sección 1.1.4) y como $g \in S_1(\Gamma_0(N),\chi) \subset S_1(\Gamma_0(3N))$, entonces $gE_{1,\psi} \in S_2(\Gamma_0(3N))$; denotamos $f := gE_{1,\chi}$.

Como el nebentypus de g es χ y el nebentypus de $E_{1,\psi}$ es ψ, tenemos que $f \in S_2(\Gamma_0(3N),\chi\psi)$. En particular $\langle d\rangle f = \chi(d)\psi(d)f$ (cf. la proposición 23) o a nivel de coeficientes de Fourier:

$$a_n(\langle d\rangle f) = \chi(d)\psi(d)a_n(f) \qquad \forall d \in (\mathbb{Z}/3N\mathbb{Z})^*,\ n > 0. \tag{2.8}$$

Además, g y $E_{1,\psi}$ están normalizadas, entonces f está normalizada, i.e. $a_1(f) = 1$. Los demás coeficientes de Fourier de f se pueden calcular módulo 3 con (2.7):

$$a_n(f) = a_n(g) + \sum_{\substack{i+j=n\\ i,j>0}} a_i(g)a_j(E_{1,\chi}) \equiv a_n(g) \pmod 3 \qquad (\forall n > 1),$$

que también es válida para $n = 1$. Es decir

$$a_n(f) \equiv a_n(g) \pmod 3 \qquad (\forall n > 0). \tag{2.9}$$

Si juntamos esta congruencia con (2.6), obtenemos que para casi todo primo q se tiene

$$a_q(f) \equiv \operatorname{tr}\big(\bar\rho_{E,3}(\mathrm{Frob}_q)\big) \pmod{\mathfrak{P}}. \tag{2.10}$$

Otra vez parece que estamos en posición de aplicar la proposición 97 para concluir que $\bar\rho_{E,3}$ es modular pero inmediatamente vemos que f no necesariamente es forma primitiva. Por la elección de $E_{1,\psi}$ tenemos que, aunque f no sea una forma primitiva genuina, sí es una "eigenforma módulo $\mathfrak{P}$". Más precisamente, mediante la asignación de la serie de Fourier, podemos pensar a g como elemento del anillo de series de potencias formales $\mathcal{O}_g[[e^{2\pi iz}]]$. Similarmente $E_{1,\psi} \in \mathbb{Z}[[e^{2\pi iz}]] \subset \mathcal{O}_g[[e^{2\pi iz}]]$. Bajo esta interpretación, la congruencia (2.9) se reescribe como

$$f \equiv g \pmod{\mathfrak{P}[[e^{2\pi iz}]]}, \tag{2.11}$$

ya que $(3) \subset \mathfrak{P} \subset \mathcal{O}_g$. Entonces si aplicamos un operador de Hecke T_n, donde $(n, 3N) = 1$, a ambos lados la congruencia se preserva. En efecto, por la proposición 28 y la fórmula 2.8, los coeficientes de $T_n(f)$ cumplen:

$$\begin{aligned} a_m(T_nf) &= \sum_{d|(m,n)} d\chi(d)\psi(d)a_{nm/d^2}(f) \overset{(2.9)}{\equiv} \sum_{d|(m,n)} d\chi(d)\psi(d)a_{nm/d^2}(g) \pmod 3 \\ &\equiv \sum_{d|(m,n)} d^2\chi(d)a_{nm/d^2}(g) \equiv \sum_{d|(m,n)} \chi(d)a_{nm/d^2}(g) \\ \therefore\ a_m(T_nf) &\equiv a_m(T_ng) \pmod 3, \end{aligned}$$

donde hemos usado que $\psi(d) \equiv d \pmod 3$ y $d^2 \equiv 1 \pmod 3$ ya que $d \mid n$ y $(n, 3) = 1$. Si usamos la notación de (2.11), las congruencias anteriores se reescriben como

$$T_nf \equiv T_ng \pmod{\mathfrak{P}[[e^{2\pi iz}]]} \qquad \forall (n, 3N) = 1.$$

De esta manera:

$$T_n(f) \equiv T_n(g) = a_n(g)g \equiv a_n(g)f \pmod{\mathfrak{P}[[e^{2\pi iz}]]},$$

donde la igualdad se sigue de que los valores propios de la forma primitiva g son sus coeficientes de Fourier (cf. el teorema 33). En palabras, los coeficientes de $T_n(f)$ y de $a_n(g)f$ son iguales módulo $\mathfrak{P}$; es a esto a lo que nos referimos cuando decimos que f es una eigenforma "módulo $\mathfrak{P}$".

El siguiente y último paso es aplicar el lema de levantamiento de Deligne-Serre a f para obtener una eigenforma genuina que sea congruente a f módulo $\mathfrak{P}$ para que preserve la congruencia (2.6) que es necesaria para deducit la modularidad de $\bar{\rho}_{E,3}$. Para enunciar el lema, introducimos la notación: sea $\mathfrak{O}$ un dominio de Dedekind con un ideal maximal $\mathfrak{m}$ y cociente $k = \mathfrak{O}/\mathfrak{m}$; sean M un $\mathfrak{O}$-módulo libre de rango finito y $\mathcal{F} \subseteq \mathrm{End}_{\mathfrak{O}}(M)$ una familia de endomorfismos que conmutan dos a dos. Decimos que dos elementos $h, h' \in M$ son congruentes módulo $\mathfrak{m}$, denotado de la manera usual, si sus imágenes en $M/\mathfrak{m}M$ son iguales.

Lema 101. *(Deligne-Serre) Si $f \in M - \{0\}$ es tal que $Tf \equiv a_T f \pmod{\mathfrak{m}}$ para toda $T \in \mathcal{F}$, i.e. es un vector propio módulo $\mathfrak{m}$ para todo endomorfismo de $\mathcal{F}$, entonces existe un dominio de Dedekind $\mathfrak{O}'$ y un ideal primo $\mathfrak{m}' \subset \mathfrak{O}'$ tal que $\mathfrak{O} \subseteq \mathfrak{O}'$, $\mathfrak{m} = \mathfrak{O} \cap \mathfrak{m}'$ y el campo de fracciones de $\mathfrak{O}'$ es una extensión finita del campo de fracciones de $\mathfrak{O}$; además existe un elemento $f' \in \mathfrak{O}' \otimes_{\mathfrak{O}} M$ distinto de cero tal que $Tf' = a'_T f'$ para toda $T \in \mathcal{F}$ y tal que $a_T \equiv a'_T \pmod{\mathfrak{m}'}$.*

Nota. El lema original está enunciado para $\mathfrak{O}$ un anillo de valoración discreta pero la prueba es fácilmente adaptada para dominios de Dedekind porque localmente, éstos son anillos de valoración discretas.

Aplicamos el lema con $\mathfrak{O} = \mathcal{O}_g$, $\mathfrak{m} = \mathfrak{P}$, $M = S_2(\Gamma_0(3N), \chi\psi)$, $\mathcal{F} = \{T_n \mid (n, 3N) = 1\}$ y $f = gE_{1,\psi}$. Obtenemos una extensión de anillos $\mathcal{O}_g \subseteq \mathcal{O}$, un ideal primo $\mathfrak{P}' \subset \mathcal{O}$ tal que $\mathfrak{P} = \mathfrak{P}' \cap \mathcal{O}_g$ y un elemento $f' \in \mathcal{O} \otimes S_2(\Gamma_0(3N), \chi\psi)$ que es eigenforma para todo operador de Hecke fuera de $3N$ cuyos valores propios $a'_{T_n} \in \mathcal{O}$ cumplen:

$$a'_{T_n} \equiv a_n(f) \pmod{\mathfrak{P}'}. \tag{2.12}$$

Como f' es eigenforma sus valores propios son sus coeficientes de Fourier (cf. el teorema 33). Además, como $\mathfrak{P} \subset \mathfrak{P}'$, podemos juntar las congruencias (2.10) y (2.12) para concluir que para casi todo primo q (que además cumple $q \nmid N$) tenemos:

$$a_q(f') = a'_{T_q} \equiv a_q(f) \equiv \mathrm{tr}(\bar{\rho}_{E,3}(\mathrm{Frob}_q)) \pmod{\mathfrak{P}'}.$$

Finalmente tenemos las condiciones suficientes para aplicar la proposición 97 para concluir que $\bar{\rho}_{E,3}$ es modular. Por lo tanto lo último que falta es probar el lema de levantamiento de Deligne-Serre que hacemos a continuación. □

Demostración del lema 101. Sea $\mathcal{H}$ la $\mathfrak{O}$-subálgebra de $\mathrm{End}_{\mathfrak{O}}(M)$ generada por $\mathcal{F}$. Como M es libre de rango finito, entonces $\mathrm{End}_{\mathfrak{O}}(M)$ es libre de rango finito, y así $\mathcal{H}$ es un $\mathfrak{O}$-módulo libre de rango finito, en particular es un módulo plano[4].

Ahora, definimos $\varepsilon : \mathcal{H} \to k$ como el morfismo de $\mathfrak{O}-$álgebras que asigna valores propios, es decir definimos ε sobre los generadores de $\mathcal{H}$ como

$$\varepsilon(T) := a_T + \mathfrak{m} \qquad (\forall T \in \mathcal{F})$$

[4]Un $\mathfrak{O}-$módulo $\mathcal{H}$ es plano si el funtor $N \mapsto N \otimes \mathcal{H}$ es exacto izquierdo (recuerde que este funtor siempre es exacto derecho). Gracias a que el producto tensorial y la suma directa conmutan, todo módulo libre es plano.

Observa que por construcción $\varepsilon|_{\mathfrak{O}} = \mathrm{Id}_{\mathfrak{O}}$, entonces ε es sobreyectivo. Por lo tanto $\mathcal{H}/\ker\varepsilon \cong k$ y así $\ker\varepsilon \subset \mathcal{H}$ es un ideal maximal.

Sea $\mathfrak{p} \subseteq \ker\varepsilon$ un ideal primo minimal. La existencia de primos minimales del anillo se sigue de la existencia de conjuntos multiplicativamente cerrados maximales. Más precisamente, si A es cualquier anillo y Σ es la familia de subconjuntos de A multiplicativamente cerrados que no contienen al 0, entonces por el lema de Zorn, Σ tiene elementos maximales y además $S \in \Sigma$ es maximal si y solo si $A - S$ es un ideal primo minimal con respecto de otros ideales primos (véase el ejercicio 3.6 de [Atiyah and Macdonald, 1994, §3]). Por lo tanto si aplicamos estos resultados a la localización de $\mathcal{H}$ en el ideal $\ker\varepsilon$, concluimos que existen ideales primos minimales contenidos en $\ker\varepsilon$.

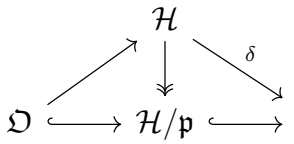
Como $\mathfrak{p}$ es minimal, todo sus elementos distintos de cero son divisores de cero. En efecto: si denotamos al conjunto de divisores del cero junto con el mismo 0 por D y suponemos que $\mathfrak{p} \nsubseteq D$ entonces $\mathcal{H} - D \nsubseteq \mathcal{H} - \mathfrak{p}$; tomamos $h \in \mathcal{H} - D$ tal que $h \notin \mathcal{H} - \mathfrak{p}$. Como $1 \in \mathcal{H} - \mathfrak{p}$ concluimos que $h = h \cdot 1 \in (\mathcal{H} - D)(\mathcal{H} - \mathfrak{p})$ y así el conjunto multiplicativamente cerrado $(\mathcal{H} - D)(\mathcal{H} - \mathfrak{p})$ contiene estictamente al conjunto multiplicativo maximal $\mathcal{H} - \mathfrak{p}$. Esto es una contradicción. Por lo tanto $\mathfrak{p} \subseteq D$.

Como $\mathcal{H}$ es un $\mathfrak{O}$-módulo libre, para toda $x \in \mathfrak{O}$ el endomorfismo $h \mapsto xh$ de $\mathcal{H}$ se representa por la matriz diagonal $x\mathrm{Id}_M$ cuyo determinante es una potencia de x que (salvo en el caso $x = 0$) es distinto de cero porque $\mathfrak{O}$ es un dominio entero. En particular $h \mapsto xh$ es inyectiva para toda $x \in \mathfrak{O} - \{0\}$. Por lo tanto $\mathfrak{O}$ no tiene divisores de cero en $\mathcal{H}$ y así $\mathfrak{p} \cap \mathfrak{O} = 0$.

De esta manera la composición $\mathfrak{O} \to \mathcal{H} \twoheadrightarrow \mathcal{H}/\mathfrak{p}$ es inyectiva; por lo tanto podemos considerar a $\mathfrak{O}$ como un subanillo de $\mathcal{H}/\mathfrak{p}$. Además, como $\mathcal{H}$ es un $\mathfrak{O}$-módulo finitamente generado, entonces $\mathcal{H}/\mathfrak{p}$ también es un $\mathfrak{O}$-módulo finitamente generado. Como $\mathfrak{O}$ es un anillo noetheriano (por ser dominio de Dedekind), entonces $\mathcal{H}/\mathfrak{p}$ es un $\mathfrak{O}$-módulo noetheriano, i.e. todos sus submódulos son finitamente generados (véase por ejemplo la proposición 1.4 de [**?**])

Este comentario sirve para probar que $\mathcal{H}/\mathfrak{p}$ es una extensión entera de $\mathfrak{O}$. En efecto, si tomamos $T + \mathfrak{p} \in \mathcal{H}/\mathfrak{p}$ arbitrario, entonces como $\mathfrak{O}[T + \mathfrak{p}] = \mathfrak{O}[T] + \mathfrak{p} \subseteq \mathcal{H}/\mathfrak{p}$, tenemos que $\mathfrak{O}[T + \mathfrak{p}]$ es un $\mathfrak{O}$-módulo finitamente generado para toda $T + \mathfrak{p} \in \mathcal{H}/\mathfrak{p}$. Esto es una condición equivalente a ser entero sobre $\mathfrak{O}$ (cf. la proposición 5.1 de [Atiyah and Macdonald, 1994]), por lo tanto $T + \mathfrak{p}$ es entero sobre $\mathfrak{O}$ para toda $T + \mathfrak{p} \in \mathcal{H}/\mathfrak{p}$.

Ahora, sea L el campo de fracciones del dominio entero $\mathcal{H}/\mathfrak{p}$ y $\mathfrak{O}_L$ la cerradura entera de $\mathfrak{O}$ en L. Esto hace que $\mathfrak{O}_L$ sea un dominio de Dedekind (cf. la proposición 8.1 de §1.8 en [Neukirch, 1999]). Como $\mathfrak{O} \subseteq \mathcal{H}/\mathfrak{p}$ es una extensión entera, tenemos que $\mathcal{H}/\mathfrak{p} \subseteq \mathfrak{O}_L$. Con esto definimos $\delta : \mathcal{H} \to \mathfrak{O}_L$ como la composición de $\mathcal{H} \twoheadrightarrow \mathcal{H}/\mathfrak{p} \hookrightarrow \mathfrak{O}_L$ y denotamos $a'_T := \delta(T)$ para toda $T \in \mathcal{F}$. Resumimos estos dos párrafos con el siguiente diagrama conmutativo:



Como $\ker\varepsilon \subset \mathcal{H}$ es un ideal maximal que contiene a $\mathfrak{p}$, entonces $\ker\varepsilon + \mathfrak{p} \subset \mathcal{H}/\mathfrak{p}$ es un ideal maximal. Sea $\mathfrak{m}' \subset \mathfrak{O}_L$ un ideal primo divisor del ideal $(\ker\varepsilon + \mathfrak{p})\mathfrak{O}_L$, en particular $\mathfrak{m}' \cap \mathcal{H}/\mathfrak{p} = \ker\varepsilon + \mathfrak{p}$ y además, como $\mathfrak{O}_L$ es un dominio de Dedekind, $\mathfrak{m}'$ también es maximal. Por lo tanto, del diagrama anterior tenemos

$$\delta(\ker\varepsilon) \subseteq \mathfrak{m}'. \tag{2.13}$$

Esto último nos garantiza que $a'_T \equiv a_T \pmod{\mathfrak{m}'}$, porque las igualdades $\varepsilon(T - a_T\mathrm{Id}_M) = \varepsilon(T) - a_T + \mathfrak{m} = 0 + \mathfrak{m}$ para toda $T \in \mathcal{F}$ implican que $T - a_T\mathrm{Id}_M \in \ker\varepsilon$ y por lo anterior tenemos que:

$$\delta(T - a_T\mathrm{Id}_M) = a'_T - a_T \in \mathfrak{m}' \quad \Longrightarrow \quad a'_T \equiv a_T \pmod{\mathfrak{m}'} \tag{2.14}$$

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

$$\mathcal{H} \cong \mathfrak{O} \otimes_{\mathfrak{O}} \mathcal{H} \hookrightarrow L \otimes_{\mathfrak{O}} \mathcal{H}.$$

Observe que $L \otimes M$ es un $L \otimes \mathcal{H}$-módulo finitamente generado con la acción $(\lambda \otimes T)(\mu \otimes f) = (\lambda\mu \otimes Tf)$. En efecto, M es finitamente generado y libre sobre sobre $\mathcal{O}$, entonces es finitamente generado sobre $\mathcal{H}$. Como hacer producto tensorial con L conmuta con la suma directa, $L \otimes M$ es finitamente generado sobre $L \otimes \mathcal{H}$.

Sea $\mathfrak{P} \subseteq L \otimes \mathcal{H}$ el ideal generado por la imagen de $\mathfrak{p}$ bajo la inclusión $\mathcal{H} \subset L \otimes \mathcal{H}$ (note que $\mathfrak{P}$ no necesariamente es primo). Como $\mathcal{H}$ es un $\mathfrak{O}$-módulo noetheriano, $\mathfrak{p}$ es un ideal finitamente generado por algunas $\{T_1, \ldots, T_n\} \subset \mathfrak{p}$. Por lo tanto $\mathfrak{P}$ es un ideal de $L \otimes \mathcal{H}$ finitamente generado por $\{1 \otimes T_1, \ldots, 1 \otimes T_n\}$. Como $\mathfrak{p}$ consta de puros divisores de cero, existen $T'_1, \ldots, T'_n \in \mathcal{H} - \{0\}$ tales que $T_iT'_i = 0$ para toda $i = 1, \ldots, n$. Además, para cada $1 \otimes T_i \in \mathfrak{P}$ toma un $f_i \in M$ tal que $T'_i(f_i) \neq 0$. De esta manera

$$(1 \otimes T_i)(1 \otimes T'_i(f_i)) = (1 \otimes T_i(T'_i(f_i))) = 1 \otimes 0 = 0.$$

Por lo tanto todos los generadores de $\mathfrak{P}$ son divisores de cero de $L \otimes M$ como $L \otimes \mathcal{H}$-módulo y así $\mathfrak{P} \subseteq D'$ donde D' es el conjunto de divisores de cero de $L \otimes M$.

El conjunto de los divisores de cero de un módulo finitamente generado (junto con el cero) es la unión de los ideales primos asociados[5] al módulo [Eisenbud, 2004, teorema 3.1, pg 89]. Por lo tanto si denotamos al conjunto de ideales primos asociados de $L \otimes M$ como $\mathcal{A} = \mathrm{Ass}_{L\otimes\mathcal{H}}(L \otimes M)$ tenemos que

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

Por el teorema de "Prime Avoidence" (véase por ejemplo la proposición 1.11 de [?]), $\mathfrak{P}$ está contenido en algún $\mathfrak{q} \in \mathcal{A}$. Por lo tanto existe un elemento $h = \sum_i \mu_i \otimes h_i \in L \otimes M - \{0\}$ tal que $\mathfrak{q}$ es su anulador, es decir $\mathfrak{P} \subseteq \mathfrak{q} = (h : 0)$.

Sea $T \in \mathcal{H}$, tengo que probar $\mathcal{H} \cong \mathfrak{p} \oplus \mathcal{H}/\mathfrak{p}$, asi $T = x + \delta(T)\mathrm{Id}$ (usa el diagrama conmutativo para calcular el factor de $\mathcal{H}/\mathfrak{p}$). Cuando extendemos a $T : L \otimes M \to L \otimes M$ obtenemos $T = X + \delta(T)\mathrm{Id}_{L\otimes M}$. Aplicamos T a h y ya. □

2.2 El truco "3-5"

En esta sección estudiamos las propiedades aritméticas de la curva elípitica $X_0(15)$ para probar:

Teorema 102. *Sea $E/\mathbb{Q}$ una curva elíptica. Si $\bar{\rho}_{E,3}$ y $\bar{\rho}_{E,5}$ son reducibles, entonces E es modular.*

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

Este teorema es la primera parte de la estrategia que usó Wiles para poder reducir el problema de probar la modularidad de una representación $\bar{\rho}_{E,\ell}$ a probar la modularidad de $\bar{\rho}_{E,3}$. Si $\bar{\rho}_{E,3}$ es irreducible, aplicamos el teorema de Langlands-Tunnell como vimos en la sección 2.1. Si $\bar{\rho}_{E,3}$ no es irreducible, Langlands-Tunnell no se puede aplicar, pero lo que dice el teorema 102 es que podemos asumir que $\bar{\rho}_{E,5}$ es irreducible. Este nuevo dato nos va a permitir construir una familia de curvas elípticas, todas con la misma representación módulo 5, que contiene al menos una curva E' cuya representación $\bar{\rho}_{E',3}$ es irreducible.

Para justificar esta nueva vía, necesitamos el teorema 102. La estrategia de probarlo es parametrizar la familia de curvas elípticas tales que $\bar{\rho}_{E,3}$ y $\bar{\rho}_{E,5}$ reducibles, con los cuatro puntos racionales de $X_0(15)$ no cuspidales, i.e. $Y_0(15)(\mathbb{Q})$. Cada punto corresponde a una clase de isomorfismo de curvas elípticas cuyos isomorfismos preservan un subgrupo cíclico de orden 15. Con esta descripción de las curvas elípticas con $\bar{\rho}_{E,3}$ y $\bar{\rho}_{E,5}$ reducibles, es posible asociarles una forma primitiva en $S_2(\Gamma_0(50))$ y así probar la modularidad de esas curvas elípticas.

El primer paso es probar:

Lema 103. *Si E es una curva elíptica sobre $\mathbb{Q}$ tal que $\bar{\rho}_{E,3}$ y $\bar{\rho}_{E,5}$ son reducibles, entonces $E(\overline{\mathbb{Q}})$ contiene un subgrupo cíclico de orden 15 que es estable bajo la acción de $G_{\mathbb{Q}}$.*

Proof. Supongamos que $\bar{\rho}_{E,3}$ y $\bar{\rho}_{E,5}$ son reducibles. Por definición existen subespacios no triviales $V_3 \subset E[3]$ y $V_5 \subset E[5]$ que son invariantes bajo la acción de $G_{\mathbb{Q}}$. Recuerda que $\#E[N] = N^2$, entonces el orden de cualquier subgrupo divide a N^2, pero en este caso $N = 3, 5$. Por lo tanto cualquier subgrupo no-trivial de $E[3]$ (respectivamente $E[5]$) necesariamente es de orden 3 (respectivamente 5). En particular $V_i \cong \mathbb{Z}/i\mathbb{Z}$ para $i = 3, 5$ y sean P_3 un generador de V_3 y P_5 un generador de V_5. Por último, como subgrupos de $E(\overline{\mathbb{Q}})$, V_3 y V_5 tienen intersección trivial (porque los elementos distintos del neutro de V_3 tienen orden 3 y los de V_5 tienen orden 5).

Ahora definimos $V = V_3 + V_5 = \{P + P' \in E(\overline{\mathbb{Q}}) \mid P \in E[3],\ P' \in E[5]\}$. Claramente el orden de cada punto de V divide a 15 pues $15(P + P') = 5(3P) + 3(5P') = 3O + 5O = O$, es decir $V \subset E[15]$. Por otro lado el punto $P_3 + P_5$ es de orden exactamente 15 porque

$$3(P_3 + P_5) = 3P_5 \neq O \quad \text{y} \quad 5(P_3 + P_5) = 5P_3 = 2P_3 \neq O.$$

Por lo tanto V es un subgrupo de $E(\overline{\mathbb{Q}})$ de orden 15.

Por último, V es invariante bajo la acción de $G_{\mathbb{Q}}$. En efecto, sea $\sigma \in G_{\mathbb{Q}}$ arbitrario, entonces

$$(P + P')^{\sigma} = P^{\sigma} + P'^{\sigma} \in V_3 + V_5 = V$$

ya que la $G_{\mathbb{Q}}$-estabilidad de V_3 (respectivamente de V_5) implica que $P^{\sigma} \in V_3$ (respectivamente $P'^{\sigma} \in V_5$). Por lo tanto $E(\overline{\mathbb{Q}})$ contiene un subgrupo de orden 15 estable bajo la acción de $G_{\mathbb{Q}}$. □

Este lema nos dice que las curvas elípticas E con $\bar{\rho}_{E,3}$ y $\bar{\rho}_{E,5}$ reducibles tiene subgrupos cíclicos de orden 15. Vimos en §1.2.3 que las clases de isomorfismos $[E, C]$ de curvas elípticas con subgrupos cíclicos fijos C de orden N son parametrizados por los puntos racionales no cuspidales de $X_0(N)$, i.e. $Y_0(N)(\mathbb{Q})$. Por lo tanto si $E/\mathbb{Q}$ es una curva elíptica con $\bar{\rho}_{E,3}$ y $\bar{\rho}_{E,5}$ reducibles, su clase de isomorfismo $[E, C] \in S_0(15)(\mathbb{Q})$ (donde C es el subgrupo dado por el lema 103) corresponde a un punto racional no cuspidal en $X_0(15)(\mathbb{Q})$. Esta asignación nos permite ver cómo tiene que ser E y concluir que efectivamente es modular.

El siguiente paso es encontrar una ecuación de Weierstrass para la curva elíptica $X_0(15)$ para calcular sus puntos racionales. La ecuación de Weierstrass de $X_0(15)$ lo calculó Fricke en su obra

celebrada *Die Elliptischen Funktionen Und Ihere Anwendungen* en 1922. En el teorema 60 vimos que para encontrar una ecuación de Weierstrass bastaba exhibir dos funciones $x, y \in \mathbb{C}(X_0(N))$, tales que x y y solamente tienen polos en ∞ de orden 2 y 3 respectivamente. Por la prueba del teorema 60, las funciones $\{1, x, y, x^2, xy, y^2, x^3\}$ satisfacen una $\mathbb{C}-$combinación lineal que resulta ser una ecuación de Weierstrass. Esta ecuación define una curva elíptica sobre $\mathbb{C}$ isomorfa a $X_0(15)$.

El método que seguimos es debido a Gerard Ligozat, un alumno de Nerón, que en su tesis doctoral calcula las ecuaciones de Weierstrass y los invariantes de las curvas modulares $X_0(N)$ de género 1, i.e. para $N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$ [Ligozat, 1975]. Además calculó otros invariantes como el conductor y el rango de las curvas $X_0(N)$ y con estos cálculos, Ligozat pudo verificar la conjetura de Birch y Swinnerton-Dyer para las curvas modulares elípticas. Ligozat generalizó un método desarrollado por Morris Newmann en los años 50 para construir sistemáticamente funciones meromorfas sobre $X_0(N)$.

Para construir $x, y \in \mathbb{C}(X_0(15))$ usaremos la función η de Dedekind definida por

$$\eta(z) := e^{2\pi i z/24} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z}) = \sum_{n=1}^{\infty} \left(\frac{n}{12}\right) q^{n^2/24}, \tag{2.15}$$

donde $(n/12)$ es el símbolo de Legendre. Observe que $\eta(z)$ está definido sobre $\mathbb{H}$ por un producto convergente cuyos factores no se anulan, por lo tanto $\eta(z) \neq 0$ para toda $z \in \mathbb{H}$.

Más precisamente, usamos $\eta-$*cocientes*, i.e. funciones holomorfas $H : \mathbb{H} \to \mathbb{C}$ de la forma

$$\prod_{0<d|N} \eta(dz)^{r_d} \quad (r_d \in \mathbb{Z}).$$

Al conjunto de exponentes $\{r_d\}$, indexados por los divisores positivos de N, lo denotamos $\mathbf{r} := \{r_d \in \mathbb{Z} \mid d > 0,\ d \mid N\}$. Por lo tanto, el $\eta-$*cociente asociado a* $\mathbf{r}$ lo definimos como:

$$\eta_{\mathbf{r}} : \mathbb{H} \longrightarrow \mathbb{C} \quad \text{definido por} \quad \eta_{\mathbf{r}}(z) = \prod_{\substack{d|N \\ d>0}} \eta(dz)^{r_d}$$

El discriminante modular Δ y las funciones de Fricke, e.g. (2.17), son ejemplos de $\eta-$cocientes.

Newmann probó que bajo ciertas condiciones sobre el conjunto $\mathbf{r}$, la función holomorfa $\eta_{\mathbf{r}}$ era débilmente modular con respecto de $\Gamma_0(N)$; el caso $(N, 6) = 1$ aparece en [Newman, 1956] (véase el teorema 1) y el caso $(N, 6) > 1$, e.g. $N = 15$, aparece en la segunda parte [Newman, 1958]. Ligozat aumentó las condiciones de Newmann para caracterizar cuándo un $\eta-$cociente define una función meromorfa sobre $X_0(15)$. Enunciamos este resultado

Teorema 104. *(Ligozat) Sea N fijo y sea $\eta_{\mathbf{r}}$ un $\eta-$cociente. Entonces $\eta_{\mathbf{r}}$ define una función meromorfa sobre $X_0(N)$ si y solo si el conjunto de exponentes $\mathbf{r}$ satisface las siguientes condiciones:*

(i) $\sum r_d d \equiv 0 \pmod{24}$,

(ii) $\sum N r_d/d \equiv 0 \pmod{24}$

(iii) $\sum r_d = 0$,

(iv) $\prod (N/d)^{r_d} = \frac{a^2}{b^2}$ *donde* $a, b \in \mathbb{Z}$.

donde las sumas y el producto se hacen sobre los divisores positivos de N.

Proof. Véase la proposición 3.2.1 de [Ligozat, 1975]. Para probar la necesidad, curiosamente aparece el teorema de reciprocidad cuadrática. □

Este resultado nos permite construir funciones meromorfas sobre $X_0(15)$ de manera sistemática. Esto nos va a permitir encontrar generadores para el campo de funciones de $X_0(15)$ y así encontrarle una ecuación de Weierstrass:

Lema 105. *La curva elíptica $X_0(15)$ sobre $\mathbb{C}$ es isomorfa a la curva $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ definida por los ceros de la homogenización de la ecuación*

$$Y^2 + XY + Y = X^3 + X^2 - 10X - 10. \tag{2.16}$$

Proof. Primero aplicamos el resultado de Ligozat para construir tres funciones en $\mathbb{C}(X_0(15))$ y a partir de éstas, definimos x y y. Por último probaremos que x y y satisfacen (2.16) mediante comparaciones de series de Fourier.

En seguida exhibimos tres conjuntos de exponentes $\mathbf{r} = \{r_1, r_3, r_5, r_{15}\}$ que satisfacen las condiciones del teorema 104 junto con sus series de Fourier que se pueden calcular a partir de (2.15):

$$\begin{aligned}
\mathbf{r}_1 &= \{-1, 1, 5, -5\}, \quad \eta_{\mathbf{r}_1}(z) = q^{-2} + q^{-1} + 2 + 2q + 4q^2 + \cdots \\
\mathbf{r}_2 &= \{7, -1, 1, -7\}, \quad \eta_{\mathbf{r}_2}(z) = q^{-4} - 7q^{-3} + 7q^{-2} + 8q^{-1} - 56 + 34q + 51q^2 + \cdots \\
\mathbf{r}_3 &= \{2, 4, 2, -8\}, \quad \eta_{\mathbf{r}_3}(z) = q^{-4} - 2q^{-3} - q^{-2} - 2q^{-1}9 + 4q - 4q^2 + \cdots
\end{aligned}$$

Con estas tres funciones meromorfas sobre $X_0(15)$, definimos:

$$x(z) := \eta_{\mathbf{r}_1}(z) - 2 \quad \text{y} \quad y(z) := \frac{1}{5}(\eta_{\mathbf{r}_3}(z) - \eta_{\mathbf{r}_2}(z)) + 3\eta_{\mathbf{r}_1}(z) - 19.$$

La combinación lineal que define a y es para cancelarle el polo de $\eta_{\mathbf{r}_3}$ en ∞ de orden 4 para que quede un polo de orden 3. En efecto la serie de Fourier de y es:

corregir serie de Fourier de y

$$y(z) = q^{-3} + q^{-1} + q^2 + 6q^3 + \cdots$$

Por el teorema 60, el conjunto de funciones meromorfas $\{1, x, y, x^2, xy, y^2, x^3\}$ es linealmente dependiente como subconjunto del sistema lineal $\mathcal{L}(6\infty)$, entonces satisfacen una relación de dependencia no trivial con coeficientes en $\mathbb{C}$, i.e. existen $A_1, \ldots, A_7 \in \mathbb{C}$, no todos cero tales que:

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0$$

Como solamente necesitamos siete coeficientes, solamente tenemos que calcular las series de Fourier de $\{1, x, y, x^2, xy, y^2, x^3\}$ hasta orden siete para poder calcular las A_i. De esta manera podemos deducir los valores de las A_i y con el cambio de variable (1.46) del teorema 60 obtenemos la ecuación de Weierstrass buscada:

$$y^2 + xy + y = x^3 + x^2 - 10x - 10.$$

Otra vez por el teorema 60 concluimos que $X_0(15) \cong \mathcal{C}$ donde $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ es la curva proyectiva definida por la ecuación anterior. □

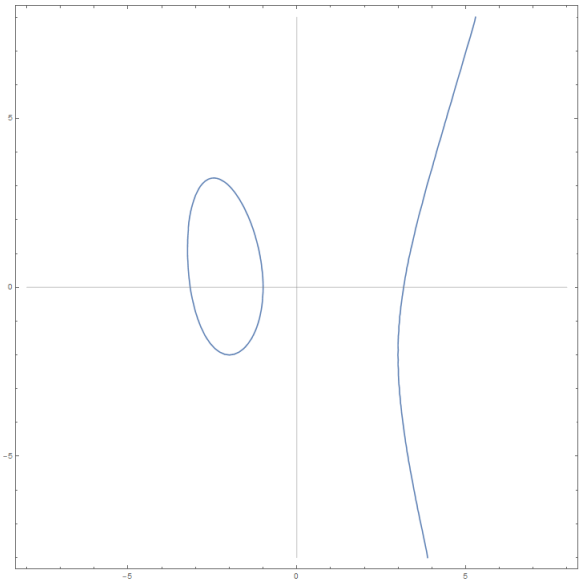


Figure 2.1: La curva real definida por la ecuación $Y^2 + XY + Y = X^3 + X^2 - 10X - 10$.

Nota. Lo que hizo Fricke para calcular una ecuación de $X_0(15)$ fue un poco distinto. Él definió el $\eta-$cociente

$$x(z) := \frac{\eta(3z)^3\eta(5z)^3}{\eta(z)^3\eta(15z)^3} = q^{-2} + 3 + 9q^2 + O(q^4). \tag{2.17}$$

Una vez definida x, Fricke considera un múltiplo adecuado de la derivada de x y lo llama y. De esta manera obtiene el segundo generador de $\mathbb{C}(X_0(15))$ como $\mathbb{C}-$álgebra, es decir $K(X_0(15)) = \mathbb{C}(x, y)$. Después, Fricke calcula y compara coeficientes de Fourier para encontrar la relación algebraica entre x y y que resulta ser:

$$y^2 = x^4 - 10x^3 - 13x^2 + 10x + 1. \tag{2.18}$$

Véase [Fricke, 1922, página 439]. Es posible llevar (2.18) a una ecuación de Weierstrass mediante el siguiente cambio de variable:

$$x \mapsto \frac{2y + x + 46}{2(x-8)} + \frac{5}{2}, \quad y \mapsto \frac{(2y + x + 46)^2}{4(x-8)^2} - 2(x-8) - \frac{101}{4}$$

De esta manera obtenemos la ecuación de Weierstrass:

$$y^2 + xy + y = x^3 + x^2 - 10x - 10. \tag{2.19}$$

Con la ecuación de Weierstrass de $X_0(15)$ podemos calcular sus puntos racionales que denotamos por $G = X_0(15)(\mathbb{Q})$. Para esto usamos el teorema de Mordell-Weil[6] que nos dice que

$$G \cong G_{\text{tor}} \times \mathbb{Z}^r,$$

[6]Para toda curva elíptica E sobre un campo numérico K, el grupo $E(K)$ es un grupo abeliano finitamente generado (cf. teorema 6.7 del capítulo VIII de [Silverman, 2009]).

donde G_{tor} es el subgrupo de torsión y $r \geq 0$ es el rango de G. Con esta descripción de G, nuestra tarea se divide en dos: estudiar el grupo de torsión y calcular el rango. Primero calculamos el subgrupo de torsión con el teorema de Lutz-Nagell:[7]

Teorema 106. *(Lutz-Nagell) Sea $E/\mathbb{Q}$ una curva elíptica con ecuación de Weierstrass*

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}. \tag{2.20}$$

A la ecuación de Weierstrass le asociamos el entero $D := 4A^3+27B^2$, además denotamos $G = E(\mathbb{Q})$ y escribimos $x(P)$ y $y(P)$ como las coordenadas de $P \in G$ dadas por (2.20)*. Entonces para todo $P \in G_{\text{tor}}$ tenemos que $x(P), y(P) \in \mathbb{Z}$ y*

$$P + P = O \quad \acute{o} \quad y(P)^2 \mid D.$$

Este teorema lo usamos para probar:

Proposición 107. *Sea $G = X_0(15)(\mathbb{Q})$ el grupo de puntos racionales de la curva modular $X_0(15)$. Entonces G_{tor} tiene 8 elementos y son:*

$$G_{\text{tors}} = \left\{ \left(-\tfrac{13}{4}, \tfrac{9}{8}\right), (-1, 0), (3, -2), (8, -27), (8, 18), (-2, -2), (-2, 3) \right\} \cup \{O\}.$$

Proof. Para aplicar Lutz-Nagell, necesitamos transformar la ecuación de Weierstrass generalizada de $X_0(15)$ dada por el lema 105 a una ecuación simplificada. El cambio de variable es:

$$x = \frac{x'}{36} - \frac{15}{36}, \qquad y = \frac{y'}{216} - \frac{x'}{72} - \frac{21}{72} \tag{2.21}$$

y simplifica la ecuación a

$$y'^2 = x'^3 - 12987x' - 263466 = (x' + 102)(x' + 21)(x' - 123) \tag{2.22}$$

donde:

$$D = 4(-12987)^3 + 27(-263466)^2 = -(2^4 3^8 5^2)^2.$$

Ahora sea $P_0 = (x_0, y_0) \in G_{\text{tor}}$ donde las coordenadas están dadas por (2.22). Por Lutz-Nagell tenemos que $x_0, y_0 \in \mathbb{Z}$ y el punto P_0 cumple una de dos casos:

Caso 1: $P_0 + P_0 = O$.

En este caso, $P_0 = -P_0$. Por la ecuación (1.49), tenemos $-P_0 = (x_0, -y_0)$. Por lo tanto $P_0 = -P_0$ si y solo si $y_0 = 0$. Ahora sustituimos $y_0 = 0$ en (2.22) y obtenemos tres posibles valores para x_0 que corresponden a los siguientes tres puntos racionales de orden 2 en G_{tor}:

$$(-102, 0), \quad (-21, 0) \quad \text{y} \quad (123, 0)$$

[7] Aquí enunciamos la versión que aparece en VIII.7.2 de [Silverman, 2009], pero este teorema fue probado independientemente por T. Nagell y E. Lutz en los 1930's. La prueba primero apareció en [Nagell, 1935] y después en [Lutz, 1937].

Caso 2: $y(P_0)^2 \mid D$.

Si $P_0 = (x_0, y_0)$, entonces por la factorización de D, solamente tenemos que considerar coordenadas y_0 que sean divisores de $2^4 3^8 5^2 = \sqrt{-D}$. Sustituimos cada divisor en (2.22) y resolvemos la ecuación cúbica en x para obtener (o probar que no tienen) soluciones y así posibles coordenadas de P_0. Como $\sqrt{-D}$ tiene 270 divisores (positivos y negativos), este proceso lo verificamos con Mathematica y otenemos los siguientes cuatro puntos racionales:

$$(303, 4860), \quad (303, -4860), \quad (-57, -540) \quad \text{y} \quad (-57, 540)$$

Juntando ambos casos obtenemos la lista completa de puntos racionales de orden finito de la ecuación (2.22):

$$\{(-102, 0), (-21, 0), (123, 0), (303, -4860), (303, 4860), (-57, -540), (-57, 540)\} \cup \{O\}.$$

Bajo el cambio de coordenadas inverso a (2.21), dado por:

$$x' = 36x + 15, \quad y' = 216y + 108x + 108$$

podemos concluir que:

$$G_{\text{tors}} = \left\{\left(-\tfrac{13}{4}, \tfrac{9}{8}\right), (-1, 0), (3, -2), (8, -27), (8, 18), (-2, -2), (-2, 3)\right\} \cup \{O\}.$$

□

Como G_{tor} es abeliano y de orden 8, el teorema de estructura de grupos abelianos finitamente generados[8] nos dice que G_{tor} es isomorfo a uno de los siguientes tres posibilidades:

$$\mathbb{Z}/8\mathbb{Z}\mathbb{Z}, \quad , \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad \text{ó} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Para saber cual de estas tres posibilidades es la correcta, necesitamos estudiar el orden del los puntos de G_{tor}. Por suerte, la definición geométrica, nos permite calcular a vista la duplicación de los puntos de G_{tor}.

En el diagrama 2.2 graficamos los 7 puntos racionales afines sobre la curva elíptica y trazamos rectas tangentes en esos puntos. Si la recta tangente es vertical, omitimos la recta y marcamos el punto de verde; estos puntos son de orden 2. Si duplicamos el resto de los cuatro puntos, obtenemos el punto $(3, -2)$ que es de orden 2. Por lo tanto el resto de los puntos, i.e. $\{-2, 3), (-2, -2), (8, 18), (8, -27)\}$ tienen orden 4. En conclusión G_{tor} tiene tres elementos de orden 2 y cuatro de orden cuatro. Es implica que

$$G_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Para cada punto $P \in G_{\text{tor}}$ de orden 2, i.e. $P \in \{(-\frac{13}{4}, \frac{9}{8}) =, (-1, 0), (3, -2)\}$, el subgrupo generado por P actúa sobre G_{tor} mediante traslación:

$$\langle P \rangle \curvearrowright G_{\text{tor}} \quad \text{definido por} \quad (O, Q) \mapsto Q, \;\; (P, Q) \mapsto P + Q.$$

Como $\langle P \rangle$ solamente tiene dos elementos y G_{tor} tiene ocho elementos, entonces cada acción $\langle P \rangle \curvearrowright G_{\text{tor}}$ descompone G_{tor} en cuatro órbitas. En la figura 2.3 ilustramos estas particiones para cada punto de orden 2. Esos diagramas también muestran parte de la tabla de operaciones.

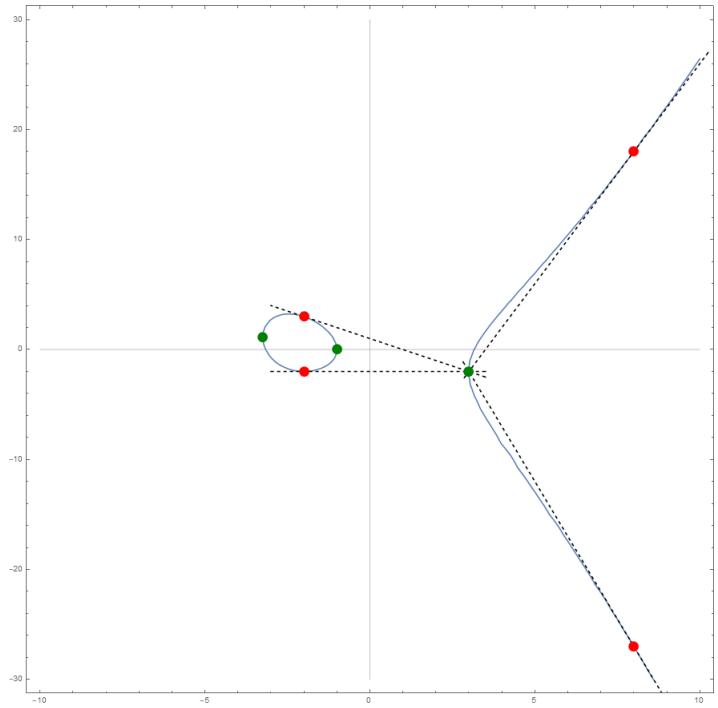


Figure 2.2: Visualización de la suplicación de los puntos racionales de $X_0(15)$. Los puntos verdes son de orden 2 y los puntos rojos son de orden 4.

Los siguientes tres diagramas representan las órbitas de G bajo la acción $O, P \curvearrowright G$ donde P corre sobre los puntos de orden 2:

El próximo paso es probar que el rango de $G \cong G_{\text{tor}} \times \mathbb{Z}^r$ es cero, i.e. $r = 0$. Para esto estudiamos el grupo $G/2G$ para encontrar una fórmula para r. El teorema de Mordell-Weil dice que G es un grupo abeliano finitamente generado y por lo tanto el teorema de estructura de grupos abelianos finitamente generados nos dice que:

$$G \cong \mathbb{Z}^r \times \frac{\mathbb{Z}}{p_1^{n_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_s^{n_s}\mathbb{Z}},$$

para algunos números primos $p_1, \ldots, p_s \in \mathbb{Z}$ y exponentes $n_i > 0$. Con esta expresión para G podemos calcular $G/2G$. En efecto, tenemos que

$$\frac{G}{2G} \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^r \times \frac{\mathbb{Z}/p_1^{n_1}\mathbb{Z}}{2\mathbb{Z}/p_1^{n_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}/p_s^{n_s}\mathbb{Z}}{2\mathbb{Z}/p_s^{n_s}\mathbb{Z}},$$

donde

$$\frac{\mathbb{Z}/p_i^{n_i}\mathbb{Z}}{2\mathbb{Z}/p_i^{n_i}\mathbb{Z}} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & p_i = 2 \\ 0 & p_i \neq 2 \end{cases}.$$

Por lo tanto $G/2G$ es un producto de $\mathbb{Z}/2\mathbb{Z}$'s. Hay r copias en la parte libre de torsión y tantas copias como potencias de 2 que aparecen en la parte de torsión, i.e.

$$(G : 2G) = 2^{r+\#\{j|p_j=2\}}. \tag{2.23}$$

[8] ●

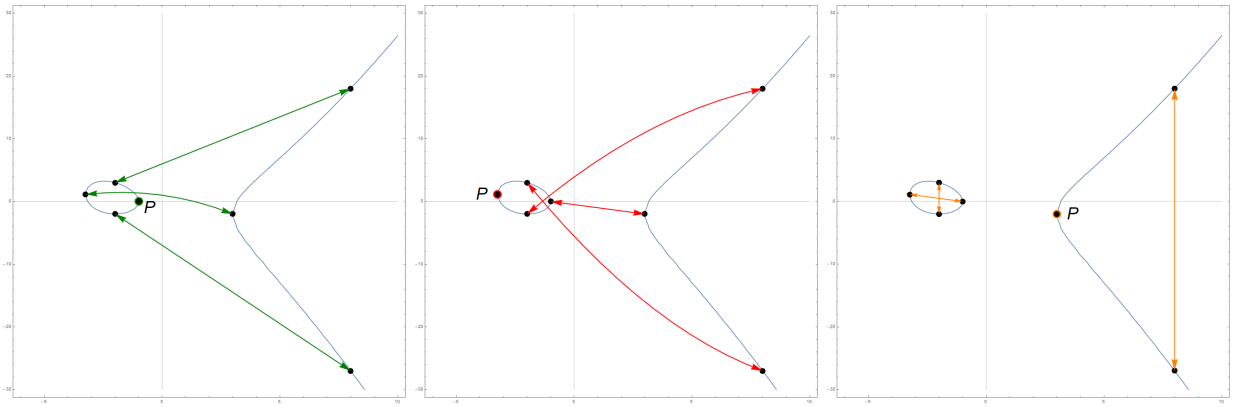


Figure 2.3: Construcción geométrica de la suma de puntos P y Q sobre una curva elíptica según si $P+Q=O$, $P\neq Q$ y $P=Q$ respectivamente.

Para calcular $2^{\#\{j|p_j=2\}}$, simplemente calculamos el núcleo del homomorfismo $[2]:G\to G$ definido por $P\mapsto P+P$; al núcleo lo denotamos por G_2. Si $P\in G$ es de la forma $P=m_1P_1+\cdots+m_rP_r+l_1Q_1+\cdots 1_sQ_s$ con $m_i\in\mathbb{Z}$ y $0\leq l_j<p_j^{n_j}$, entonces

$$\begin{aligned} P+P=O \quad &\iff \quad 2m_1P_1+\cdots+2m_rP_r+2l_1Q_1+\cdots 2l_sQ_s=0 \\ m_i=0, \quad &2l_j\equiv 0 \pmod{p_j^{n_j}} \quad \forall i,j \end{aligned}$$

Si $p_j\neq 2$, entonces 2 es invertible en $\mathbb{Z}/p_j^{n_j}\mathbb{Z}$ y por lo tanto $2l_j\equiv 0 \pmod{p_j^{n_j}}$ es equivalente a que $l_j\equiv 0 \pmod{p_j^{n_j}}$. Esto junto con los posibles valores de l_j implican que $l_j=0$ cuando $p_j\neq 2$. Por lo tanto los únicos coeficientes de P libres son las l_j's tales que $p_j=2$. En este caso los únicos dos valores son $l_j=0$ ó $l_j=2^{n_j-1}$. Por lo tanto:

$$P+P=0 \quad \iff \quad m_i=0 \quad \forall i, \quad l_j=0 \quad \forall j \text{ tal que } p_j\neq 2, \quad l_j\in\{0,2^{n_j-1}\} \quad \forall j \text{ tal que } p_j=2.$$

De esta manera el núcleo G_2 tiene $2^{\#\{j|p_j=2\}}$ elementos y por lo tanto (2.23) se convierte en

$$2^r=\frac{(G:2G)}{\#G_2}. \tag{2.24}$$

Para calcular r de la ecuación anterior, necesitamos estudiar con mayor detalle el homomorfismo $[2]:G\to G$. La clave es decomponer $[2]$ como composición de dos homomorfismos $\varphi:G\to\bar{G}$ y $\psi:\bar{G}\to G$, donde $\bar{G}$ es un grupo auxiliar. Estos homomorfismos vienen de isogenias entre curvas elípticas, en particular de $X_0(15)$. Para facilitar los cálculos nos restringimos a curvas elípticas con un punto de orden 2 trasladado al origen; por suerte $X_0(15)$ tiene puntos de orden 2.

En general, sea E una curva elíptica sobre $\mathbb{Q}$ definida por una ecuación de la forma

$$E \ : \ y^2=x^3+ax^2+bx,$$

donde $a,b\in\mathbb{Z}$ y cuyo grupo de puntos racionales denotamos por $G=E(\mathbb{Q})$. El neutro lo denotamos por O y al origen lo denotamos por $T=(0,0)$; T es un punto de orden 2. Por el caso 1 de la prueba de la proposición 107 los puntos de orden 2 son O y los puntos de la forma $P=(x,0)$. Como las coordenadas de P tienen que satisfacer la ecuación de E, tenemos que

$$0=x^3+ax^2+bx=x(x^2+ax+b).$$

Por lo tanto $a^2 - 4b$, el discriminante de la ecuación cuadrática $x^2 + ax + b = 0$, es un cuadrado perfecto si y sólo si las soluciones x_1 y x_2 de $x^2 + ax + b = 0$ son racionales. De esta manera tenemos que si $a^2 - 4b$ es un cuadrado perfecto, hay 4 puntos racionales de orden 2, i.e. $G_2 = \{O, T, (x_1, 0), (x_2, 0)\}$ y cuando $a^2 - 4b$ no es un cuadrado perfecto, $(x_1, 0), (x_2, 0) \notin G$ y por lo tanto solamente hay 2 puntos racionales de orden 2. Resumimos este hecho en la siguiente fórmula:

$$\#G_2 = \begin{cases} 4 & a^2 - 4b \text{ es un cuadrado perfecto} \\ 2 & a^2 - 4b \text{ no es un cuadrado perfecto} \end{cases}. \tag{2.25}$$

Por lo tanto ya calculamos el término $\#G_2$ de (2.24). Ahora nos falta calcular $(G : 2G)$. Para esto descomponemos el homomorfismo $[2] : G \to G$ como composición de otros dos homomorfismos, pero primero necesitamos construir una curva elíptica auxiliar asociada a E.

Para toda E podemos construir una curva elíptica $\bar{E}$ sobre $\mathbb{Q}$ definida por:

$$\bar{E} \,:\, y^2 = x^3 + \bar{a}x^2 + \bar{b}x, \quad \text{donde} \quad \bar{a} := -2a, \;\; \bar{b} := a^2 - 4b.$$

Denotamos por $\bar{G}$ al grupo de puntos racionales de $\bar{E}$ y también denotamos por $\bar{O}$ al neutro de $\bar{E}$ y $\bar{T}$ al punto $(0, 0)$ de $\bar{E}$. Observe que $\bar{b}$ es el discriminante de la ecuación cuadrática $x^2 + ax + b = 0$ y por lo tanto la fórmula (2.25) se puede reescribir según si $\bar{b}$ es cuadrado perfecto o no.

Observe que si repetimos dos veces esta construcción obtenemos la curva $\bar{\bar{E}}$ definida por la ecuación $y^2 = x^3 + 4ax^2 + 16bx$ que, bajo el cambio de variable admisible $x' = 4x$ y $y' = 8y$ obtenemos la ecuación original de E. Es decir $\bar{\bar{E}} \cong E$.

Ahora consideramos la siguiente función: $\varphi : E \to \bar{E}$ definido por:

$$\varphi(x, y) := \begin{cases} \left(\frac{y^2}{x^2}, y\frac{x^2 - b}{x^2}\right) & (x, y) \neq O, T \\ \bar{O} & (x, y) = O, T. \end{cases}$$

Si aplicamos φ a $\bar{E}$ obtenemos una función $\bar{E} \to \bar{\bar{E}}$ que bajo el isomorfismo $\bar{\bar{E}} \cong E$, obtenemos la función $\psi : \bar{E} \to E$ definida por

$$\psi(\bar{x}, \bar{y}) := \begin{cases} \left(\frac{\bar{x}^2}{\bar{y}^2}, \bar{y}\frac{\bar{x}^2 - \bar{b}}{\bar{x}^2}\right) & (\bar{x}, \bar{y}) \neq \bar{O}, \bar{T} \\ O & (\bar{x}, \bar{y}) = \bar{O}, \bar{T}. \end{cases}$$

Las funciones φ y ψ son muy útiles para estudiar la isogenia $[2] : E \to E$ ya que cumplen las siguientes propiedades:

Proposición 108. *Las funciones φ y ψ definidas arriba cumplen las siguientes propiedades:*

(i) φ y ψ están bien definidas e inducen homomorfismos de grupos $\varphi : G \to \bar{G}$ y $\psi : \bar{G} \to G$ con núcleos $\{O, T\}$ y $\{\bar{O}, \bar{T}\}$ respectivamente.

(ii) La composición de los dos homomorfismos es la multiplicación por 2, i.e. $\psi(\varphi(P)) = [2]P$ para todo $P \in G$ y $\varphi(\psi(\bar{P})) = [2]\bar{P}$ para todo $\bar{P} \in \bar{G}$. Si abusamos de notación, esto lo denotamos por

$$\psi \circ \varphi = [2] = \varphi \circ \psi.$$

(iii) $\bar{O} \in \varphi(G)$ y $O \in \psi(\bar{G})$.

(iv) $\bar{T} \in \varphi(G)$ *(resp.* $T \in \psi(\bar{G})$*) si y solo si* $\bar{b}$ *(resp.* b*) es un cuadrado perfecto.*

(v) Si $\bar{P} = (\bar{x}, \bar{y}) \in \bar{G}$ *con* $\bar{x} \neq 0$ *(resp.* $P = (x, y) \in G$*,* $x \neq 0$*), entonces*

$$\bar{P} \in \varphi(G) \ \big(\text{resp. } P \in \psi(\bar{G})\big) \quad \Longleftrightarrow \quad \bar{x} \in \mathbb{Q}^2 \ \big(\text{resp. } x \in \mathbb{Q}^2\big).$$

Proof. Véase la proposición 3.7 de [Silverman and Tate, 2009] para ver que φ y ψ están bien definidas y que cumplen (i) y (ii). Véase §3.5 de [Silverman and Tate, 2009] para la prueba de los otros dos incisos. □

Observe que el inciso (ii) garantiza que $2G = \psi(\varphi(G)) \subseteq \psi(\bar{G}) \subseteq G$. Por lo tanto tenemos que

$$(G : 2G) = (G : \psi(\bar{G}))(\psi(\bar{G}) : 2G).$$

Además, tenemos que[9]

$$(\psi(\bar{G}) : 2G) = \big(\psi(\bar{G}) : \psi(\varphi(G))\big) = \frac{(\bar{G} : \varphi(G))}{(\ker\psi : \varphi(G) \cap \ker\psi)}.$$

Por lo tanto la fórmula (2.24) para el rango se convierte en:

$$2^r = \frac{(G : \psi(\bar{G}))(\bar{G} : \varphi(G))}{(\ker\psi : \varphi(G) \cap \ker\psi) \cdot \#G_2}$$

Primero calculamos $(\ker\psi : \varphi(G) \cap \ker\psi)$. Como $\ker\psi = \{\bar{O}, \bar{T}\}$, hay solamente dos posibles valores para $(\ker\psi : \varphi(G) \cap \ker\psi)$: si $\bar{T} \in \varphi(G)$, entonces $\varphi(G) \cap \ker\psi = \ker\psi$ y así $(\ker\psi : \varphi(G) \cap \ker\psi) = 1$; si $\bar{T} \notin \varphi(G)$ tenemos que $\varphi(G) \cap \ker\psi = \{O\}$ y así $(\ker\psi : \varphi(G) \cap \ker\psi) = \#\ker\psi = 2$. Si juntamos estas observaciones con el inciso (iv), obtenemos la siguiente fórmula:

$$(\ker\psi : \varphi(G) \cap \ker\psi) = \begin{cases} 1 & \bar{b} \text{ es un cuadrado perfecto} \\ 2 & \bar{b} \text{ no es un cuadrado perfecto} \end{cases}.$$

Esta fórmula es afortunada porque al multiplicar $(\ker\psi : \varphi(G) \cap \ker\psi)$ por la fórmula (2.25) para $\#G_2$ obtenemos $(\ker\psi : \varphi(G) \cap \ker\psi) \cdot \#G_2 = 4$ y por lo tanto:

$$2^{r+2} = (G : \psi(\bar{G}))(\bar{G} : \varphi(G)) \tag{2.26}$$

y el problema de calcular el rango se reduce a estudiar las imágenes de φ y ψ.

[9]Estamos usando el siguiente resultado general de teoría de grupos abelianos: Si $f : G \to G'$ es un homomorfismo de grupos abelianos y $H \subseteq G$ un subgrupo de índice finito, entonces

$$(f(G) : f(H)) = \frac{(G : H)}{(\ker f : H \cap \ker f)}.$$

Esto se sigue de los teoremas de isomorfismo que nos dan:

$$\frac{f(G)}{f(H)} \cong \frac{G/\ker f}{H/H \cap \ker f} \cong \frac{G}{H + \ker f} \cong \frac{G/H}{(H + \ker f)/H} \cong \frac{G/H}{\ker f/(H \cap \ker f)}.$$

En el texto usamos $G = \bar{G}$, $f = \psi$ y $H = \varphi(G)$.

Para esto recurrimos a una función puramente aritmética: consideramos $\mathbb{Q}^*$ como grupo multiplicativo y tomamos el cociente con su subgrupo de cuadrados $\mathbb{Q}^{*2}$, con esto definimos:

$$\alpha : G \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2} \quad \text{con} \quad \alpha(P) = \begin{cases} x(P) \pmod{\mathbb{Q}^{*2}} & x(P) \neq 0 \\ 1 \pmod{\mathbb{Q}^{*2}} & P = O \\ b \pmod{\mathbb{Q}^{*2}} & P = T \end{cases}.$$

De manera análoga, podemos definir $\bar{\alpha} : \bar{G} \to \mathbb{Q}^*/\mathbb{Q}^{*2}$; simplemente hay que agregar "-" en donde sea necesario.

Lema 109. *Sea G el grupo de puntos racionales de una curva elíptica $E/\mathbb{Q}$. Las funciones $\alpha : G \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ y $\bar{\alpha} : \bar{G} \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ son homomorfismos de grupos y además:*

$$\ker \alpha = \psi(\bar{G}), \qquad \ker \bar{\alpha} = \varphi(G).$$

En particular tenemos que

$$(G : \psi(\bar{G})) = \#\alpha(G), \qquad (\bar{G} : \varphi(G)) = \#\bar{\alpha}(\bar{G}),$$

y por lo tanto, si r es el rango de E, tenemos:

$$2^{2+r} = \#\alpha(G) \cdot \#\bar{\alpha}(\bar{G}).$$

Proof. Solamente consideramos α y observamos que la misma prueba funciona para $\bar{\alpha}$. Para probar que α es un homomorfismo de grupos, recordemos que en la sección 1.3.1 deducimos varias ecuaciones que deben cumplir las coordenadas de P, Q y $P + Q$. En particular la ecuación 1.51 nos dice que:

$$x(P)x(Q)x(P+Q) = \mu^2, \qquad \mu = y(P) - \frac{y(Q) - y(P)}{x(Q) - x(P)} x(P) \in \mathbb{Q},$$

o en particular

$$x(P)x(Q)x(P+Q) \equiv 1 \pmod{\mathbb{Q}^{*2}}.$$

Si multiplicamos ambos lados de la congruencia por $x(P)x(Q)$ entonces obtenemos

$$x(P+Q) \equiv x(P)x(Q) \pmod{\mathbb{Q}^{*2}},$$

porque $x(P)^2 \equiv x(Q)^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}$ ya que $x(P), x(Q) \in \mathbb{Q}$. Salvo algunos pocos casos, como cuando $Q = T$, hemos probado que α es un homomorfismo de grupos; el resto de los casos se siguen de la definición de α.

Ahora probamos que el núcleo de α es la imagen de ψ. Primero sea $P \in \ker \alpha$. Si $P = O$, por el inciso (iii) de la proposición 108, tenemos que $P \in \psi(\bar{G})$. Si $b \in \mathbb{Q}^{*2}$ entonces puede suceder que $P = T$, pero el inciso (iv) nos dice que si b es un cuadrado perfecto, entonces $P = T \in \psi(\bar{G})$. Por último si $P \neq O, T$, entonces

$$P \in \ker \alpha \iff x(P) \equiv 1 \pmod{\mathbb{Q}^{*2}} \iff x(P) \in \mathbb{Q}^{*2} \overset{*}{\iff} P \in \psi(\bar{G}),$$

donde (*) es exactamente el inciso (v). Con esto concluimos que $\ker \alpha = \psi(\bar{G})$. Las siguientes dos afirmaciones del lema se siguen del primer teorema de isomorfismo y de la fórmula (2.26) para el rango que deducimos arriba. □

Con este lema, hemos reducido el problema de calcular el rango de la curva elíptica $X_0(15)$, a calcular la imagen de α y $\bar{\alpha}$. Para hacer esto, vamos a deducir una condición necesaria que cumplen los elementos de la imagen de α. Esto nos va a producir una lista de posibles candidatos y por lo tanto un algoritmo para calcular puntos en la imagen.

En general sea $\alpha(P) \in \alpha(G)$ donde $P = (x(P), y(P)) \in G$. Si $x = 0$, entonces $y(P)^2 = 0(0^2 + a0 + b) = 0$ y así $P = T$. Entonces $\alpha(T) = b\mathbb{Q}^{*2} \in \alpha(G)$. Si $y = 0$ entonces $0 = x(x^2 + ax + b)$ y por lo tanto x puede asumir uno de los siguientes tres valores:

$$x = 0, \qquad x = \frac{-a \pm \sqrt{a^2 - 4b}}{2} = \frac{-a \pm \sqrt{\bar{b}}}{2}.$$

Si $x = 0$ nos regresamos al caso $P = T$, entonces supongamos que $x = (a \pm \sqrt{\bar{b}})/2$. Si $\bar{b}$ no es un cuadrado perfecto, entonces $x \notin \mathbb{Q}$ y por lo tanto $P \notin G$ por lo que no obtenemos un punto nuevo en $\alpha(G)$. Si $\bar{b}$ es un cuadrado perfecto, por ejemplo $\bar{b} = d^2$, entonces

$$\left(\frac{-a \pm d}{2}, 0\right) \in G \quad \Longrightarrow \quad \alpha\left(\frac{-a \pm d}{2}, 0\right) = \frac{-a \pm d}{2}\mathbb{Q}^{*2}.$$

Por lo tanto los dos elementos $\frac{1}{2}(-a \pm d)\mathbb{Q}^{*2}$ están en la imagen de α.

El último caso $xy \neq 0$ lo tratamos en el siguiente lema:

Lema 110. *Sea G el grupo de puntos racionales de una curva elíptica E definido por $y^2 = x^3 + ax^2 + bx$. Para todo punto $P = (x, y) \in G$ tal que $xy \neq 0$, existe un divisor δ de b, positivo o negativo, tal que la ecuación diofantina:*

$$X^2 = F_\delta(Y, Z) = 0, \quad \text{donde por} \quad F_\delta(Y, Z) := \delta Y^4 + aY^2Z^2 + b_0Z^4 \quad (b = \delta b_0)$$

tiene una solución (X_0, Y_0, Z_0), con $Y_0 \neq 0$, y además:

$$P = \left(\frac{\delta Y_0^2}{Z_0^2}, \frac{\delta X_0 Y_0}{Z_0^3}\right), \qquad \alpha(P) \equiv \delta \pmod{\mathbb{Q}^{*2}}.$$

Si $Z_0 = 0$ tomamos $P = O$ y por lo tanto $\alpha(P) \equiv 1 \pmod{\mathbb{Q}^{*2}}$.

Proof. Sea $P = (x, y) \in G$ tal que $x \neq 0$ y $y \neq 0$. Como $x, y \in \mathbb{Q}$, podemos reescribir estas fracciones como

$$x = \frac{m}{e^2}, \qquad y = \frac{n}{e^3},$$

donde $n, m, e \in \mathbb{Z}$, $e > 0$ y las fracciones son irreducibles. Como P es un punto sobre la curva elíptica, sus coordenadas satisfacen la ecuación que define a E. De esta manera tenemos:

$$\left(\frac{n}{e^3}\right)^2 = \frac{m}{e^2}\left(\frac{m^2}{e^4} + a\frac{m}{e^2} + b\right) \quad \Longrightarrow \quad n^2 = m(m^2 + ame^2 + e^4b).$$

Por otro lado, sea $\delta = \pm(m, b)$ donde elegimos el signo de tal manera que $\delta m > 0$. Con esto en mente escribimos $m = \delta m_0$ y $b = \delta b_0$ donde, por construcción, tenemos que $(m_0, b_0) = 1$. Si sustituimos estas expresiones en la ecuación anterior, obtenemos:

$$n^2 = \delta m_0(\delta^2 m_0^2 + a\delta m_0 e^2 + e^4 \delta b_0) = \delta^2 m_0(\delta m_0^2 + ae^2 m_0 + e^4 b_0), \tag{2.27}$$
$$\therefore \quad \delta^2 \mid n^2 \quad \Longrightarrow \quad \delta \mid n.$$

Con esto, escribimos $n = \delta n_0$ y volvemos a sustituir en la ecuación (2.27) para obtener:

$$\delta^2 n_0^2 = \delta^2 m_0(\delta m_0^2 + ae^2 m_0 + e^4 b_0) \quad \Longrightarrow \quad n_0^2 = m_0(\delta m_0^2 + ae^2 m_0 + e^4 b_0). \tag{2.28}$$

El siguiente paso es probar que los dos factores de lado derecho, m_0 y $\delta m_0^2 + ae^2 m_0 + e^4 b_0$, son primos relativos. De esta manera tendríamos que ambos factores son cuadrados perfectos. Para esto, supongamos que existe un primo p que es un factor común. Primero observemos que como $p \mid m_0$ y $(m_0, b_0) = 1$, entonces $p \nmid b_0$. Además tenemos que:

$$\begin{gathered} p \mid \delta m_0^2 + ae^2 m_0 + e^4 b_0 \quad \Longrightarrow \quad p \mid e^4 b_0 \quad \overset{p \nmid b_0}{\Longrightarrow} \quad p \mid e^4 \quad \Longrightarrow \quad p \mid e \\ \therefore \quad p \mid (m_0, e) \quad \Longrightarrow \quad p \mid (m, e) = 1 \quad \to\leftarrow . \end{gathered}$$

La contradicción es por elección de m y e que tomamos como primos relativos. Por lo tanto el primo p no puede existir y así m_0 y $\delta m_0^2 + ae^2 m_0 + e^4 b_0$ son primos relativos.

Gracias a lo anterior y a (2.28), existen enteros N y M tales que

$$M^2 = m_0, \qquad N^2 = \delta m_0^2 + ae^2 m_0 + e^4 b_0.$$

Con esto, (2.28) implica que $n_0 = MN$. Si sustituimos estas nuevas expresiones en (2.28), obtenemos:

$$(MN)^2 = M^2(\delta M^4 + ae^2 M^2 + e^4 b_0) \quad \Longrightarrow \quad N^2 = \delta M^4 + aM^2 e^2 + b_0 e^4.$$

Por lo tanto $(X, Y, Z) = (N, M, e)$ es una solución de la ecuación diofantina:

$$X^2 = \delta Y^4 + aY^2 Z^2 + b_0 Z^4.$$

Además, el punto P tiene coordenadas:

$$P = (x, y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right) = \left(\delta \frac{M^2}{e^2}, \frac{\delta MN}{e^3}\right).$$

Por lo tanto

$$\alpha(P) = \delta \frac{M^2}{e^2} \equiv \delta \pmod{\mathbb{Q}^{*2}} \quad \Longrightarrow \quad \delta \pmod{\mathbb{Q}^{*2}} \in \alpha(G).$$

□

Con el lema anterior nos sugiere un algoritmo que calcula la imagen de α: toma todos los divisores de b y ve si la ecuación diofantina $X^2 = F_\delta(Y, Z)$ tiene solución; los que tengan solución nos producen elementos en la imagen y todos los elementos en la imagen surgen de esta manera.

Podemos mejorar el algoritmo. Supongamos que hay dos divisores δ_1 y δ_2 tales que $\delta_1 \equiv \delta_2 \pmod{\mathbb{Q}^{*2}}$. Entonces existe un racional $d/e \in \mathbb{Q}$ tal que $\delta_1 e^2 = \delta_2 d^2$. Esto implica que el punto P asociado a la solución (X_0, Y_0, Z_0) es igual a:

$$P = (\delta_1 Y_0^2 Z_0^{-2}, \delta_1 X_0 Y_0 Z_0^{-3}) = (\delta_2 (dY_0)^2 (eZ_0)^{-2}, \delta_2 (deX_0)(dY_0)(eZ_0)^{-3}),$$

que es el punto asociado a la solución (deX_0, dY_0, eZ_0) de la ecuación diofantina asociada a δ_2, en efecto:

$$\begin{aligned} \delta_2 (dY_0)^4 + a(dY_0)^2 (eZ_0)^2 + \frac{b}{\delta_2}(eZ_0)^4 &= \frac{e^2}{d^2}\delta_1 (dY_0)^4 + a(dY_0)^2 (eZ_0)^2 + \frac{bd^2}{\delta_1 e^2}(eZ_0)^4 \\ &= e^2 d^2 (\delta Y_0^4 + aY_0^2 Z_0^2 + b_0 Z_0^4) \\ &= e^2 d^2 X_0^2, \end{aligned}$$

$$\therefore \quad (deX_0)^2 = F_{\delta_2}(dY_0, eZ_0).$$

Acabamos de probar que si $\delta_1 \equiv \delta_2 \pmod{\mathbb{Q}^{*2}}$ entonces $X^2 = F_{\delta_1}(Y, Z)$ tiene solución si y solo si $X^2 = F_{\delta_2}(Y, Z)$ tiene solución.

Por lo tanto si partimos el conjunto de divisores de b en clases de equivalencia módulo $\mathbb{Q}^{*2}$, entonces basta verificar si $X^2 = F_\delta(Y, Z) = 0$ para solamente un divisor δ por cada clase de equivalencia. De esta manera tenemos el siguiente algoritmo para calcular la imagen de α:

Algoritmo 111. Cálculo de $\alpha(G)$. Sea G el grupo de puntos racionales de una curva elíptica E definido por $y^2 = x^3 + ax^2 + bx$. Denotamos por $\mathfrak{D}$ al conjunto de divisores positivos y negativos de b.

1. Parte $\mathfrak{D}$ en clases de equivalencia módulo $\mathbb{Q}^{*2}$ y toma un sistema completo de residuos $\mathfrak{D}' = \{\delta_1, \ldots, \delta_n\}$ módulo $\mathbb{Q}^{*2}$.

2. Para todo divisor $\delta_i \in \mathfrak{D}'$, determina si la ecuación diofantina $X^2 = \delta_i Y^4 + aY^2Z^2 + b_i Z^4$ (donde $b = \delta_i b_i$) tiene una solución (X_i, Y_i, Z_i) con $Y_i \neq 0$.

   (a) Si existe tal solución, entonces $b \pmod{\mathbb{Q}^{*2}} \in \alpha(G)$.

   (b) Si no tiene tal solución, cambia de divisor y repite.

3. Cuando se terminen los divisores, la lista de elementos obtenidos en 2a es la imagen de α.

Nota. Cuando $\bar{b}$ es un cuadrado perfecto vimos que $\frac{-a\pm d}{2}\mathbb{Q}^{*2}$ son dos elementos de la imagen de α, pero el algoritmo anterior ya nos produce estos dos elementos. En efecto, si $\bar{b} = d^2$ es un cuadrado perfecto, entonces b admite la factorización

$$b = \frac{-a+d}{2}\frac{-a-d}{2}\mathbb{Q}^{*2}.$$

Si tomamos $\delta = (-a \pm d)/2$, entonces la ecuación diofantina:

$$X^2 = \frac{-a \pm d}{2}Y^4 + aY^2Z^2 + \frac{-a \mp d}{2}Z^4$$

tiene la solución trivial $(X_0, Y_0, Z_0) = (0, 1, 1)$ y por lo tanto el algoritmo nos produce los dos elementos $\frac{-a\pm d}{2}\mathbb{Q}^{*2}$.

Usamos este algoritmo para probar que

Proposición 112. *Sea $G = X_0(15)(\mathbb{Q})$ el grupo de puntos racionales El rango de la curva modular $X_0(15)$ es 0, por lo tanto $G = G_{\text{tor}}$ y $\#G = 8$.*

Proof. Si aplicamos el algoritmo a la curva $X_0(15)$ con la ecuación de Weierstrass $y^2 + xy + y = x^3 + x^2 - 10x - 10$, los coeficientes de las ecuaciones diofantinas son muy grandes para describir el proceso en este texto, entonces vamos a cambiar $X_0(15)$ por una curva isógena que tenga coeficientes más pequeños. Para encontrar tal curva, primero buscamos la ecuación de Weierstrass en las tablas de Cremona [Cremona, 1997], que está en la lista de curvas de conductor 15.[10] Ahora buscamos

[10]En general, cuando $X_0(N)$ es una curva elíptica, entonces su conductor es N; esto lo prueba Ligozat en su tesis. Además, comentamos que si usamos las tablas de Cremona, entonces a priori tenemos que el rango de $X_0(15)$ es 0, pero solamente estamos invocando las tablas de Cremona para simplificar los cálculos y la exposición.

otra curva elíptica en esa misma clase de isogenia con coeficientes más pequeños, en este caso tomamos la ecuación $y^2+xy+y=x^3+x^2$. Si simplificamos la ecuación de Weierstrass, obtenemos $y^2 = x^3 - 27x + 8694$ y después del cambio de variable $(x, y) \to (9x - 21, 27y)$, obtenemos una ecuación de Weierstrass de la forma adecuada para aplicar el algoritmo 111:

$$E \ : \ y^2 = x^3 - 7x^2 + 16x.$$

Las constantes necesarias para el algoritmo son $a = -7$ y $b = 2^4$. De una vez calculamos la curva elíptica asociada:

$$\bar{E} \ : \ y^2 = x^3 + 14x^2 - 15x,$$

donde $\bar{a} = 14$ y $\bar{b} = -15$. Empezamos con el algoritmo que aplicamos simultáneamente a E y a $\bar{E}$:

Todo divisor δ de b es de la forma $\pm 2^\alpha$ donde $0 \leq \alpha \leq 4$. Si $2 \mid \alpha$, entonces δ es un cuadrado perfecto y $\pm\delta \equiv \pm 1 \pmod{\mathbb{Q}^{*2}}$; si $2 \nmid \alpha$ tenemos $\pm 2^\alpha \equiv \pm 2 \pmod{\mathbb{Q}^{*2}}$. Por lo tanto.

$$\mathfrak{D}' = \{-2, -1, 1, 2\}.$$

Todos los divisores de $\bar{b}$ son libres de cuadrados, entonces ninguna pareja de divisores son congruentes módulo $\mathbb{Q}^{*2}$ y por lo tanto

$$\bar{\mathfrak{D}}' = \mathfrak{D} = \{-15, -5, -3, -1, 1, 3, 5, 15\}.$$

En el caso E, la ecuación asociada al divisor $\delta \mid b$

$$X^2 = F_\delta(Y, Z) = \delta Y^4 - 7Y^2Z^2 + \frac{16}{\delta}Z^4$$

no tiene solución real (no trivial) cuando $\delta < 0$ porque en este caso $16/\delta < 0$ y así el lado derecho es negativo. Por lo tanto, si $\delta < 0$, la ecuación diofantina $X^2 = F_\delta(Y, Z)$ no tiene solución y por lo tanto $\delta \pmod{\mathbb{Q}^{*2}} \notin \alpha(G)$; descartamos los divisores negativos y nos quedamos con solamente $\delta = 1, 2$. Si $\delta = 1$ tenemos que

$$(1, 1, 0) \text{ es una solución de } \quad X^2 = Y^4 - 7Y^2Z^2 + 16Z^4.$$

Por lo tanto $1 \pmod{\mathbb{Q}^{*2}} \in \alpha(G)$, pero esto ya lo sabíamos porque $\alpha(O) = 1 \mod \mathbb{Q}^{*2}$. Sin embargo, si $\delta = 2$, la ecuación diofantina $X^2 = 2Y^4 - 7Y^2Z^2 + 8Z^4$, no tiene soluciones.

Para ver esto reducimos la ecuación módulo 4:

$$X_0^2 \equiv 2Y_0^4 + Y^2Z^2 \equiv Y_0^2(2Y_0^2 + Z_0^2) \pmod 4. \tag{2.29}$$

Hay dos casos según si $Y_0^2 \equiv 0$ ó $Y_0^2 \equiv 1 \pmod 4$, ya que éstos son los únicos residuos cuadráticos módulo 4. Si ocurre lo último tenemos:

$$Y_0 \equiv 1 \pmod 4 \quad \Longrightarrow \quad X_0^2 \equiv 2 + Z_0^2 \equiv \begin{cases} 2 \pmod 4 & Z_0^2 \equiv 0 \pmod 4 \\ -1 \pmod 4 & Z_0^2 \equiv 1 \pmod 4 \end{cases} \quad \to\leftarrow . \tag{2.30}$$

Por lo tanto necesariamente tenemos $Y_0^2 \equiv 0 \pmod 4$ ó equivalentemente $2 \mid Y_0$. Esto, junto con la congruencia (2.29), implica que $X_0^2 \equiv 0 \pmod 4$ y también $2 \mid X_0$.

Por lo tanto existen $x_0, y_0 \in \mathbb{Z}$ tales que $X_0 = 2x_0$ y $Y_0 = 2y_0$. Si sustituimos esto en la ecuación diofantina original para $\delta = 2$, obtenemos:

$$4x_0^2 = 32y_0^4 - 28y_0^2Z_0^2 + 8Z_0^4 = 4(8y_0^4 - 7y_0^2Z_0^2 + 2Z_0^4) \quad \Longrightarrow \quad x_0^2 = 8y_0^4 - 7y_0^2Z_0^2 + 2Z_0^4. \quad (2.31)$$

Módulo 4 la ecuación se vuelve

$$x_0^2 \equiv Z_0^2(y_0^2 + 2Z_0^2).$$

Si $Z_0^2 \equiv 1 \pmod 4$ obtenemos la misma contradicción que en (2.30), entonces $Z_0^2 \equiv 0 \pmod 2$, i.e. $Z_0 = 2z_0$ para alguna $z_0 \in \mathbb{Z}$. Esto, junto con la congruencia anterior, implica que también $x_0^2 \equiv 0 \pmod 4$; escribimos $x_0 = 2x_1$ para alguna $x_1 \in \mathbb{Z}$. Sustituimos estas expresiones en la ecuación (2.31) para obtener

$$4x_1^2 = 8y_0^4 - 28y_0^2z_0^2 + 32z_0^4 \quad \Longrightarrow \quad x_1^2 = 2y_0^4 - 7y_0^2z_0^2 + 8z_0^4,$$

es decir $(x_1, y_0, z_0) = (X_0/4, Y_0/2, Z_0/2)$ es una solución a la ecuación diofantina $X^2 = F_2(Y, Z)$.

Observe que las entradas de la nueva solución son estrictamente menores que las entradas originales y en particular $0 < Y_0/2 < Y_0$. Por lo tanto podemos construir una cadena infinita de soluciones enteras cuyas entradas decrecen estrictamente, lo cual es imposible. Esto es un ejemplo de *descenso a infinito*, un método famoso para probar que una ecuación diofantina no tiene solución. Por lo tanto $X^2 = F_2(Y, Z)$ no tiene soluciones y de esta manera el divisor $\delta = 2$ no contribuye a la imagen. Hemos probado que

$$\alpha(G) = \{1 \pmod{\mathbb{Q}^{*2}}\} \quad \Longrightarrow \quad \#\alpha(G) = 1 \quad (2.32)$$

Ahora estudiamos las ecuaciones diofantinas asociadas a la curva $\bar{E}$: para todo divisor $\bar{\delta} \in \bar{\mathfrak{D}}'$, la ecuación diofantina asociada a $\bar{\delta}$ es $X^2 = F_{\bar{\delta}}(Y, Z)$ donde $F_{\bar{\delta}}$ está definida por

$$F_{\bar{\delta}}(Y, Z) = \bar{\delta}Y^4 + 14Y^2Z^2 - \frac{15}{\delta}Z^4.$$

Con una computadora, o incluso a mano, uno puede encontrar soluciones pequeñas a varias ecuaciones diofantinas. Por ejemplo:

$(0, 1, 1)$ es una solución de $X^2 = Y^4 + 14Y^2Z^2 - 15Z^4$ y $X^2 = -15Y^4 + 14Y^2Z^2 + 1Z^4$,

$(4, 1, 1)$ es una solución de $X^2 = 5Y^4 + 14Y^2Z^2 - 3Z^4$ y $X^2 = -3Y^4 + 14Y^2Z^2 + 5Z^4$.

Entonces las ecuaciones asociadas a $\bar{\delta} = -15, -3, 1, 5$ tienen soluciones. De hecho, éstas son las únicas:

$$\{-15 \pmod{\mathbb{Q}^{*2}}, -3 \pmod{\mathbb{Q}^{*2}}, 1 \pmod{\mathbb{Q}^{*2}}, 5 \pmod{\mathbb{Q}^{*2}}\} = \bar{\alpha}(\bar{G}) \quad \Longrightarrow \quad \#\bar{\alpha}(\bar{G}) = 4. \quad (2.33)$$

El resto de las ecuaciones no tienen soluciones. Como ya hemos descrito con detalle este proceso para la curva E, solamente mencionamos bajo qué módulo sale la contradicción. Para $F_{-1}(Y, Z)$ y $F_{15}(Y, Z)$, reduce módulo 8 porque ahí $F_{-1} \equiv F_{15} \pmod 8$; para $F_3(Y, Z)$ y $F_{-15}(Y, Z)$, reduce módulo 16. En ambos casos, la existencia de una solución nos produce una contradicción mediante un argumento de "descenso a infinito". Por lo tanto:

$$\bar{P}_{15} = \bar{P}_3 = \bar{P}_{-1} = \bar{P}_{-5} = O.$$

Para terminar juntamos nuestras fórmulas para las imágenes de α, (2.32) y (**??**), y sustituimos en la fórmula del rango de E del lema 110 para concluir que:

$$2^{2+r} = 4 \quad \Longrightarrow \quad r = 0.$$

□

Bibliography

[Ahlfors, 1979] Ahlfors, L. V. (1979). *Complex Analysis*. McGraw-Hill.

[Apostol, 1990] Apostol, T. (1990). *Modular Functions and Dirichlet Series in Number Theory*. Springer.

[Atiyah and Macdonald, 1994] Atiyah, M. and Macdonald, I. (1994). *Introduction to Commutative Algebra*. Avalon Publishing.

[Atkin and Lehner, 1970] Atkin, A. and Lehner, J. (1970). Hecke operators on $\gamma_0(n)$. *Mathematische Annalen*, pages 185:134–160.

[Bump, 1998] Bump, D. (1998). *Automorphic Forms and Representations*. Cambridge University Press.

[Cremona, 1997] Cremona, J. (1997). *Algorithms for Modular Elliptic Curves*. Springer New York.

[Deligne, 1971] Deligne, P. (1971). *Formes modulaires et représentations $\ell-$adiques*. Springer. en "Lecture Notes in Math", volumen 179, páginas 139-172.

[Deligne and Serre, 1974] Deligne, P. and Serre, J.-P. (1974). Formes modulaires de poids 1. *Annales scientifiques de L'É.N.S.*, pages 507–530.

[Diamond and Shurman, 2005] Diamond, F. and Shurman, J. (2005). *A First Course in Modular Forms*. Springer.

[Eisenbud, 2004] Eisenbud, D. (2004). *Commutative Algebra with a View Toward Algebraic Geometry*. Springer.

[Euler, 1740] Euler, L. (1740). De summis serierum reciprocarum. *Commentarii academiae scientiarum Petropolitanae 7*, pages 123–134.

[Fricke, 1922] Fricke, R. (1922). *Die Elliptischen Funktionen Und Ihere Anwendungen*. Leipzig, Berlin, B.G. Teubner.

[Fulton, 2008] Fulton, W. (2008). *Algebraic Curves: an Introduction to Algebraic Geometry*. Addison-Wesley Pub. Co.

[Gelbart, 1997] Gelbart, S. (1997). *Three Lectures on the Modularity of $\bar{\rho}_{E,3}$ and the Langlands Reciprocity Conjecture*. Springer. en "Modular Forms and Fermat's Last Theorem" editado por Cornell, Silverman y Stevens.

[Hartshorne, 1977] Hartshorne, R. (1977). *Algebraic Geometry*. Springer.

[Ireland and Rosen, 1990] Ireland, K. and Rosen, M. (1990). *A Classical Introduction to Modern Number Theory*. Springer.

[Kato et al., 2011] Kato, K., Kurokawa, N., and Saito, T. (2011). *Number Theory 2: An introduction to Class Field Theory*. American Mathematical Society.

[Lang, 2005] Lang, S. (2005). *Algebra*. Graduate Texts in Mathematics. Springer New York.

[Langlands, 1980] Langlands, R. P. (1980). *Base Change for GL(2)*. Annals of Mathematics Studies. Princeton University Press.

[Ligozat, 1975] Ligozat, G. (1975). *Courbes modulaires de genre 1*. Number 43 in Mémoires de la Société Mathématique de France. Société mathématique de France.

[Lutz, 1937] Lutz, E. (1937). Sur l'équation $y^2 = x^3 - ax - b$ dans les corps $p-$adiques. *Journal für die reine und angewandte Mathematik*, 177:238–247.

[Matsumura, 1970] Matsumura, H. (1970). *Commutative Algebra*. Mathematics lecture note series. Benjamin.

[Milne, 2017] Milne, J. (2017). *Modular Functions and Modular Forms*. Disponible en www.jmilne.org/math/.

[Miyake, 1989] Miyake, T. (1989). *Modular Forms*. Springer.

[Nagell, 1935] Nagell, T. (1935). Solution de quelques problèmes dans la theéorie arithmeétique des cubiques nagell planes du premier genre. *Wid. Akad. Skrifter Oslo I*.

[Neukirch, 1999] Neukirch, J. (1999). *Algebraic Number Theory*. Springer.

[Newman, 1956] Newman, M. (1956). Construction and application of a class of modular functions i. *Proc. London Math. Soc.*, pages 334–350.

[Newman, 1958] Newman, M. (1958). Construction and application of a class of modular functions ii. *Proc. London Math. Soc.*, pages 373–387.

[Rotman, 1995] Rotman, J. J. (1995). *An Introduction to the Theory of Groups*. Springer.

[Saito, 2013a] Saito, T. (2013a). *Fermat's Last Theorem: Basic Tools*. American Mathematical Society.

[Saito, 2013b] Saito, T. (2013b). *Fermat's Last Theorem: The Proof*. American Mathematical Society.

[Serre, 1959] Serre, J.-P. (1959). *Groupes algébriques et corps de classes*. Hermann Paris.

[Serre, 1973] Serre, J.-P. (1973). *A Course in Arithmetic*. Springer.

[Serre, 1977a] Serre, J.-P. (1977a). *Linear Representations of Finite Groups*. Springer.

[Serre, 1977b] Serre, J.-P. (1977b). *Modular Forms of Weight 1 and Galois Representations*. Academic Press. en "Algebraic Number Fields", editado por A. Frölich.

[Shimura, 1994] Shimura, G. (1994). *Introduction to the Arithmetic Theory of Automorphics Functions*. Springer.

[Shimura, 2012] Shimura, G. (2012). *Modular Forms: Basics and Beyond*. Springer.

[Silverman, 2009] Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves*. Springer.

[Silverman and Tate, 2009] Silverman, J. H. and Tate, J. T. (2009). *Rational Points on Elliptic Curves*. Springer.

[Stein and Shakarchi, 2002] Stein, E. M. and Shakarchi, R. (2002). *Fourier Analysis*. Princeton University Press.

[Tunnell, 1981] Tunnell, J. (1981). Artin's conjecture for representations of octahedral type. *Bulletin of the American Mathematical Society*, 5:173–175.

[Vélu, 1971] Vélu, J. (1971). Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris*, 273:A238–A241.

[Wiles, 1995] Wiles, A. (1995). Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 141:443–551.