UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN CIENCIAS MATEMÁTICAS Y DE LA ESPECIALIZACIÓN EN ESTADÍSTICA APLICADA

Curvas elípticas, formas modulares y el teorema de modularidad

TESIS
QUE PARA OPTAR POR EL GRADO DE:
MAESTRO (A) EN CIENCIAS

PRESENTA:
Alejandro De Las Peñas Castaño

DIRECTOR
Timothy Gendron
Instituto de Matemáticas – Unidad Cuernavaca

CIUDAD DE MÉXICO julio de 2020

Índice general

Capítulo 1

Introducción

El propósito de esta tesis es exponer la teoría de curvas elípticas y formas modulares para entender el papel que toman en la prueba del teorema de modularidad para curvas elípticas semiestables. También estudiamos las representaciones de Galois que nos dan un puente entre las curvas elípticas y las formas modulares que permite reescribir la prueba del teorema de modularidad en términos de representaciones de Galois.

La prueba del teorema de modularidad es de las más celebradas en matemáticas y es producto de décadas de desarrollo en diversas áreas por muchos grandes matemáticos. Gracias a esto, no daremos una prueba completa del teorema de modularidad, sino que nos enfocaremos en las partes de la prueba que directamente involucran curvas elípticas y formas modulares como la teoría de curvas modulares y cálculos explícitos de invariantes de curvas elípticas. En particular omititmos las pruebas del teorema de Langlands-Tunnell, repasamos brevemente y sin pruebas la teoría de espacios moduli de Deligne-Rapaport y la teoría de deformaciones de Galois de Wiles.

Panorama histórico

El teorema de modularidad para curvas elípticas semiestables dice que

Toda curva elíptica semiestable definida sobre $\mathbb{Q}$ es modular.

Este resultado fue conjeturado por Shimura, Taniyama y Weil sin la hipótesis de semiestabilidad. Con esta hipótesis adicional, este resultado fue demostrado por Wiles, Wiles-Taylor en 1994 (la prueba completa aparece en [Wil95]). Con las herramientas desarrolladas por Wiles, una prueba completa del teorema de modularidad, sin la hipotesis de semiestabilidad, fue probada por Breuil, Conrad, Diamond y Taylor en 2001 [BCDT01]

La fama del teorema de modularidad claramente viene de su participación en la prueba del último teorema de Fermat (UTF) que dice: para $n > 2$ tenemos

$$\exists x, y, z \in \mathbb{Z} \text{ tales que } x^n + y^n = z^n \quad \Longrightarrow \quad xyz = 0.$$

Claramente si $d \mid n$, entonces UTF(d) $\Longrightarrow$ 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.

En 1823, Sophie Germain probó el primer caso del UTF (cuando $n \nmid x, y, z$) para exponentes que son *primos de Germain*[1] y propuso una estrategia para probar el UTF en general que, aunque no terminó siendo la prueba completa, introdujo una clasificación del UTF en dos casos que después le sirvió a Kummer. En 1839 Lamé pruebó el caso $n = 7$. Ocho años después, Lamé presentó una prueba completa del UTF, pero resultó estar equivocada pues había supuesto, 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.[2]

Todo cambió cuando Frey sugirió una nueva alternativa en los 1980's. Para ese entonces la geometría algebráica estaba bien fundamentada y ofrecía herramientas poderosas para estudiar el UTF. Frey sugirió que de un contraejemplo $a^p + b^p = c^p$ de UTF(p), la curva elíptica asociada

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

podría ser un contraejemplo al teorema de modularidad, que en aquel entonces era apenas una conjetura desarrollada a lo largo de los 60s y 70s por Shimura, Taniyama y Weil. Esta curva se llama la *curva de Frey* en su honor a pesar de que la conexión entre la curva de Frey y el UTF fue establecida por Hellegouarch unos años antes.

Para argumentar por qué $E = E_{a,b,c,p}$ podría contradecir el teorema de modularidad, Frey, junto con Serre, describieron las propiedades de las representaciones de Galois $\bar{\rho} = \bar{\rho}_{E,p}$ asociadas a los puntos de $p-$torsión de E. En particular, ellos probaron que $\bar{\rho}$ debería ser impar, absolutamente irreducible, no ramificada fuera de $2p$ y plana 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 cuándo 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 conductor de Artin.

La reducción de nivel de (ciertas) representaciones modulares lo probaron Ribet y Mazur en los 80s. Por fin la intuición de Frey se confirmó. Si la conjetura de Shimura-Taniyama-Weil fuese ciertay E fuese modular, la representación $\bar{\rho}$ sería modular. Por el teorema de Mazur-Ribet, $\bar{\rho}$ induce una representación modular de nivel 2 (el conductor de Artin de $\bar{\rho}$), asociada a una forma modular cuspidal f de nivel 2 no trivial. Como es bien conocido que el espacio de tales formas modulares es nulo, esto produce una contradicción.

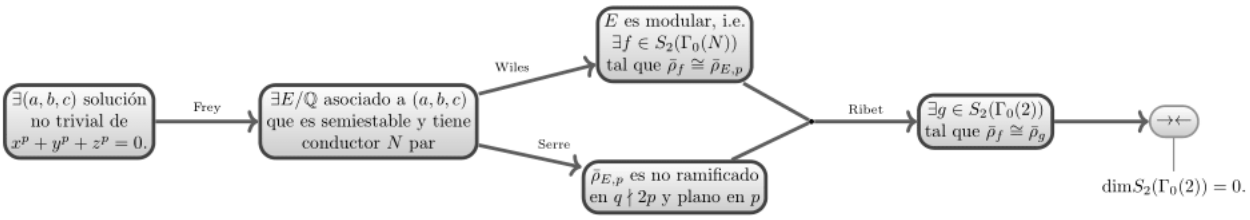
Por lo tanto si el UTF fuese falso, existiría una curva elíptica, la curva de Frey, no modular y entonces sería un contraejemplo a la conjetura de Shimura-Taniyama-Weil. El camino a la prueba del UTF se iluminó: pruebas la conjetura de Shimura-Taniyama-Weil y pruebas el último teorema de Fermat.

Por lo tanto, en los 90s solamente faltaba probar que toda curva elíptica sobre $\mathbb{Q}$ era efectivamente una curva modular. En 1993, Andrew Wiles expuso una prueba, pero durante la revisión de su artículo, encontraron un error en un argumento de inducción. En un año, Wiles, junto con Richard Taylor, un exalumno suyo, presentaron una prueba completa que fue publicada en 1995.

[1] Un primo p es de Germain si $2p + 1$ también es primo.

[2] 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 Spec($\mathcal{O}_K$). Siegel conjeturó que había una infinidad de tales primos y se cree que la densidad de los primos regulares es de $e^{-1/2}$ (cf. [IR90]).

Esquemáticamente, la prueba del UTF se ve así:



Para una discusión más profunda sobre esta prueba, véase la sección 6.5.

Sobre la tesis

El propósito de esta tesis es probar las partes del teorema de modularidad que involucran la teoría de curvas elípticas, formas modulares y la teoría elemental de representaciones de Galois. Para esto la tesis se divide en dos partes:

Primero introducimos la teoría básica de curvas elípticas, formas modulares y representaciones de Galois para poder probar resultados básicos sobre curvas modulares y en particular la definición de modularidad de curvas elípticas.

En la segunda parte de la tesis, probamos los pasos del teorema de modularidad para curvas elípticas semiestables, que se deducen de los hechos establecidos en la primera parte. Gracias al tamaño de la prueba, es necesario omitir ciertos pasos. Específicamente, omitimos los resultados de Wiles sobre deformaciones de Galois, la prueba del teorema de Langlands-Tunnel y la teoría de representabilidad de Deligne-Rapaport. Al final exponemos la aplicación del teorema de modularidad a la prueba del último teorema de Fermat. Más precisamente, la estructura de la tesis es de la siguiente forma:

En el segundo capítulo, exponemos la teoría básica de curvas elípticas y en particular estudiamos ecuaciones de Weierstrass y sus invariantes asociados. También repasamos la estructura de grupo que tienen los puntos de una curva elítpica y en particular exponemos las propiedades de sus subgrupos de torsión.

Después, nos enfocamos en el estudio de curvas elípticas según sobre qué campo están definidas para profundizar sobre las propiedades específicas que cumplen las curvas elípticas al cambiar el campo de definición. En particular estudiamos curvas elípticas sobre campos finitos, campos locales (e.g. racionales $p-$ádicos y sus extensiones finitas), campos numéricos y campos de funciones de curvas, i.e. superficies elípticas. En estas partes repasamos resultados importantes, como el teorema de Mordell-Weil, y definiciones esenciales como semiestabilidad y rango de una curva elíptica.

En el tercer capítulo, introducimos la teoría clásica de formas modulares. En particular, empezamos con la acción de $\mathrm{SL}_2(\mathbb{Z})$, y sus diferentes subgrupos de índice finito, en el semiplano superior. Esto nos da la definición de curva modular como una superficie de Riemann. Luego definimos formas modulares, cuspidales y automorfas y estudiamos la estructura del espacio vectorial de las formas modulares y cuspidales. Después estudiamos los operadores de Hecke que operan sobre estos espacios vectoriales para poder definir una clase importante de formas modulares invariantes llamadas formas primitivas (o *newforms* en la literatura clásica) que servirán como fuente de curvas elípticas modulares.

El el cuarto capítulo retomamos las curvas modulares del anterior y las estudiamos como objetos aritméticos en lugar de analíticos. Más precisamente, repasamos la teoría de Shimura que le asocia a cada curva modular, un modelo definido sobre algún campo numérico. Luego estudiamos el caso particular de la curva modular $X_0(N)$ y definimos la modularidad de curvas elípticas. Luego estudiamos las curvas modulares como espacios moduli, es decir estudiamos cómo interpretar las curvas modulares de tal manera que sus puntos corresponden a clases de isomorfimo de curvas elípticas cuyos isomorfismos preservan cierta estructura de torsión.

En el quinto capítulo introducimos las representaciones de Galois, i.e. representaciones del grupo absoluto de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, que nos dan una herramienta puramente algebraica para estudiar curvas elípticas y en particular su estructura de torsión. Vemos que muchas propiedades de las curvas elípticas se pueden traducir a propiedades de representaciones de Galois como la semiestabilidad y la modularidad. Por último exponemos brevemente la teoría de deformaciones de Galois y en particular el resultado esencial de Wiles sobre las deformaciones modulares de una representación de Galois asociada a los puntos de torsión de una curva elíptica.

En el sexto capítulo describimos la prueba del teorema de modularlidad para curvas elípticas semiestables, en cinco secciones:

1. En la primera sección descomponemos la prueba del teorema de modularidad en sus componentes básicas y probamos cómo estas componentes implican el teorema de modularidad.

2. En la segunda sección enunciamos el teorema de Langlands-Tunnell y probamos cómo implica la modularidad de la representación $\bar{\rho}_{E,3}$ asociada a los puntos de $3-$torsión de E, una curva elíptica, bajo una condición adicional de irreducibilidad de $\bar{\rho}_{E,3}$.

3. En la tercera sección probamos el "truco 3-5": cuando $\bar{\rho}_{E,3}$ es reducible, entonces $\bar{\rho}_{E,5}$ es irreducible.

4. En la cuarta sección estudiamos familias de curvas elípticas módulo 5 que, bajo la condición de irreducibilidad de $\bar{\rho}_{E,5}$, nos permite cambiar a otra curva elíptica E', cuya modularidad es equivalente a la de E y cuya representación $\bar{\rho}_{E',3}$ sí es irreducible; esto permite aplicar el teorema de Langlands-Tunnel sin alterar las conclusiones sobre la curva original E.

5. En la última sección probamos el UTF usando el teorema de modularidad junto con una exposición breve de los resultados de Serre, Mazur y Ribet.

En el séptimo capítulo reproducimos los cálculos requeridos, a lo largo del texto, como un documento independiente de Mathematica.

Prerequisitos: Vamos a asumir conocimiento sobre algebra abstracta, en particular teoría de campos y de Galois; sobre análisis complejo y topología elemental; sobre las definiciones y resultados básicos de geometría algebraica. Cualquier resultado que requerimos en la tesis que necesita una profundización en algunos de estos temas, lo citamos y damos referencias estándares a estos hechos.

Capítulo 2

Curvas elípticas

2.1. Definiciones preliminares

Definición 2.1.1. Una *curva elíptica* $E = (E, O)$ es una curva proyectiva lisa de género 1 con un punto distinguido $O \in E(K)$. Decimos que E *está definida sobre* un campo K, si E está definida 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 definida sobre K, $a_i \in K$. De hecho, la homogenización de esta ecuación es el polinomio que define la imagen de E bajo una inmersión cerrada $E \hookrightarrow \mathbb{P}^2(K)$,[1] es decir E es isomorfa a una curva cúbica lisa en $\mathbb{P}^2(K)$ con ecuación

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3. \tag{2.1.1}$$

Más precisamente tenemos el siguiente teorema:

Teorema 2.1.2. *Sea (E, O) una curva elíptica sobre K, $\overline{K}$ una cerradura algebraica de K, y sea $K(E)$ el 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*

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

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

$$y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{2.1.2}$$

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 un cambio de variable de la forma:

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

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

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

Demostración. 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 [Sil09, 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

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0, \qquad A_i \in K \text{ no todas } = 0 \tag{2.1.3}$$

Observe que si $A_6 \neq 0$ entonces A_7x^3 sería el único término de (2.1.3) 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

$$x \mapsto -A_6A_7x, \quad y \mapsto A_6A_7^2y \tag{2.1.4}$$

a (2.1.3) 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 (2.1.2), pero aquí dejamos la exposición y referimos al lector a [Sil09].

Solamente comentamos que si a priori tenemos funciones $x, y \in K(E)$ con polos de órdenes 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 (2.1.2), entonces esa relación algebraica define una curva elíptica isomorfa a E. Este método lo usaremos en la sección 6.3. □

Nota. Supongamos que tenemos una curva elíptica E/K con ecuación de Weierstrass $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ y constantes asociadas $b_2, b_4, b_6, b_8, c_4, c_6$, discriminante Δ y $j-$invariante j. Si aplicamos un cambio de variable admisible de la forma $x = u^2x' + r$ y $y = u^3y' + su^2x' + t$ (donde $u, r, s, t \in \overline{K}$ y $u \neq 0$), obtenemos una ecuación de Weierstrass de la forma $y'^2 + a_1'x'y' + a_3'y' = x'^3 + a_2'x'^2 + a_4'x' + a_6'$, donde los coeficientes, las constantes asociadas, el discriminante y el

$j-$invariante de esta nueva ecuación están dados por:

$$\begin{aligned}
ua_1' &= a_1 + 2s,\\
u^2a_2' &= a_2 - sa_1 + 3r - s^2,\\
u^3a_3' &= a_3 + ra_1 + 2t,\\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,\\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1,\\
u^2b_2' &= b_2 + 12r,\\
u^4b_4' &= b_4 + rb_2 + 6r^2,\\
u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3,\\
u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4,\\
u^4c_4' &= c_4,\\
u^6c_6' &= c_6,\\
u^{12}\Delta' &= \Delta,\\
j' &= j.
\end{aligned}$$

Estas fórmulas son estándar y se pueden encontrar en [Sil09, §3.1].

La ecuación 2.1.2 asociada a E/K se llama la *ecuación de Weierstrass generalizada* de E. Si la característica de K es distinta 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:

$$Y'^2 = 4X'^3 + b_2X'^2 + b_4X' + b_6, \tag{2.1.5}$$

donde

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

También definimos $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. Si la característica de K también es distinta 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 2.1.3. 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:

$$\Delta = -16(4A^3 + 27B^2) = \frac{c_4^3 - c_6^2}{1728} \qquad j(E) = -1728\frac{64A^3}{\Delta} = \frac{c_4^3}{\Delta}. \tag{2.1.6}$$

Nota. Si combinamos ambas ecuaciones para Δ y $j(E)$, obtenemos

$$j - 1728 = \frac{c_6^2}{\Delta}. \tag{2.1.7}$$

El discriminante Δ, y las constantes c_4 y c_6 caracterizan cuándo la curva definida por $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ es no singular y cuando resulta singular, caracterizan el tipo de singularidad:

Proposición 2.1.4. *Sea E la curva definida por una ecuación de Weierstrass $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Entonces*

1. *E es no singular $\iff$ $\Delta \neq 0$,*
2. *E tiene un punto singular $\iff$ $\Delta = 0$. El punto singular es un* nodo *si $c_4 \neq 0$ y una* cúspide *si $c_4 = 0$.*

Demostración. Véase la proposición 1.4 del capítulo III de [Sil09]. □

Si K' es una extensión arbitraria de K, entonces E/K es naturalmente una curva elíptica sobre K'. El j-invariante obtiene su nombre gracias al siguiente teorema importante:

Teorema 2.1.5. *Sean E y E' curvas elípticas definidas sobre un campo K y sea $\bar{K}$ una cerradura algebraica. Entonces las siguientes tres afirmaciones son equivalentes:*

1. *Existe una extensión finita K' de K tal que E es isomorfa a E' sobre K',*
2. *E es isomorfa a E' sobre $\bar{K}$,*
3. *$j(E) = j(E')$.*

Demostración. Véase la proposición III.1.4 de [Sil09]. □

Del teorema anterior, tenemos que una condición necesaria para que dos curvas E/K y E'/K sean isomorfas sobre K es que $j(E) = j(E')$. Entonces hay que pedirles una condición adicional:

Proposición 2.1.6. *Sean E y E' dos curvas elípticas sobre un campo K de característica diferente de 2 o 3. Supongamos además que $j(E), j(E') \neq 0, 1728$, entonces:*

$$E \cong_K E' \quad \iff \quad j(E) = j(E'),\ \frac{c_6}{c_6'} \in K^{*2},$$

donde c_6 (resp. c_6') es la constante asociada a una ecuación de Weierstrass para E (resp. E') sobre K.

Nota. Esta proposición se puede generalizar a campos de cualquier característica y para los valores $j = 0, 1728$.

Demostración. Como la característica de K es distinta de 2 y 3, entonces $y^2 = x^3 - 27c_4x - 54c_6$ (resp. $y^2 = x^3 - 27c_4'x - 54c_6'$) es una ecuación de Weierstrass de E (resp. E') sobre K.

($\Longrightarrow$) Por las fórmulas de cambio de variable, obtenemos $j(E) = j(E')$ y $c_6 = u^6c_6'$ para alguna $u \in K^*$. Por lo tanto $c_6/c_6' = u^6 \in K^{*2}$.

($\Longleftarrow$) Por hipótesis, tenemos que $c_6/c_6' = v^2$ para alguna $v \in K^*$ y también $j(E) = j(E')$. Por las fórmulas (2.1.6) y (2.1.7) tenemos que

$$\frac{c_4^3}{\Delta} = \frac{c_4'^3}{\Delta'}, \quad \frac{c_6^2}{\Delta} = \frac{c_6'^2}{\Delta'} \qquad \Longrightarrow \qquad \frac{c_4^3}{c_4'^3} = \frac{c_6^2}{c_6'^2} = v^4.$$

Definimos $w := c_4' c_6 / c_4 c_6'$, lo cual implica que

$$w = \frac{c_4'}{c_4} v^2 \quad \Longrightarrow \quad \frac{c_4}{c_4'} = \frac{v^2}{w} \quad \Longrightarrow \quad v^4 = \frac{c_4^3}{c_4'^3} = \frac{v^6}{w^3} \quad \Longrightarrow \quad w = \frac{v^2}{w^2} \in K^{*2}.$$

Entonces, si escribimos $u := v/w \in K$, i.e.

$$u = \frac{c_4}{c_4' v} = \frac{c_4 \sqrt{c_6'}}{c_4' \sqrt{c_6}},$$

de tal manera que $u^2 = w$, obtenemos:

$$c_4' u^4 = c_4' w^2 = \frac{c_4'^3 c_6^2}{c_4^2 c_6'^2} = \frac{c_4'^3}{c_4^2} \cdot \frac{c_4^3}{c_4'^3} = c_4,$$
$$c_6' u^6 = c_6' w^3 = \frac{c_4'^3 c_6^3}{c_4^3 c_6'^2} = \frac{c_6'^2}{c_6^2} \cdot \frac{c_6^3}{c_6'^2} = c_6.$$

Por lo tanto, el cambio de variable $x = u^2 x'$, $y = u^3 y'$ (donde $u \in K^*$) lleva la ecuación $y^2 = x^3 - 27c_4 x - 54c_6$ a la ecuación $y^2 = x^3 - 27c_4' x - 54c_6'$. Concluimos que $E \cong E'$ sobre K. □

Corolario 2.1.7. *Sea E (resp. E') una curva elíptica definida sobre $\mathbb{Q}$ con ecuación de Weierstrass $y^2 = x^3 - 27c_4 x - 54c_6$ (resp. $y^2 = x^3 - 27c_4' - 54c_6'$) y $j-$invariante distinto de 0 o 1728. Entonces:*

$$j(E) = j(E') \qquad \Longleftrightarrow \qquad E \cong_K E' \ \text{ donde } \ K = \mathbb{Q}(\sqrt{c_6 c_6'}).$$

Un isomorfismo está dado por el cambio de variable $x = u^2 x'$, $y = u^3 y'$ donde $u = c_4 \sqrt{c_6'}/c_4' \sqrt{c_6}$.

Demostración. Solamente hay que observar que c_6/c_6' es un cuadrado en el campo $\mathbb{Q}(\sqrt{c_6/c_6'}) = \mathbb{Q}(\sqrt{c_6 c_6'})$, ya que $\sqrt{c_6/c_6'} = \sqrt{c_6 c_6'}/c_6'$. □

Los puntos de E forman un grupo abeliano (cf. [Sil09, §3.2]). Para definir la operación geométricamente nos basamos en el celebrado teorema de Bézout[2] 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 una ecuación de Weierstrass de la forma 2.1.5 escrita sin tanta notación como:

$$E : Y^2 = 4X^3 + aX^2 + bX + c. \tag{2.1.8}$$

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

[2]Este teorema es famoso y se encuentra en muchos textos sobre curvas, por ejemplo en §5.3 de [Ful08].

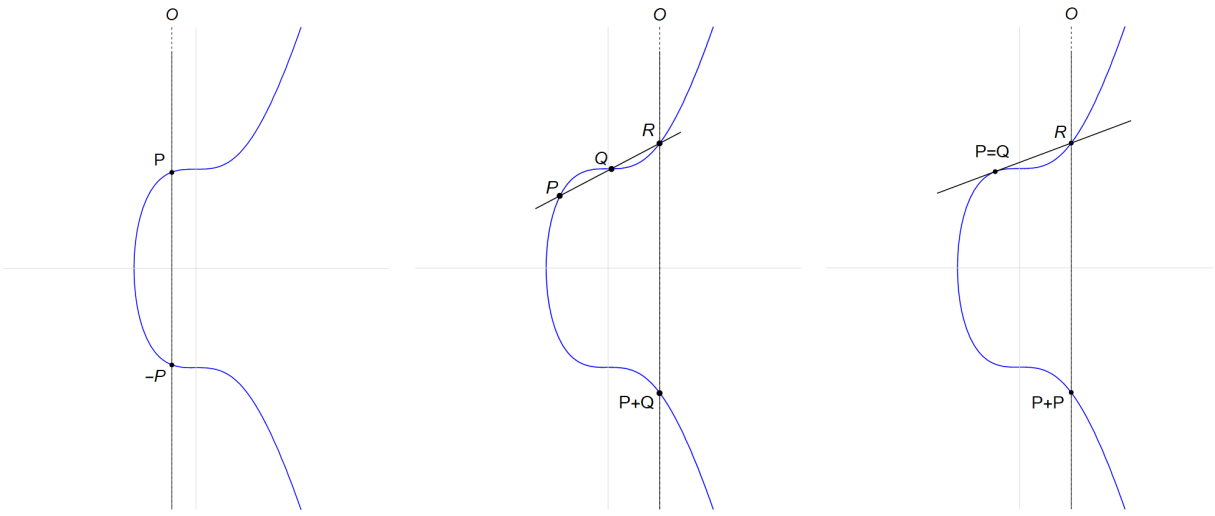


Figura 2.1: Construcción geométrica de la suma de puntos P y Q sobre una curva elíptica según si $P+Q=O$, $P\neq Q$ y $P=Q$ respectivamente.

multiplicidad tres. Por el teorema de Bézout, esto quiere decir que la curva E intersecta a la recta al infinito solamente en $O=[0,1,0]$; el punto O va a ser el neutro 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 2.1.8. 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 Bézout hay un tercer punto de intersección que puede ser O o 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

$$x(-P)=x(P), \qquad y(-P)=-y(P), \tag{2.1.9}$$

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 2.1 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 términos 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 (2.1.8) 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 raíces de 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:

$$x(P) + x(Q) + x(P + Q) = \lambda^2 - a, \tag{2.1.10}$$
$$x(P)x(Q) + x(P)x(P + Q) + x(Q)x(P + Q) = b - 2\lambda\mu,$$
$$x(P)x(Q)x(P + Q) = \mu^2 - c, \tag{2.1.11}$$

donde (2.1.10) nos dice que

$$x(P + Q) = \left(\frac{y(P) - y(Q)}{x(P) - x(Q)}\right)^2 - a - x(P) - x(Q) \quad \text{cuando} \quad P \neq Q. \tag{2.1.12}$$

La fórmula (2.1.11) la usaremos en la sección 6.3.

En general si tomamos una ecuación de Weierstrass generalizada $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ y un punto $P = (x, y) \neq O$, entonces las coordenadas de $2P$ son:

$$x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}, \tag{2.1.13}$$
$$y(2P) = \frac{1}{2}\left(\frac{2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)}{(2y + a_1x + a_3)^3} - a_3 - a_1x(2P)\right)$$

Estas fórmulas se llaman las fórmulas de duplicación. Véase III.2.3 y el ejercicio 3.25 de [Sil09] para más detalles.

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 muchos cálculos que no ilustran la teoría. Nos referimos a la sección III.2 de [Sil09] para las pruebas.

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

Teorema 2.1.8. *Sea $\varphi : E \to E'$ una isogenia de curvas elípticas, entonces cumple:*

I) *Para todas $P, Q \in E$, 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) *Por otro lado, 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 $\ker\varphi = C$.*

Demostración. Las pruebas de las tres partes son III.4.8, III.4.9 y III.4.12 de [Sil09] respectivamente. Solamente mencionamos un comentario adicional que hace Silverman: si E está definida 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 [Vé71] para más detalles.

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

Definición 2.1.9. 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 $\mathrm{Div}(E)$.

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:

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

donde ν_P es la valuación asociada a $K[E]_P$, la localización de $K[E]$ (el anillo de coordenadas de E) en el ideal maximal $\mathfrak{m}_P = \{f \in K[E] \mid f(P) = 0\}$. Recuerde que como E es lisa, $K[E]_P$ es un anillo de valuación discreta.[3] De esta manera, para un $f \in K[E]_P$ la valuación $\nu_P(f)$ se define como el único entero n tal que $f \in \mathfrak{m}_P^n$ pero $f \notin \mathfrak{m}_P^{n+1}$.

Definición 2.1.10. Un divisor D de E es *principal* si existe una función racional $f \in K(E)$ distinta de cero tal que $D = \mathrm{div}(f)$. Además hay una relación de equivalencia sobre $\mathrm{Div}(E)$: 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 $\mathrm{Pic}(E)$.

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

Proposición 2.1.11. *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).*

Demostración. Véase [Sil09, capítulo III, §3, corolario 3.5]. □

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

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

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

[3] 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 valuación discreta (cf. [AM94, §9,proposición 9.2]).

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 multiplicación por $N \in \mathbb{Z}$ nos permite estudiar el grupo de torsión de E.

Definición 2.1.12. 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

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

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

Proposición 2.1.13. *Sea E una curva elíptica sobre K y sea c la característica de 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 $c > 0$.

Demostración. Nada más probamos el caso cuando $K \subseteq \mathbb{C}$. Por el teorema de uniformización (teorema 2.2.3), existe una retícula 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 2.1.14. 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:

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

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

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell \quad (\text{característica de } K \neq \ell).$$

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 apareamiento de Weil. Para poder definirlo, necesitamos regresar a $E[m]$, construir ahí el apareamiento de Weil y después pasar al límite inverso.

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

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

donde

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

donde $e_{[m]}(R)$ es el índice de ramificación de $[m] : E \to E$ en $R \in E$. Con esto definimos el apareamiento 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 raíces m-ésimas de la unidad y $X \in E$ es un punto elegido de tal manera que g está bien definida 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. [Sil09, capítulo III, §8]). La función e_m cumple las siguientes propiedades:

Proposición 2.1.15. *El apareamiento de Weil e_m es una función bilineal, alternante, no-degenerada, invariante bajo la acción del grupo de Galois* $\operatorname{Gal}(\overline{K}|K)$ *y cumple:*

$$e_{mm'}(P, Q) = e_m\big([m']P, Q\big) \tag{2.1.14}$$

cf. [Sil09, 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 (2.1.14); 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 2.1.16. *Sea $\varphi \in \mathrm{End}(E)$ y $\varphi_\ell \in \mathrm{End}(T_\ell(E))$ el morfismo inducido, entonces*

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

Demostración. Véase [Sil09, capítulo III, §8, proposición 8.6] □

2.2. Curvas elípticas sobre $\mathbb{C}$

En el caso "geométrico" ($K = \mathbb{C}$), las curvas elípticas también se pueden describir usando retículas. 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 independientes o equivalentemente $\mathrm{Im}\,(z_1/z_2) \neq 0$. 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. Recuerde 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 2.2.1. 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 $\mathbb{C}(\Lambda)$. Observe que una función elíptica define una función meromorfa sobre $\mathbb{C}/\Lambda$

La función elíptica más importante para clasificar curvas elípticas con retículas 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. [Apo90, §1.6, teorema 1.10] o [Ahl79, 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 escribimos $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$ 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. [Sil09, capítulo 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 2.2.2. *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. lisa) 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 la curva cúbica asociada en $\mathbb{P}^2(\mathbb{C})$.

Demostración. Véase [Sil09, 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 2.2.3. *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 2.2.2 y 2.2.3 también son homomorfismos de grupo, i.e. de grupos de Lie.

2.3. 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. [Sil09, capítulo V, teorema 1.1]). En esta sección calcularemos $\#E(\mathbb{F}_q)$ usando la traza del morfismo de Frobenius que está definido para cualquier curva elíptica sobre un campo finito.

El morfismo 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 2.3.1. *Sea $E/\mathbb{F}_q$ una curva elíptica, $\varphi : E \to E$ el morfismo de Frobenius de orden q y escriba $a_q(E) := q + 1 - \#E(\mathbb{F}_q)$. 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 morfismo de Frobenius satisface $\varphi^2 - a_q(E)\varphi + q = 0 \in \mathrm{End}(E)$.*

Demostración. Como el grupo absoluto de Galois $G_{\mathbb{F}_q}$ es generado topológicamente por el morfismo 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. [Sil09, capítulo III, corolario 5.5]) y las isogenias separables cumplen que $\#\ker\varphi = \deg\varphi$ (cf. [Sil09, capítulo III, teorema 4.10.c]), tenemos que

$$\#E(\mathbb{F}_q) = \#\ker(1 - \varphi) = \deg(1 - \varphi). \tag{2.3.1}$$

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 2.1.16 a 2.3.1 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 2.1.16 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 finitos también surgen de curvas elípticas definidas sobre $\mathbb{Q}$ o en general sobre campos locales (i.e. localmente compactos con respecto a 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:

$$\mathbb{Z}_{(p)} \xrightarrow{\mathrm{mod}\, p} \tfrac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} \cong \tfrac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p.$$

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 2.3.2. Sea $E/\mathbb{Q}$ una curva 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 lisa (o equivalentemente que la ecuación $y^2 = ax^3+bx^2+cx+d \pmod p$ tiene tres raíces 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 raíz de multiplicidad dos y otra raíz 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 raíz 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.

2.4. Curvas elípticas sobre campos locales

En esta sección estudiamos el caso cuando una curva elíptica E está definida sobre un campo local K, i.e. un campo completo con respecto de una valuación no arquimediana discreta ν. El ejemplo más usado es cuando K es una extensión finita de $\mathbb{Q}_p$, los racionales $p-$ádicos junto con la extensión (única) de la valuación p-ádica de $\mathbb{Q}_p$ a K. Fijamos la siguiente notación:

1. $\mathcal{O} := \{x \in K \mid \nu(x) \geq 0\}$ es el anillo de enteros de K.

2. $\mathfrak{m} := \{x \in K \mid \nu(x) > 0\}$ es el ideal maximal del anillo local $\mathcal{O}$.

3. $k := \mathcal{O}/\mathfrak{m}$ es el campo residual de $\mathcal{O}$.

4. $\pi \in \mathcal{O}$ es un generador del ideal principal $\mathfrak{m}$, es decir $\mathfrak{m} = (\pi)$. Además asumimos que $\nu(\pi) = 1$, i.e. ν es una valuación normalizada.

Recuerde que K es el campo de cocientes de $\mathcal{O}$ y que todo elemento de K se puede expresar como una serie de Laurent en π y en particular para toda $x \in K$ existe una $n \geq 0$ tal que $\pi^n x \in \mathcal{O}$.

Ahora consideremos E una curva elíptica sobre K con una ecuación de Weierstrass generalizada:

$$y^2 + a_1xy + y = x^3 + a_2x^2 + a_4x + a_6, \qquad (a_i \in K). \tag{2.4.1}$$

Por el comentario anterior, para cada coeficiente a_i existe un exponente n_i tal que $\pi^{n_i}a_i \in \mathcal{O}$. Si tomamos $N = \text{máx}\{a_1, \ldots, a_6\}$, entonces tenemos que $\pi^N a_i \in \mathcal{O}$ para toda i. Por lo tanto si hacemos el cambio de variable admisible $x' = \pi^{-2N}x$, $y' = \pi^{-3N}y$, obtenemos la siguiente ecuación de Weierstrass:

$$y'^2 + \pi^N a_1 x'y' + \pi^{3N} a_3 y' = x'^3 + \pi^{2N} a_2 x'^2 + \pi^{4N} a_4 x' + \pi^{6N} a_6,$$

donde cada coeficiente $\pi^{iN}a_i \in \mathcal{O}$. Por lo tanto podemos asumir *a priori* que la ecuación de Weierstrass (2.4.1) de la curva E/K tiene coeficientes en $\mathcal{O}$.

Con esta suposición, tenemos que los coeficientes de Weierstrass de E cumplen $a_i \in \mathcal{O}$. Como Δ es un polinomio en los coeficientes de Weierstrass, tenemos que $\Delta \in \mathbb{Z}[a_1, \ldots, a_6] \subseteq \mathcal{O}$ y por lo tanto $\nu(\Delta) \geq 0$. Con esto podemos definir ecuaciones de Weierstrass minimales, i.e. ecuaciones tales que $\nu(\Delta)$ es mínimo dentro de otras ecuaciones de Weierstrass con coeficientes en $\mathcal{O}$. Más precisamente:

Definición 2.4.1. Sea E una curva elíptica sobre un campo local K. Decimos que una ecuación $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ de E/K es una *ecuación minimal de Weierstrass*, si cumple las siguientes dos propiedades:

1. $a_1, \ldots, a_6 \in \mathcal{O}$.

2. Si $y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$ es otra ecuación de Weierstrass de E/K con $a_i' \in \mathcal{O}$ y discriminante Δ', entonces $\nu(\Delta) \leq \nu(\Delta')$.

Nota. Bajo cualquier cambio de variable admisible $x = u^2x' + r$, $y = u^3y' + u^2sx' + t$, tenemos que el discriminante se transforma como $\Delta' = u^{-12}\Delta$ y por lo tanto $\nu(\Delta') = \nu(\Delta) - 12\nu(u)$. Esto lo escribimos como $\nu(\Delta') \in \nu(\Delta) + 12\mathbb{Z}$. Similarmente tenemos que $\nu(c_4') \in \nu(c_4) + 4\mathbb{Z}$ y $\nu(c_6') \in \nu(c_6) + 6\mathbb{Z}$. De esta manera, si la ecuación de Weierstrass no es miminal, podemos reducir los valores de $\nu(\Delta), \nu(c_4)$ y $\nu(c_6)$ por múltiplos de 12, 4 y 6 respectivamente. Por lo tanto tenemos la siguiente condición suficiente para que una ecuación de Weierstrass sea minimal: sea $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ una ecuación de Weierstrass para E/K donde $a_i \in \mathcal{O}$, si Δ, c_4 o c_6 cumplen una de las siguientes tres propiedades:

$$\nu(\Delta) < 12, \;\; \nu(c_4) < 4 \;\text{ o }\; \nu(c_6) < 6 \quad \Longrightarrow \quad \text{la ecuación de Weierstrass es minimal.} \tag{2.4.2}$$

Ejemplo 2.4.2. Tomemos la curva elíptica E definida por $y^2 + xy + y = x^3 - x - 2$. Como los coeficientes son racionales, podemos pensar que E está definida sobre $\mathbb{Q}_p$ para todo primo p con la valuación $p-$ádica ν_p. El discriminante es $\Delta = -2 \cdot 5^4$, entonces por el criterio anterior tenemos que $\nu_p(2 \cdot 5^4) < 12$ para todo primo p. Por lo tanto la ecuación de Weierstrass es minimal.

En seguida enunciamos algunas propiedades que cumplen las ecuaciones minimales y en particular las propiedades que cumplen los cambios de variables admisibles que producen ecuaciones minimales.

Proposición 2.4.3. *Sea E una curva elíptica definida sobre un campo local K. Entonces:*

1. *E tiene una ecuación de Weierstrass minimal.*

2. *Cualesquiera dos ecuaciones de Weierstrass minimales son equivalentes mediante un cambio de variable admisible de la forma:*

$$x = u^2x' + r, \quad y = u^3y' + u^2x's + t, \quad (u \in \mathcal{O}^*,\ r, s, t \in \mathcal{O}).$$

3. *Por otro lado, si el cambio de variable $x = u^2x' + r$, $y = u^3y' + u^2x's + t$ lleva la ecuación de E en una ecuación de Weierstrass minimal, entonces $u, r, s, t \in \mathcal{O}$.*

Demostración. La existencia de la ecuación minimal se sigue de que ν es discreta. Los otros incisos se siguen de las fórmulas que describen la transformación de los coeficientes de Weierstrass bajo cambios de coordenadas admisibles. Véase la proposición 1.3 del capítulo VII de [Sil09] para más detalles. □

Ahora, como las ecuaciones minimales siempre existen, para toda curva elíptica E/K, podemos reducir la ecuación minimal módulo $\mathfrak{m} = (\pi)$. Sabemos que la reducción módulo $\mathfrak{m}$ es un homomorfismo suprayectivo $\mathcal{O} \twoheadrightarrow k$ que hace $x \mapsto x \pmod{\pi}$. Esto lo denotamos por $x \mapsto \bar{x}$ para simplificar la notación. Por lo tanto si $y^2 + a_1xy + y = x^3 + a_2x^2 + a_4x + a_6$ es una ecuación minimal de E, tenemos que $a_i \in \mathcal{O}$ entonces reducimos cada coeficiente módulo $\mathfrak{m}$ para obtener la siguiente ecuación polinomial sobre el campo residual k:

$$\bar{E} \ : \ y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6, \quad (\bar{a}_i \in k)$$

Este proceso se puede generalizar para definir una función de "reducción módulo $\mathfrak{m}$" sobre el espacio proyectivo $\mathbb{P}^n(K)$ sobre un campo local. Sea $P \in \mathbb{P}^n(K)$ con coordenadas homogéneas $P = [x_0, \ldots, x_n]$ y supongamos que $m = \min\{\nu(x_0), \ldots, \nu(x_n)\}$. Entonces $\pi^{-m}x_i \in \mathcal{O}$ para toda $i = 0, \ldots, n$ y hay un índice j tal que $\pi^{-m}x_j \in \mathcal{O}^*$ (el índice j es tal que $\nu(x_j)$ es mínimo). Por lo tanto podemos asumir que las coordenadas homogéneas de P son elementos de $\mathcal{O}$ y al menos una coordenada pertenece a $\mathcal{O}^*$. De esta manera definimos la reducción módulo $\mathfrak{m}$ del espacio $\mathbb{P}^n(K)$ como la función:

$$\bar{\cdot} : \mathbb{P}^n(K) \longrightarrow \mathbb{P}^n(k) \quad \text{donde} \quad P = [x_0, \ldots, x_n] \mapsto \bar{P} := [\bar{x}_0, \ldots, \bar{x}_n].$$

Es claro que la reducción módulo $\mathfrak{m}$, se restringe a la siguiente función:

$$E(K) \longrightarrow \bar{E}(k), \quad \text{donde} \quad P \mapsto \bar{P}.$$

En el caso común, cuando K es una extensión finita de $\mathbb{Q}_p$, tenemos que k es una extensión finita de $\mathbb{F}_p$ y por lo tanto $\bar{E}$ es una curva elíptica sobre un campo finito.

En general, $\bar{E}$ puede ser una curva singular. Es posible que un punto $P \in E(K)$ (no singular) se reduce a un punto singular $\bar{P} \in \bar{E}(k)$ que sea nodo o cúspide. En seguida clasificamos estas posibilidades:

Definición 2.4.4. Sea E una curva elíptica sobre un campo local K y sea $\bar{E}$ la reducción módulo $\mathfrak{m}$ de una ecuación de Weierstrass minimal para E, entonces:

1. E tiene *reducción buena*, si $\bar{E}$ es no singular (i.e. $\nu(\Delta) = 0$)
2. E tiene *reducción multiplicativa*, si $\bar{E}$ es singular con un nodo (i.e. $\nu(\Delta) > 0$ y $\nu(c_4) = 0$).
3. E tiene *reducción aditiva*, si $\bar{E}$ es singular con una cúspide (i.e. $\nu(\Delta), \nu(c_4) > 0$).

Si E/K no tiene reducción buena (i.e. tiene reducción multiplicativa o aditiva), decimos que E tiene *reducción mala*. Si E/K no tiene reducción aditiva, decimos que E es *semiestable*.

Ejemplo 2.4.5. (Cont. de ejemplo 2.4.2) Sea $E/\mathbb{Q}_p$ la curva elíptica definida por $y^2 + xy + y = x^3 - x - 2$. Recuerde que $\Delta = -1250 = -2 \cdot 5^4$ y $c_4 = 25$. Entonces para $p = 2$, $E/\mathbb{Q}_2$ tiene reducción multiplicativa y en $p = 5$ tiene reducción aditiva. Por lo tanto $E/\mathbb{Q}_p$ es semiestable si y solo si $p \neq 5$.

El nombre de reducción multiplicativa (resp. aditiva) viene del hecho que el grupo de puntos no singulares en $\bar{E}(\bar{k})$ es isomorfo al grupo multiplicativo $\bar{k}^*$ (resp. el grupo aditivo $\bar{k}^+$). Véase III.2.5 y VII.5.1 de [Sil09] para más detalles. La palabra *semiestable* viene del hecho que el tipo de reducción de E/K se preserva de maneras distintas bajo extensiones K'/K de campos locales. Más precisamente:

Teorema 2.4.6. *(de reducción semiestable) Sea E una curva elíptica sobre un campo local K y sea K' una extensión de campos locales*[4] *finita de K, entonces si E/K es semiestable, entonces E/K' es semiestable. Por otro lado para toda curva E/K, existe una extensión finita K'/K tal que E/K' es semiestable.*

Nota. En general, si K'/K es una extensión no ramificada, el tipo de reducción de E/K es equivalente al tipo de reducción de E/K'. Esto, junto con la proposición anterior, Silverman lo llama el "Semistable Reduction Theorem" y lo prueba para el caso cuando la característica de k es mayor que 3 (cf. [Sil09, VII.5.4]). El caso general se deduce del *algoritmo de Tate*, véase [Tat75] para la fuente original o [Cre97, §3.2] para el algoritmo explícito y un resumen de las definiciones necesarias.

Cuando la reducción de E/K es buena, la curva $\bar{E}$ es elíptica y nos permite encajar grupos de $m-$torsión de E en $\bar{E}(k)$. Más precisamente:

Proposición 2.4.7. *Sea E una curva elíptica sobre un campo local K con campo residual k de característica ℓ y sea $m \geq 1$ primo relativo con ℓ. Si E tiene buena reducción, entonces la función $\mathbb{P}^2(K) \to \mathbb{P}^2(k)$ de reducción módulo $\mathfrak{m}$ se restringe a una inclusión:*

$$E(K)[m] \hookrightarrow \bar{E}(k),$$

donde $E(K)[m]$ es el conjunto de puntos de $E(K)$ de orden m.

La inclusión $E(K)[m] \hookrightarrow \bar{E}(k)$ nos permite estudiar la reducción buena en términos de la acción del grupo de Galois de la extensión $\overline{K}/K$. Para desarrollar esta idea, primero recordemos que el grupo de Galois absoluto $G_K := \mathrm{Gal}(\overline{K}/K)$ admite una proyección sobre el grupo de Galois absoluto del campo residual k, i.e. el homomorfismo

$$\pi : G_K \longrightarrow G_k, \quad \text{definido por} \quad \sigma \mapsto \big(x + \mathfrak{m} \mapsto \sigma(x) + \mathfrak{m}\big)$$

es suprayectivo. De hecho $G_k \cong \mathrm{Gal}(K^{\mathrm{nr}}/K)$ donde K^{nr} es la extensión maximal no ramificada de K. Al núcleo de este homomorfismo lo llamamos el *subgrupo de inercia* de K y lo denotamos I_ν porque depende únicamente de la valuación ν. Es claro de la definición que I_ν es el subgrupo de elementos de G_K que actúan trivialmente módulo $\mathfrak{m}$. Con esto definimos:

Definición 2.4.8. Sea K un campo local con valuación ν y sea X un conjunto con una acción $G_K \curvearrowright X$. Decimos que X es *no ramificado* en ν si la restricción de la acción al subgrupo de inercia I_ν es trivial, i.e. si $\sigma \in I_\nu$, entonces $\sigma(x) = x$ para toda $x \in X$.

Ahora la acción usual $G_K \curvearrowright E(\overline{K})$ se restringe a una acción a los puntos de $m-$torsión: $G_K \curvearrowright E[m]$ (cf. sección 5.2). La reducción buena de la curva E/K se puede caracterizar con la acción $I_\nu \curvearrowright E[m]$. Este resultado fue probado por Néron, Ogg y Shafarevich, y lleva su nombre:

[4] Un campo local (K', ν') es una extensión de un campo local (K, ν) si ν' es una extensión de ν, i.e. $\nu'(x) = \nu(x)$ para toda $x \in K$.

Teorema 2.4.9. *(Criterio de Néron-Ogg-Shafarevich) Sea E una curva elíptica sobre un campo local K con valuación ν. Sea p la característica del campo residual k de K. Entonces las siguientes condiciones son equivalentes:*

1. *E tiene buena reducción sobre K.*
2. *$E[m]$ es no ramificada en ν para toda $m \geq 1$ tal que $(m, p) = 1$.*
3. *$T_\ell(E)$ es no ramificada en ν para algún primo $\ell \neq p$.*
4. *$E[m]$ es no ramificada en ν para una infinidad de enteros $m \geq 1$ tales que $(m, p) = 1$.*

Demostración. Véase el teorema VII.7.1 de [Sil09]. □

Un corolario importante del criterio de Nerón-Ogg-Shafarevich es que la reducción buena es invariante bajo isogenias:

Corolario 2.4.10. *Sean E/K y E'/K curvas elípticas sobre un campo local y $\varphi : E \to E'$ una isogenia definida sobre K, entonces E tiene buena reducción si y sólo si E' tiene buena reducción.*

(cf. el corolario VII.7.2 de [Sil09])

Para cerrar la sección mencionamos un resultado de Cassels que calcula la valuación de las coordenadas de un punto de $m-$torsión. El siguiente resultado se usará para calcular condiciones de integrabilidad de las coordenadas de los puntos de torsión de $E(\mathbb{Q})$.

Proposición 2.4.11. *Sea E/K una curva elíptica sobre un campo local K de característica cero y con campo residual de característica $\ell > 0$. Sea $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ una ecuación de Weierstrass con $a_i \in \mathcal{O}$, i.e. $\nu(a_i) \geq 0$ para toda i. Sea $P \in E(K)[m]$ un punto de orden m con coordenadas $x(P)$ y $y(P)$. Entonces según la forma de m tenemos:*

1. *Si $m \neq \ell^n$ para toda $n > 0$, entonces $x(P), y(P) \in \mathcal{O}$,*
2. *Si $m = \ell^n$, entonces $\pi^{2r}x(P), \pi^{3r}y(P) \in \mathcal{O}$ donde $r = [\nu(\ell)/(\ell^n - \ell^{n-1})]$, i.e. la parte entera del racional $\nu(\ell)/(\ell^n - \ell^{n-1})$.*

Demostración. [Cas49] o [Sil09, VII.3.4] para una prueba con grupos formales. □

2.5. Curvas elípticas sobre campos globales

En esta sección estudiaremos curvas elípticas definidas sobre campos globales y en particular sobre extensiones finitas de $\mathbb{Q}$. Fijamos la siguiente notación para el resto de esta sección:

1. K es una extensión finita de $\mathbb{Q}$ con anillo de enteros $\mathcal{O}$.
2. M_K es el conjunto de valores absolutos sobre K, módulo equivalencia topológica.[5]

[5]Un *valor absoluto* sobre K es una función $|\,| : K \to \mathbb{R}_{\geq 0}$, cuya acción la denotamos por $x \mapsto |x|$, que cumple las siguientes tres propiedades:

a) $|x| = 0$ si y solo si $x = 0$,

b) $|xy| = |x|\,|y|$ para toda $x, y \in K$,

3. Para toda $|\,| \in M_K$ definimos la valuación asociada $\nu(x) = -\log |x|_\nu$. Si $|\,|$ es no arquimediano, asumimos que el logaritmo se toma con la base adecuada para que ν esté normalizada, i.e. $\nu(K^*) = \mathbb{Z}$. Gracias a esta asociación, es común referirse a un valor absoluto por su valuación asociada, i.e. a los elementos de M_K los denotamos por ν y al valor absoluto de una $x \in K$ lo denotamos por $|x|_\nu$.

4. $M_K^0 \subset M_K$ es el subconjunto de valores absolutos no arquimedianos y $M_K^\infty \subset M_K$ el subconjunto de valores absolutos arquimedianos. Recuerde que M_K^0 está en biyección con los ideales primos ($\neq 0$) de $\mathcal{O}$, entonces al ideal primo de $\mathcal{O}$ que corresponde a $\nu \in M_K^0$ lo denotamos por $\mathfrak{p}_\nu$.

5. K_ν es la completación de K con respecto de $\nu \in M_K$. Si $\nu \in M_K^0$, K_ν es un campo local y por lo tanto tiene un anillo de enteros $\mathcal{O}_\nu$ local con ideal maximal $\mathfrak{m}_\nu$ y campo residual k_ν.

Esta notación vuelve a aparecer en las secciones 4.1, 5.1 y 6.4.

El teorema principal que cumplen las curvas elípticas sobre un campo global es el teorema de Mordell-Weil:

Teorema 2.5.1. *Sea E una curva elíptica sobre un campo global K. Entonces $E(K)$ es un grupo abeliano finitamente generado. En particular existe un entero $r \geq 0$, llamado el* rango *de E, tal que*

$$E(K) \cong E(K)_{\text{tor}} \oplus \mathbb{Z}^r,$$

donde $E(K)_{\text{tor}}$, el subgrupo de torsión, es finito.

Demostración. Véase el capítulo VIII de [Sil09] y en particular VIII.6.7. □

Nota. La existencia de la isogenia dual junto con la finitud de los núcleos de las isogenias implican que el rango de $E(K)$ es invariante bajo isogenias. En efecto:

Sean E y E' curvas elípticas sobre un campo global K, denotamos por $G = E(K)$ (resp. $G' = E'(K)$) a sus grupos de puntos racionales. Sea $\varphi : E \to E'$ una isogenia definida sobre K, entonces φ se restringe a un homomorfismo de grupos $\varphi : G \to G'$. Por otro lado, si denotamos por r (resp. r') al rango de G (resp. r'), entonces

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

Por el inciso II), Como el núcleo de φ es finito por el teorema 2.1.8.II), tenemos que $\ker \varphi \subseteq G_{\text{tor}}$. Por lo tanto φ se factoriza a través de un homomorfismo $\bar{\varphi}$ inyectivo:

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

c) $|x+y| \leq |x| + |y|$ para toda $x, y \in K$.

Si además el valor absoluto cumple la siguiente condición más fuerte:

d) $|x+y| \leq \max\{|x|, |y|\}$,

decimos que es *no arquimediano*. Los valores absolutos que no cumplen (d) se llaman *arquimedianos*.

Gracias a los incisos a) y c), la función $(x, y) \mapsto |x - y|$ es una métrica y por lo tanto induce una topología sobre K. Decimos que dos valores absolutos $|\cdot|_1$ y $|\cdot|_2$ son equivalentes si K_1 es homeomorfo a K_2 donde K_i es K con la topología inducida por $|\cdot|_i$.

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

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

En el caso $K = \mathbb{Q}$, está conjeturado que el rango de $E/\mathbb{Q}$ está completamente determinado por la función L de E. Más precisamente tenemos:

Conjetura. *(Birch y Swinnerton-Dyer) Sea $E/\mathbb{Q}$ una curva elíptica con rango r y sea $L(E,s)$ la extensión holomorfa a todo el plano complejo de la función L de E. Entonces r es el orden de $L(E,s)$ en $s = 1$, i.e la serie de Taylor de $L(E,s)$ alrededor de $s = 1$ es de la forma:*

$$L(E,s) = c_r(s-1)^r + c_{r+1}(s-1)^{r+1} + \cdots, \quad (c_r \neq 0).$$

Esta conjetura aparece de esta manera por primera vez en [SDB65]. Véase [CWJ06] para una descripción breve e histórica de la conjetura de Birch y Swinnerton-Dyer para introducir la conjetura como uno de los premios milenarios del instituto Clay. Para un tratado más completo sobre la conjetura, véase [Tat66].

El grupo de torsión de $E(\mathbb{Q})$ es mejor conocido. El teorema de Mazur caracteriza las diferentes posibles estructuras de $E(\mathbb{Q})_{\text{tor}}$:

Teorema 2.5.2. *(Mazur) Sea E una curva elíptica sobre $\mathbb{Q}$, entonces $E(\mathbb{Q})_{\text{tor}}$ es isomorfo a uno de los siguientes quince grupos:*

1. *$\mathbb{Z}/N\mathbb{Z}$ para $1 \leq N \leq 10$ o $N = 12$,*
2. *$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ para $1 \leq N \leq 4$.*

Demostración. Véase el teorema 5.1 de §5 del capítulo III de [Maz77]. □

Nota. En particular $\#E(\mathbb{Q})_{\text{tor}} \leq 16$ para toda curva elíptica $E/\mathbb{Q}$.

Para curvas elípticas sobre $\mathbb{Q}$, hay un algoritmo que nos permite calcular $E(\mathbb{Q})_{\text{tor}}$ debido a T. Nagell y E. Lutz que fue probado independientemente por ambos en los 1930's. La prueba primero apareció en [Nag35] y después en [Lut37].

Teorema 2.5.3. *(Lutz-Nagell) Sea $E/\mathbb{Q}$ una curva elíptica con ecuación de Weierstrass*

$$y^2 = x^3 + Ax + B, \quad (A, B \in \mathbb{Z}). \tag{2.5.1}$$

A la ecuación de Weierstrass le asociamos el entero $D := -\Delta/16 = 4A^3 + 27B^2$, además denotamos $G = E(\mathbb{Q})$ y escribimos $x(P)$ y $y(P)$ como las coordenadas de $P \in G$ dadas por (2.5.1)*. Entonces para todo $P \in G_{\text{tor}}$ tenemos que $x(P), y(P) \in \mathbb{Z}$ y*

$$P + P = O \quad o \quad y(P)^2 \mid D.$$

Demostración. Como las coordenadas de la ecuación de Weierstrass son elementos de $\mathbb{Z} = \cap_p \mathbb{Z}_p$, donde $\mathbb{Z}_p$ es el anillo de enteros de $\mathbb{Q}_p$, entonces E está definida sobre $\mathbb{Q}_p$ para todo primo p y podemos aplicar la proposición 2.4.11 a cada p para concluir que $x(P), y(P) \in \mathbb{Z}$. Las condiciones necesarias sobre el punto P se deducen de un cálculo sencillo que involucra la fórmula de duplicación (2.1.13). Véase el corolario VIII.7.2 de [Sil09] para más detalles. □

Ahora introducimos un equivalente de discriminante minimal para campos globales. Sea E/K una curva elíptica con ecuación de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (a_i \in K).$$

Para todo valor absoluto no arquimediano $\nu \in M_K^0$, tenemos que $K \hookrightarrow K_\nu$. Entonces la curva elíptica E/K la podemos interpretar como una curva elíptica sobre el campo local K_ν con la misma ecuación de Weierstrass. Por la proposición 2.4.3, para toda $\nu \in M_K^0$ podemos encontrar un cambio de coordenadas que lleve la ecuación de E/K_ν a una ecuación minimal:

$$y^2 + a_{1,\nu}xy + a_{3,\nu}y = x^3 + a_{2,\nu}x^2 + a_{4,\nu}x + a_{6,\nu}, \qquad (a_{i,\nu} \in \mathcal{O}_\nu)$$

con discriminante minimal Δ_ν, en particular $\nu(\Delta_\nu) \geq 0$. Con esto en mente definimos:

Definición 2.5.4. Con la notación del párrafo anterior, el *discriminante minimal* de E es el ideal de $\mathcal{O}$ definido como

$$D_{E/K} := \prod_{\nu \in M_K^0} \mathfrak{p}_\nu^{\nu(\Delta_\nu)},$$

donde $\mathfrak{p}_\nu$ es el ideal primo de $\mathcal{O}$ asociado a ν.

Es posible que la ecuación de Weierstrass original de E/K es minimal para ν. En este caso no es necesario hacer un cambio de variable para convertir la ecuación en una minimal para E/K_ν. A veces es posible que la ecuación de Weierstrass de E/K es una ecuación minimal para E/K_ν para toda ν. Este tipo de ecuaciones de Weierstrass son importantes:

Definición 2.5.5. Sea E/K una curva elíptica sobre un campo global K. Decimos que una ecuación $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_5x + a_6$ para E sobre K es una *ecuación de Weierstrass minimal global*, si $a_i \in \mathcal{O}$ y si para toda $\nu \in M_K^0$ tenemos que la ecuación es minimal sobre el campo local K_ν (cf. definición 2.4.1).

Las ecuaciones de Weierstrass minimales globales se pueden caracterizar con el discriminante minimal y esto permite garantizar su existencia para una clase grande de curvas.

Proposición 2.5.6. *Una ecuación de Weierstrass de E/K con discriminante Δ es minimal global si y solo si $D_{E/K} = (\Delta)$. En particular, si K tiene número de clase 1 (i.e. $\mathcal{O}$ es un dominio de factorización única) entonces toda curva elíptica E/K, admite una ecuación de Weierstrass minimal global.*

Demostración. Véase la sección VIII.8 de [Sil09] para más detalles, en particular el corolario VIII.8.3. □

Ejemplo 2.5.7. (continuación del ejemplo 2.4.2) Definimos E/Q con la ecuación de Weierstrass $y^2 + xy + y + x^3 - x - 2$. Recuerde que $\Delta = -2 \cdot 5^4$ entonces para todo primo p tenemos que $\nu_p(\Delta) \leq \nu_5(\Delta) = 4 < 12$ (donde ν_p es la valuación p-adica)y por lo tanto la ecuación es una ecuación de Weierstrass minimal para $E/\mathbb{Q}_p$ para toda p primo. Por lo tanto $y^2+xy+y+x^3-x-2$ es una ecuación de Weierstrass minimal global. Observe que

$$D_{E/\mathbb{Q}} = \prod_p (p)^{\nu_p(\Delta)} = (2)^1(5)^4 = (\Delta).$$

Ahora estudiamos la reducción de las curvas E/K, basándonos en la reducción de las curvas elípticas E/K_ν.

Definición 2.5.8. Sea E/K una curva elíptica sobre un campo global. Decimos que E tiene *reducción buena* (resp. *multiplicativa*, *aditiva*) en $\nu \in M_K^0$ si la curva elíptica E/K_ν tiene reducción buena (resp. multiplicativa, aditiva). Decimos que E/K es semiestable si tiene reducción semiestable sobre toda $\nu \in M_K^0$.

Como solamente hay una cantidad finita de valuaciones no arquimedianas (i.e. primos) donde $E/\mathbb{Q}$ tiene reducción mala (ya que los primos asociados a las valuaciones necesariamente dividen al conductor de E, cf. la definición 2.5.11 más adelante), entonces tenemos el siguiente resultado que generaliza parte del teorema 2.4.6:

Proposición 2.5.9. *Sea $E/\mathbb{Q}$ una curva elíptica, entonces existe una extensión finita $K/\mathbb{Q}$ tal que E/K es semiestable.*

Demostración. Sean $\{p_1, \ldots, p_n\} \subset M_{\mathbb{Q}}^0$ el conjunto de primos (i.e. valuaciones) donde E tiene reducción mala, i.e. $E/\mathbb{Q}_{p_i}$ tiene reducción mala para $i \in \{1, \ldots, n\}$. Por el teorema 2.4.6 existe una extensión finita $F_i/\mathbb{Q}_{p_i}$ tal que E/F_i tiene reducción semiestable. Sea $F_i'/\mathbb{Q}$ la extensión finita de $\mathbb{Q}$ cuya completación con respecto de la valuación p_i-ádica es F_i. Con esto sea $K/\mathbb{Q}$ una extensión finita que contiene a los campos $F_1', \ldots, F_n'$ y sea $K_i/\mathbb{Q}_{p_i}$ la completación p_i-ádica de K, i.e. K_i es una extensión finita de F_i. Gracias al teorema 2.4.6 tenemos que E/K_i tiene reducción semiestable para toda $i \in \{1, \ldots, n\}$.

Sea p un primo donde E tiene reducción semiestable, i.e. $E/\mathbb{Q}_p$ tiene reducción semiestable. Gracias al teorema 2.4.6, para toda extensión finita L de $\mathbb{Q}$ tenemos que E/L_p es semiestable donde L_p es la completación de L con respecto de la valuación p-ádica en $\mathbb{Q}$. En particular si tomamos $L = K$, entonces E/K_ν es semiestable para toda $\nu \in M_K^0$. □

Ejemplo 2.5.10. (continuación del ejemplo 2.4.5) Si $E/\mathbb{Q}$ es la curva elíptica definida por $y^2+xy+y = x^3-x-2$, vimos en el ejercicio 2.4.5 que $E/\mathbb{Q}_p$ tiene reducción buena para toda $p \neq 2, 5$, $E/\mathbb{Q}_2$ tiene reducción multiplicativa y $E/\mathbb{Q}_5$ tiene reducción aditiva. Por lo tanto $E/\mathbb{Q}$ es semiestable en todo primo $p \neq 5$.

Para terminar la sección introducimos un último invariante aritmético de curvas elípticas sobre campos globales que mide la reducción de la curva en los diferentes lugares no arquimedianos.

Definición 2.5.11. Sea E/K una curva elíptica definida sobre un campo global K. El *conductor* de E es el ideal de $\mathcal{O}$ definido por

$$N_{E/K} := \prod_{\nu \in M_K^0} \mathfrak{p}_\nu^{f_\nu(E/K)},$$

donde el exponente $f_\nu(E/K)$ está dado por:

$$f_\nu(E/K) := \begin{cases} 0 & E \text{ tiene buena reducción en } \nu \\ 1 & E \text{ tiene reducción multiplicativa en } \nu \\ 2 & E \text{ tiene reducción aditiva en } \nu \text{ y } \mathfrak{p}_\nu \nmid 6 \\ 2 + \delta_\nu(E/K) & E \text{ tiene reducción aditiva en } \nu \text{ y } \mathfrak{p}_\nu \mid 6 \end{cases}.$$

El término $\delta_\nu(E/K)$ es el "l'invariant sauvage" [6] de Serre que de cierta manera mide la ramificación de las diferentes extensiones $K_\nu(E[m])/K_\nu$, donde $K_\nu(E[m])$ es la extensión de K_ν generada por las coordenadas de los puntos de $m-$torsión.

Nota. Gracias a la definición del conductor de E, tenemos que

$$E/K \text{ es semiestable} \iff N_{E/K} \text{ es libre de cuadrados.}$$

Ejemplo 2.5.12. (continuación del ejemplo 2.5.10) Si $E/\mathbb{Q}$ se define con la ecuación de Weierstrass $y^2 + xy + y = x^3 - x - 2$, entonces por el ejemplo 2.5.10, tenemos que

$$N_{E/\mathbb{Q}} = (2)^1(3)^0(5)^2(7)^0 \cdots = (50).$$

Si buscamos esta curva en las tablas de Cremona, encontramos la ecuación de Weierstrass bajo la lista de curvas con conductor 50; E es la curva A1(E) [Cre97, pg. 113].

Ejemplo 2.5.13. Si tomamos $E/\mathbb{Q}$ definida por $y^2 + xy + y = x^3 + x^2 - 10x - 10$ (i.e. la curva elíptica modular $X_0(15)$, cf. lema 6.3.4), entonces $\Delta = 3^4 5^4$ y $c_4 = 13 \cdot 37$. Por lo tanto $E/\mathbb{Q}_p$ tiene buena reducción para toda $p \neq 3, 5$, tiene reducción multiplicativa para $p = 3, 5$ y no tiene reducción aditiva porque no hay primos que dividan a Δ y c_4 simultáneamente. Por lo tanto

$$N_{E/\mathbb{Q}} = (2)^0(3)^1(5)^1(7)^0(11)^0 \cdots = (15).$$

En general, si la curva modular $X_0(N)$ es elíptica (i.e. de género 1), entonces el conductor de $X_0(N)$ es N. Esto lo prueba Ligozat en su tesis doctoral, cf. [Lig75, teorema 1.4.2].

Cerramos la sección con una discusión de las curvas de Frey. El punto de partida de la prueba del último teorema de Fermat es asociar una curva elíptica a un posible contraejemplo $a^n + b^n = c^n$. Esta curva elíptica lleva el nombre de *curva de Frey*. Aunque Yves Hellegouarch estudió este tipo de curvas elípticas antes que Frey (cf. [Hel75]), fue Frey quien primero sugirió que una curva elíptica de ese tipo asociada a una solución de la ecuación de Fermat podía producir una contradicción (cf. [Fre86]).

Empezamos con la definición de la curva de Frey:

---

[6] Para definir el término δ_ν asociado a una curva E/K y a una valuación no arquimediano ν de un campo K, primero encontramos una ecuación minimal para E/K_ν. Después consideremos los puntos de $\ell-$torsión de E/K_ν donde ℓ es un primo distinto de la característica del campo residual k_ν; a estos puntos los denotamos por $V := \{P \in E_{\mathfrak{p}}(\overline{K_{\mathfrak{p}}}) \mid \ell P = O\}$ y sus coordenadas generan una extensión finita L_ν de K_ν y a su vez una extensión finita de $\mathbb{Q}_\ell$. Claramente $\mathrm{Gal}(\overline{K_\nu}/K_\nu)$, y por lo tanto $\mathrm{Gal}(L_\nu/K_\nu)$, actúa sobre V que es un espacio vectorial sobre $\mathbb{F}_\ell$.

Por otro lado en el grupo $G = \mathrm{Gal}(L_\nu/K_\nu)$ existe una filtración de subgrupos $G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots$. Los grupos G_i se llaman los grupos de ramificación superior y se definen como

$$G_i = \{\sigma \in \mathrm{Gal}(L_\nu/K_n u) \mid \mathrm{ord}_\nu(\alpha - \sigma(\alpha)) > i \ \ \forall \alpha \in \mathcal{O}_{L,\nu}\},$$

donde $\mathcal{O}_{L,\nu}$ es el anillo de enteros de L_ν. Si denotamos por V^i al subespacio fijo de la acción $G_i \curvearrowright V$, entonces definimos $\delta_\nu(E/K)$ como

$$\delta_\nu(E/K) = \sum_{i=1}^{\infty} \frac{\#G_i}{\#G_0} \dim_{\mathbb{F}_\ell} V/V^i.$$

Véase el inicio de [Ser87] o [Ser79, §19.3]. También en §10 del capítulo IV de [Sil99] viene otra manera de definir el invariante δ_ν.

Definición 2.5.14. Sean $A, B, C \in \mathbb{Z}$ tales que $A + B + C = 0$. La *curva de Frey* asociada a la terna (A, B, C) es la curva $E_{A,B,C}$ definida por

$$E_{A,B,C} \ : \ y^2 = x(x - A)(x + B).$$

Nota. La curva de Frey $E_{A,B,C}$ es elíptica cuando es lisa, es decir cuando el discriminante es diferente de 0. El discriminante lo denotamos por $\Delta_{A,B,C}$ y es igual a:

$$\Delta_{A,B,C} = 2^4(ABC)^2. \tag{2.5.2}$$

Si (a, b, c) es una solución no trivial de la ecuación de Fermat $x^p + y^p + z^p = 0$, donde p es impar, entonces los enteros $A = a^p$, $B = b^p$ y $C = c^p$ producen una curva de Frey que denotamos:

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

Proposición 2.5.15. *Sean $a, b, c \in \mathbb{Z}$ primos relativos tales que $a^p + b^p = c^p$. Entonces la curva de Frey $E_{a,b,c,p}$ cumple:*

(I) $E_{a,b,c,p}$ es semiestable.

(II) El conductor de $E_{a,b,c,p}$ es:

$$N_{a,b,c,p} = \prod_{\substack{\ell | abc \\ \ell \text{ primo}}} \ell.$$

Demostración. Escribimos $E := E_{a,b,c,p}$ y en general suprimimos el subíndice "a, b, c, p" de la notación.

(I) Vamos a probar que E es semiestable sobre los primos impares ℓ, i.e. hay reducción buena módulo ℓ o reducción multiplicativa módulo ℓ. Cuando $\ell = 2$, E tiene reducción multiplicativa pero solamente referimos el lector al artículo de Serre donde aparece la prueba (cf. [Ser87, §4.1.3]).

Para $\ell > 2$ la ecuación que define a E se reduce módulo p a:

$$y^2 \equiv x(x - a^p)(x + b^p) \pmod{\ell}. \tag{2.5.3}$$

E es semiestable en p si las tres raíces del lado derecho $0, a^p$ y $-b^p$ no son todas iguales. Si este es el caso tendríamos $0 \equiv a^p \equiv -b^p \pmod{\ell}$ o en particular $\ell \mid a, b$ lo cual a su vez implica que $\ell \mid c$. Esto no puede suceder porque $(a, b, c) = 1$ por hipótesis. Por lo tanto al menos dos raíces del lado derecho de (2.5.3) son distintas y podemos concluir que E es semiestable en $\ell > 2$.

(II) Ya sabemos que el discriminante de E es $2^4(abc)^{2p}$ por (2.5.2). Entonces módulo p, la ecuación que define E tiene discriminante congruente a 0 módulo ℓ si y solamente $\ell \mid abc$. Por lo tanto si $\ell \nmid abc$, E tiene buena reducción en ℓ y por lo tanto el exponente de ℓ en el conductor de E es 0 (véase la definición 2.5.11). Si $\ell \mid abc$ entonces solamente hay reducción multiplicativa y por lo tanto el exponente de ℓ es 1. De esta manera el conductor de E es

$$N_{a,b,c,p} = \prod_{\substack{\ell | abc \\ \ell \text{ primo}}} \ell.$$

Observe que como $2 \mid b$, tenemos que el conductor $N_{a,b,c,p}$ es par.

□

2.6. Superficies Elípticas

En esta sección repasamos las definiciones y propiedades de superficies elípticas que son esencialmente curvas elípticas definidas sobre campos de funciones de una curva. En esta sección vamos a asumir que los campos son de característica 0.

Definición 2.6.1. Sea $\mathcal{C}$ una curva proyectiva y lisa definida sobre un campo K. Decimos que $(\mathcal{E}, \pi, \iota)$, o simplemente $\mathcal{E}$, es una *superficie elíptica sobre* $\mathcal{C}$ si cumple las siguientes propiedades:

1. $\mathcal{E}$ es una variedad proyectiva de dimensión 2.
2. $\pi : \mathcal{E} \to \mathcal{C}$ es un morfismo tal que para toda $t \in \mathcal{C}(\overline{K})$, salvo una cantidad finita de valores, la *fibra*
$$\mathcal{E}_t := \pi^{-1}(t)$$
es una curva proyectiva lisa de género 1.[7]
3. $\iota : \mathcal{C} \to \mathcal{E}$ es una *sección* de π, es decir que ι es un morfismo de variedades definido sobre K que cumple $\pi \circ \iota = \mathrm{Id}_{\mathcal{C}}$.

Nota. Si $k \subseteq K$, decimos que la superficie $(\mathcal{E}, \pi, \iota)$ está definida sobre k si $\mathcal{C}, \mathcal{E}, \pi$ y ι están definidos sobre k.

Nota. Para casi toda $t \in \mathcal{C}(\overline{K})$, la fibra $\mathcal{E}_t$ es una curva elíptica definida sobre un campo sobre el cual el punto distinguido $\iota(t)$ está definido. Como cada E_t es un grupo abeliano podemos operar secciones de π de la siguiente manera: si ι_1, ι_2 son secciones de π, entonces definimos

$$(\iota_1 + \iota_2)(t) := \iota_1(t) + \iota_2(t), \qquad (-\iota_1)(t) := -\iota_1(t),$$

donde $t \in \mathcal{C}(\overline{K})$ es tal que $\mathcal{E}_t$ es lisa. Esto hace que

$$\mathcal{E}(\mathcal{C}) := \{\sigma : \mathcal{C} \to \mathcal{E} \mid \sigma \text{ es sección de } \pi\}$$

sea un grupo abeliano, lo llamamos el *grupo de secciones* sobre $\mathcal{E}$. Esto se prueba al observar que las coordenadas de $\iota_1(t) + \iota_2(t)$ y $-\iota_1$ son funciones racionales de $K(\mathcal{C})$ y por lo tanto definen una función racional $\mathcal{C} \to \mathcal{E}$ que es automáticamente un morfismo porque $\mathcal{C}$ es una curva lisa (véase la proposición 3.10 del capítulo III de [Sil99]). Si además $\mathcal{E}$ está definido sobre un subcampo $k \subseteq K$, entonces podemos restringirnos al conjunto de secciones definidas sobre k que denotamos por $\mathcal{E}(\mathcal{C}/k)$; éste sigue siendo un grupo abeliano.

Definición 2.6.2. Sea $\mathcal{C}$ una curva proyectiva lisa definida sobre K y sea $k \subseteq K$ un subcampo. Decimos que dos superficies elípticas $\mathcal{E}$ y $\mathcal{E}'$ definidas sobre k son *$k-$birracionalmente equivalentes sobre* $\mathcal{C}$ si existe una función birracional $f : \mathcal{E} \to \mathcal{E}'$ definido sobre k tal que $\pi = \pi' \circ f$ donde π (resp. π') es la proyección de $\mathcal{E}$ (resp. $\mathcal{E}'$). Es decir

$$\mathcal{E} \approx_{\mathcal{C}} \mathcal{E}' \qquad \text{si} \qquad \begin{array}{ccc} \mathcal{E} & \xrightarrow{\quad\approx\quad} & \mathcal{E}' \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle\pi'} & \\ & \mathcal{C} & \end{array}$$

[7] Un teorema de Igusa [Igu55, Theorem 2] nos dice que el polinomio de Hilbert de una familia algebraica de variedades normales parametrizadas por los puntos de una variedad (e.g. las fibras de una superficie elíptica) es independiente del punto y por lo tanto el género de toda la familia es constante. En el caso del texto ya sabemos que existe una infinidad de fibras de género 1 y por lo tanto todas las fibras lisas son de género 1.

Las superficies elípticas son esencialmente curvas elípticas definidas sobre el campo de funciones de una curva $\mathcal{C}$. Más precisamente, sea $\mathcal{C}/K$ una curva proyectiva lisa y $A, B \in K(\mathcal{C})$ dos funciones racionales. Entonces definimos la curva elíptica sobre $K(\mathcal{C})$:

$$E \ : \ y^2 = x^3 + Ax + B,$$

donde $4A^3 + 27B^2 \neq 0 \in K(\mathcal{C})$. Si tomamos una $t \in \mathcal{C}(K)$ tal que A ni B tienen polos en t y tal que $\Delta = -16(4A^3 + 27B^2)$ no se anula en t, entonces podemos definir la curva elíptica E_t/K como:

$$E_t \ : \ y^2 = x^3 + A(t)x + B(t), \qquad \big(A(t), B(t) \neq \infty, \ \Delta(t) \neq 0\big) \tag{2.6.1}$$

Si consideramos a t como una variable, entonces definimos la siguiente variedad proyectiva:

$$\mathcal{E}(A,B) := \overline{\left\{ \big([X,Y,Z],t\big) \in \mathbb{P}^2 \times \mathcal{C} \;\middle|\; A(t), B(t) \neq \infty, \ Y^2Z = X^3 + A(t)XZ^2 + B(t)Z^3 \right\}}, \tag{2.6.2}$$

donde la barra denota la cerradura de Zariski en $\mathbb{P}^2 \times \mathcal{C}$, que está contenida en algún $\mathbb{P}^N$. Afirmamos que $\mathcal{E}(A,B)$ es una superficie elíptica sobre $\mathcal{C}$ donde $\pi : \mathcal{E}(A,B) \to \mathcal{C}$ es la restricción a $\mathcal{E}(A,B)$ de la proyección natural $\mathbb{P}^2 \times \mathcal{C} \to \mathcal{C}$ y

$$\iota : \mathcal{C} \longrightarrow \mathcal{E}(A,B), \quad \text{definida por} \quad t \mapsto \big([0,1,0],t\big)$$

como sección de π. En efecto, el conjunto de $t \in \mathcal{C}$ donde $A(t) = \infty$ o $B(t) = \infty$ o $\Delta(t) = 0$ es finito, entonces para el resto de las t tenemos que la fibra:

$$\mathcal{E}(A,B)_t = \pi^{-1}(t) = \{P \in \mathcal{E}(A,B) \mid \pi(P) = t\} = E_t$$

es la curva elíptica de (2.6.1) con el punto al infinito como su punto distinguido y por lo tanto $\mathcal{E}(A,B)$ es una superficie elíptica sobre $\mathcal{C}$.

Nota. Si cambiamos $y^2 = x^3 + Ax + B$ a otra ecuación de Weierstrass $y^2 = x^3 + A'x + B'$ con cambio de variable admisible sobre $K(\mathcal{C})$, entonces las variedades $\mathcal{E}(A,B)$ y $\mathcal{E}(A',B')$ son birracionalemente equivalentes sobre $\mathcal{C}$.

Resulta que toda superficie elíptica sobre $\mathcal{C}$ se puede obtener con el procedimiento anterior. Es decir:

Teorema 2.6.3. *Sea $\mathcal{E} = (\mathcal{E}/K, \pi, \iota)$ una superficie elíptica sobre $\mathcal{C}/K$ definida sobre un subcampo $k \subseteq K$. Entonces existen $A, B \in k(\mathcal{C})$ tales que $\mathcal{E}$ es $k-$birracionalmente equivalente a $\mathcal{E}(A,B)$ dada por* (2.6.2)*. Además la curva elíptica $E/k(\mathcal{C})$ definida por*

$$E \ : \ y^2 = x^3 + Ax + B,$$

es única salvo isomorfismo sobre $k(\mathcal{C})$.

Nota. El grupo de $k(\mathcal{C})-$puntos de E es isomorfo al grupo de secciones de $\mathcal{E}$ sobre k. Más precisamente, la función

$$E\big(k(\mathcal{C})\big) \longrightarrow \mathcal{E}(\mathcal{C}/k) \quad \text{definida por} \quad (x,y) \mapsto \big(t \mapsto ([x(t), y(t), 1], t)\big) \tag{2.6.3}$$

es un isomorfismo de grupos, i.e. $E\big(k(\mathcal{C})\big) \cong \mathcal{E}(\mathcal{C}/k)$. Véase la proposición 3.10 del capítulo III de [Sil99] para una prueba.

Veamos un ejemplo de superficie elíptica que aparece en la prueba del teorema de modularidad. La curva base $\mathcal{C}$ será $\mathbb{P}^1(\mathbb{Q})$ cuyo campo de funciones racionales es $\mathbb{Q}(t)$. Este ejemplo es originalmente de Klein (cf. [Kle45, pg. 130]).

Ejemplo 2.6.4. Definimos la curva elíptica $W/\mathbb{Q}(t)$

$$W \ : \ y^2 = x^3 + a_4(t)x + a_6(t)$$

donde $a_4, a_6 \in \mathbb{Q}(t)$ están definidos por

$$a_4(t) = -\frac{1}{48}(t^{20} - 228t^{15} + 494t^{10} + 228t^5 + 1),$$
$$a_6(t) = \frac{1}{864}(t^{30} + 522t^{25} - 10005t^{20} - 10005t^{10} - 522t^5 + 1)$$

El $j-$invariante de W es:

$$j(W) = \frac{-(t^{20} - 228t^{15} + 494t^{10} + 228t^5 + 1)^3}{t^5(t^{10} + 11t^5 - 1)^5} \tag{2.6.4}$$

En el capítulo 6 veremos que $\mathcal{W}$ es una superficie elíptica sobre una curva X_5 sobre $\mathbb{Q}$ que parametriza clases de isomorfismos $[E, P, C]$ donde $E/\mathbb{Q}$ es una curva elíptica, $P \in E[5]$ y $C \subset E[5]$ es un subgrupo cíclico $G_{\mathbb{Q}}-$estable de orden 5 que no contiene a P.

Capítulo 3

Formas Modulares

3.1. 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 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 espacio euclidiano $\mathbb{R}^4$. De esta manera, la acción $\mathrm{GL}_2^+(\mathbb{R}) \curvearrowright \mathbb{H}$ es continua.

Esta acción no es fiel[1], 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:

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

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:

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

[1]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 $x \in X$.

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[2].

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

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

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

Definición 3.1.1. 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 $A \in \mathrm{SL}_2(\mathbb{R})$ loxodrómica.

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 3.1.2. 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]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 [Mil17b]).

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

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

- Si $z \in \mathbb{H}$, se toma al conjunto $\{|z - w| < \varepsilon\}_{w \in \mathbb{H}}$ como base local de z.
- Si $z = \infty$, se toma $\{\{\mathrm{Im}\,(w) > N\} \cup \{\infty\}\}_{N \geq 1}$ como base local de ∞.
- Si $z \in \mathbb{Q}$ es una cúspide, para su base local, se toma a z y a los interiores de todos los discos en $\mathbb{H}$ tangentes al eje real sobre z, más precisamente, se 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 3.1 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.

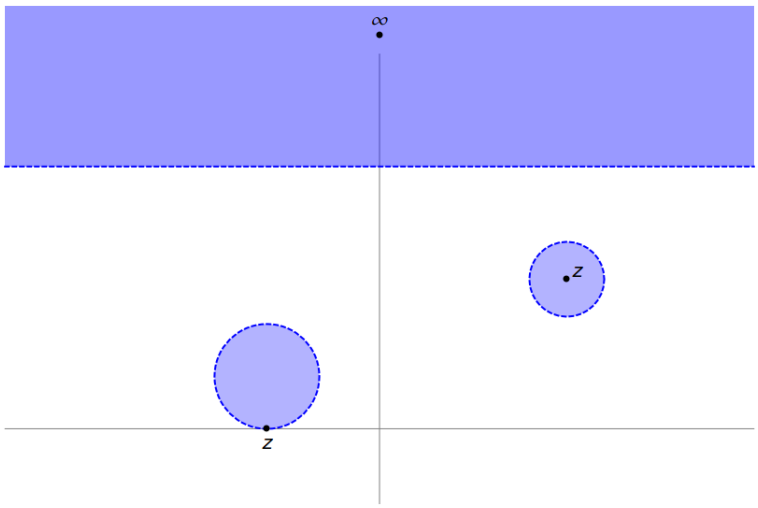


Figura 3.1: Un ejemplo de cada tipo de abierto básico de la topología de $\mathbb{H}^*$.

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 $\mathbb{H}$ 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 3.1.3. 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 3.1.4. *Si $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ es un subgrupo, entonces $X(\Gamma)$ es un espacio conexo, Hausdorff y localmente compacto.*

Demostración. Aquí solamente esbozamos la prueba, para más detalles nos referimos a [Shi94, §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[3]. 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

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

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 [DS05, §2.2, §2.3, §2.4] para detalles).

Teorema 3.1.5. *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.*

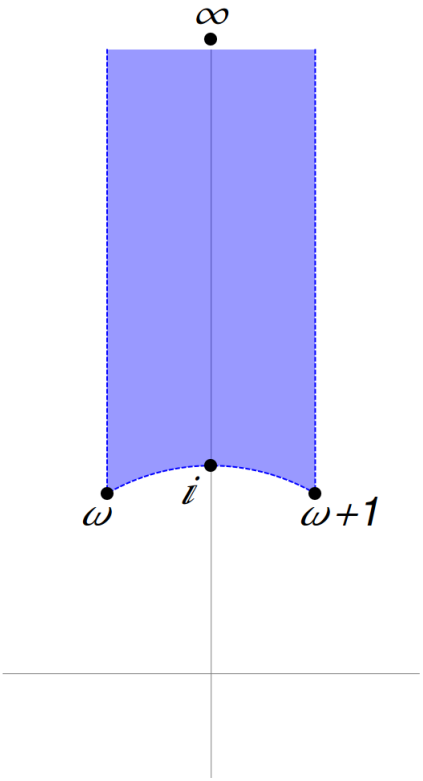


Figura 3.2: Dominio fundamental de la acción $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{H}$, donde $\omega = e^{2\pi i/3}$.

Demostración. Es bien conocido que el conjunto

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

[3]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.

es un *dominio fundamental*[4] para la acción $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{H}$ (Véase la figura 3.2). 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 finito; 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. □

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.

3.2. Subgrupos de congruencia

Los subgrupos de congruencia son ciertos subgrupos del grupo modular $\mathrm{SL}_2(\mathbb{Z})$. Como $\mathrm{SL}_2(\mathbb{Z})$ 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 3.2.1. 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 $\Gamma(N) \subseteq \Gamma$.

[4]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 $Gx \cap Gx' \supsetneq \{1\} \Longrightarrow x = x'$ y tal que para toda $x \in X$ existe $x' \in \overline{\mathcal{F}}$ (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 suprayectivo (cf. [Shi94, §1.6, lema 1.38]). Por lo tanto tenemos la siguiente sucesión exacta:

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

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. [Rot95, Teorema 8.5, pg 219]) y en general:

$$\begin{aligned} \#\mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) &= p^{4\alpha}\left(1-\tfrac{1}{p}\right)\left(1-\tfrac{1}{p^2}\right), \\ \#\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) &= p^{3\alpha}\left(1-\tfrac{1}{p^2}\right), \end{aligned} \tag{3.2.1}$$

(c.f. [Shi94, §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 (3.2.1) podemos concluir que

$$(\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)) = \#\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{p|N}\left(1-\tfrac{1}{p^2}\right). \tag{3.2.2}$$

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:

$$(\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma(N)}) = \begin{cases} \frac{1}{2}N^3 \prod_{p|N}(1-p^{-2}) & N > 2, \\ 6 & N = 2. \end{cases} \tag{3.2.3}$$

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

Definición 3.2.2. Sea $N \in \mathbb{Z}^+$. Definimos

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

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

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

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

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

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

ya que si tomamos $\gamma \in \Gamma_0(N)$ con $\det \gamma = ad - bc = 1$, la hipótesis de $c \equiv 0 \pmod N$ implica que $ad \equiv 1 \pmod N$. Para elegir un elemento arbitrario de $\Gamma_0(N)/\Gamma(N)$, solamente hay $\phi(N)$ maneras de elegir la entrada a y N maneras de elegir la entrada b.[5] 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 [IR90, Proposición 2.2.5].

Con la fórmula anterior y con la fórmula para $(\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N))$ que calculamos en (3.2.2), podemos calcular el índice de $\Gamma_0(N)$ en $\mathrm{SL}_2(\mathbb{Z})$:

$$(\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)) = \frac{(\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N))}{(\Gamma_0(N) : \Gamma(N))} = \frac{N^3 \prod (1 - p^{-2})}{N^2 \prod (1 - p^{-1})} = N \prod_{p|N} (1 + p^{-1}). \tag{3.2.4}$$

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 3.2.3. 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, si Γ es un subgrupo de congruencia, la curva modular $X(\Gamma)$ es una superficie de Riemann compacta y por lo tanto es caracterizada topológicamente por el género. Para calcular el género de $X(\Gamma)$, necesitamos estudiar los puntos elípticos y las cúspides de la acción $\Gamma \curvearrowright \mathbb{H}^*$. Abusamos un poco la notación y decimos que $z\Gamma \in X(\Gamma)$ es un punto elíptico (resp. una cúspide) si $z \in \mathbb{H}^*$ es un punto elíptico (resp. una cúspide) de la acción $\Gamma \curvearrowright \mathbb{H}^*$.

Para calcular el género de $X(\Gamma)$, se usa la fórmula de Hurwitz[6] aplicado a la función holomorfa $\varphi : X(\Gamma) = \mathbb{H}^*/\Gamma \to \mathbb{H}^*/\Gamma(1) = X(1)$ inducida por la inclusión $\Gamma \subset \Gamma(1)$. Primero sabemos que

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

[6] 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

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

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 3.1.5. Entonces la relación entre los géneros de $X(\Gamma)$ y de $\mathbb{H}^*/\Gamma(1)$ que establece la fórmula de Hurwitz se puede usar para calcular el género de $X(\Gamma)$ y así completamente caracterizar a $X(\Gamma)$ como superficie de Riemann. Como consecuencia de estas consideraciones, tenemos el siguiente teorema:

Teorema 3.2.4. *Sea Γ un subgrupo de congruencia. Sea $\mu := (\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma})$, Sea ν_∞ la cantidad de cúspides de $X(\Gamma)$ y ν_i como la cantidad de puntos elípticos de orden $i \in \{2, 3\}$ en $X(\Gamma)$. Entonces el género g de la superficie de Riemann $X(\Gamma)$ es:*

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

Demostración. La observación clave para aplicar la fórmula de Hurwitz es que el índice de ramificación de un elemento $z\Gamma \in X(\Gamma)$ en la preimagen de $z\Gamma(1) \in X(1)$ bajo la función natural $X(\Gamma) \to X(1)$ es exactamente el índice $(\overline{\Gamma(1)_z} : \overline{\Gamma}_z)$ dentro de $\mathrm{PSL}_2(\mathbb{Z})$ (cf. [Shi94, §1.5, proposición 1.37]). Para una prueba completa de este teorema vea [Shi94, §1.6, proposición 1.40] o vea [DS05, Teorema 3.1.1] para una prueba más detallada). □

Nota. Cuando $\Gamma = \Gamma(N)$, la fórmula para el género de $X(\Gamma)$ se simplifica. Para $N > 1$, $\Gamma(N)$ no tiene puntos elípticos y $\nu_\infty = \mu/N$ (cf. la proposición 1.39 de §1.6 en [Shi94] y la discusión después de ésta). Entonces tenemos que:

$$\text{género de } \ X(N) = 1 + \mu\frac{N-6}{12N}.$$

Ejemplo 3.2.5. En el caso $N = 2$, la nota anterior y la fórmula (3.2.3) nos da el género de $X(2)$:

$$\text{género de } \ X(2) = 1 + 6\frac{2-6}{24} = 0.$$

Cuando $\Gamma = \Gamma_0(N)$, las fórmulas para ν_2, ν_3 y ν_∞ son más complicadas:

Proposición 3.2.6. *Con la notación del teorema 3.2.4, la cantidad de puntos elípticos y cúspides de $X_0(N)$ se calculan con las siguientes fórmulas:*

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

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

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

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

Demostración. (c.f. [Shi94, §1.6, proposición 1.43]) □

Ejemplo 3.2.7. Aplicamos el teorema anterior al caso $N = 15$. Para calcular ν_2, ν_3 y ν_∞, usamos la proposición 3.2.6. Como -1 no es residuo cuadrático módulo 3 y -3 no es residuo cuadrático módulo 5, la proposición 3.2.6 dice que

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

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 3.2.3 se 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. Observe que las cuatro cúspides son $0, \frac{1}{3}, \frac{1}{5}, \frac{1}{15}$ (donde $\frac{1}{15}$ es la cúspide ∞). Esta curva elíptica aparece en la prueba del teorema de modularidad.

3.3. Formas modulares y automorfas

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 ciertos operadores entre los espacios de formas modulares que nos permiten "cambiar" de subgrupo de congruencia; estos operadores son ejemplos de operadores de Hecke.

Primero definimos dos conceptos fundamentales:

Definición 3.3.1. 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 3.3.2. 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.

Observe 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 desciende a $\mathbb{H}/h\mathbb{Z}$, el espacio cociente de la acción $h\mathbb{Z} \curvearrowright \mathbb{H}$ de traslaciones $\{z \mapsto z + hk\}_{k\in\mathbb{Z}}$; por el momento, denotamos a este espacio cociente por $\widetilde{\mathbb{H}}$. Por lo tanto existe una función $\tilde{f} : \widetilde{\mathbb{H}} \to \mathbb{C}$ tal que $f = \tilde{f} \circ \pi$, donde $\pi : \mathbb{H} \twoheadrightarrow \widetilde{\mathbb{H}}$ es la proyección natural (véase el diagrama conmutativo 3.3.1).

Por otro lado, la función exponencial:

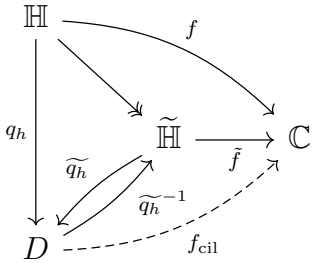
$$q_h : \mathbb{H} \longrightarrow D \qquad \text{definida por} \quad z \mapsto e^{2\pi i z/h},$$

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 $f_{\mathrm{cil}} : D \to \mathbb{C}$ definida por $f_{\mathrm{cil}} = \tilde{f} \circ \widetilde{q_h}^{-1}$, que aparece como la flecha punteada en el siguiente diagrama:



(3.3.1)

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

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

donde h es el mínimo entero positivo tal que $f(z) = f(z+h)$ y donde $m \in \mathbb{Z}$ se llama *el orden de* f *en* ∞.

Notas. Observe que f es holomorfa (resp. meromorfa) en ∞ si $m \geq 0$ (resp. $m < 0$) y se anula en ∞ cuando $m > 0$. Además, si $h = 1$, como en el caso $\Gamma_0(N)$, entonces $f(z) = f(z+1)$ y la serie de Laurent $f_\infty(q)$ es simplemente la serie de Fourier de f. A veces decimos "Fourier" en lugar de "Laurent" si estamos en el caso de $\Gamma_0(N)$.

La existencia de una extensión holomorfa $\widehat{f_{\text{cil}}}$ es equivalente a que el límite de f_{cil} existe cuando $q \to 0$. Gracias al comentario sobre el diagrama conmutativo (3.3.1), 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 ∞:

$$\big\{f(z_n)\big\}_{n\in\mathbb{N}} \text{ es acotado si } \lim_{n\to\infty} \Im(z_n) = \infty \quad \Longrightarrow \quad f \text{ es holomorfa en } \infty. \tag{3.3.2}$$

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 función débilmente $(\Gamma, k)-$modular con Γ de congruencia y sea $z \in \mathbb{Q}$ una cúspide de la acción $\Gamma \curvearrowright \mathbb{H}$. 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 $\Gamma \curvearrowright \mathbb{H}$, se 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 se obtiene 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.[7] 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 3.3.4. 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 (resp. meromorfa)* en z si $f[\gamma]_k$ es holomorfa (resp. meromorfa) en ∞ donde $\gamma \in \Gamma(1)$ es tal que $z = \gamma\infty$.

Observe 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 $f(\gamma' z)$ tienen el mismo comportamiento cerca de ∞. Por lo tanto se anulan simultáneamente.

Ahora estamos en posición para definir las formas modulares:

Definición 3.3.5. Decimos que $f : \mathbb{H} \to \mathbb{C} \cup \{\infty\}$ es una *forma modular (resp. automorfa)* de peso k con respecto de un subgrupo de congruencia Γ si cumple las siguientes tres cosas:

I) f es holomorfa (resp. meromorfa).

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

III) $f[\tau]_k$ es holomorfa (resp. meromorfa) en ∞ para toda $\tau \in \Gamma(1)$.

Al conjunto de formas modulares (resp. automorfas) de peso k con respecto de Γ se denota por $M_k(\Gamma)$ (resp. $\mathcal{A}_k(\Gamma)$). Si además cumple

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

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

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

Proposición 3.3.6. *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.*

[7] Podemos hablar de modularidad débil con respecto de $\gamma^{-1}\Gamma\gamma$ porque $\gamma^{-1}\Gamma\gamma$ es un subgrupo de congruencia cuando Γ lo es (c.f. [Bum98, §1.4, lema 1.4.1]).

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

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

donde $d\mu(z) = dxdy/y^2$ (donde $z = x + iy$) es la medida hiperbólica de $\mathbb{H}$ y V_Γ es el volumen hiperbólico[8] *de $X(\Gamma)$. i.e. $V_\Gamma = \int_{X(\Gamma)} d\mu$. A veces quitamos el "$\Gamma$" de la notación del producto interior cuando Γ es claro del contexto.*

Demostración. El inciso (i) es una aplicación clásica del teorema de Riemann-Roch[9]. 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 [Shi94]). 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 [DS05]. □

Ejemplo 3.3.7. Un paso crucial en la prueba del último teorema de Fermat es la siguiente consecuencia del inciso (ii): como el género de $X(2)$ es 0 (cf. el ejemplo 3.2.5), entonces $\dim S_2(\Gamma(2)) = 0$. Como $\Gamma(2) \subseteq \Gamma_0(2)$, entonces $S_2(\Gamma_0(2)) \subseteq S_2(\Gamma(2))$ y por lo tanto $\dim S_2(\Gamma_0(2)) = 0$.

Ejemplos 3.3.8. (De formas modulares)

1. (Series de Eisenstein) Sea $k > 1$. La *serie de Eisenstein de peso* $2k$ es la función $G_{2k} : \mathbb{H} \to \mathbb{C}$ definida por

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

La serie es absolutamente convergente (cf. la sección §2 del capítulo VII de [Ser73]) y converge uniformemente sobre compactos (esto se deduce de una aplicación estándar de la prueba M de Weierstrass). Por lo tanto G_{2k} es holomorfo sobre $\mathbb{H}$. Es fácil ver que es débilmente $\mathrm{SL}_2(\mathbb{Z})-$modular de peso $2k$, en efecto, Toda matriz

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

induce una permutación

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

[8] Como $X(\Gamma)$ es una superficie de Riemann de primer tipo, su volumen es finito (c.f. [FK12])

[9] 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 [Har77] para una prueba).

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:

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

lo cual es equivalente a que G_{2k} es débilmente modular con respecto de $\mathrm{SL}_2(\mathbb{Z})$. Por último, observemos que si $z = \sigma + i\tau$, con $\tau > 0$, entonces:

$$\left|\frac{1}{(mz+n)^{2k}}\right| = |mz+n|^{-2k} \leq |m\sigma+n|^{-2k},$$

y por lo tanto G_{2k} está acotado cuando $\Im(z) = \tau \to \infty$. Por (3.3.2), concluimos que G_{2k} es holomorfo en ∞. Esto concluye la prueba de que $G_{2k} \in M_{2k}(\mathrm{SL}_2(\mathbb{Z}))$.

La serie de Fourier de G_{2k} se calcula usando la expresión en serie de $\pi\cot\pi z$ y derivándola $2k-1$ veces con respecto de z (véase por ejemplo §1.1 de [DS05]). El resultado final es:

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

donde ζ es la función zeta de Riemann y $\sigma_{2k-1}(n)$ es la suma de los divisores positivos de n, cada uno elevado a la $2k-1$. Si queremos normalizar la serie de Fourier, escribimos $E_{2k}(z) := G_{2k}(z)/\zeta(2k)$. Como $M_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ es un $\mathbb{C}-$espacio vectorial, entonces E_{2k} también es una forma modular de peso $2k$.

2. Como $M(\mathrm{SL}_2(\mathbb{Z}))$ es un anillo graduado, podemos construir más ejemplos de formas modulares al tomar combinaciones polinomiales de series de Eisenstein. Dos ejemplos muy importantes son:
$$g_2(z) := 60G_4(z) \quad \text{y} \quad g_3(z) = 140G_6(z),$$
donde claramente $g_2 \in M_4(\mathrm{SL}_2(\mathbb{Z})$ y $g_3 \in M_6(\mathrm{SL}_2(\mathbb{Z}))$.

3. (El discriminante modular) Uno de los ejemplos más conocidos de formas modulares es el discriminante modular $\Delta : \mathbb{H} \to \mathbb{C}$ definido por
$$\Delta(z) := g_2(z)^3 - 27g_3(z)^2.$$
Observe que g_2^3 y g_3^2 son de peso 12 y por lo tanto $\Delta \in M_{12}(\mathrm{SL}_2(\mathbb{Z}))$. Si sustituimos las series de Fourier de g_2 y g_3 en la definición de Δ, obtenemos que los términos constantes se cancelan, i.e. $a_0(\Delta) = 0$ y el primer término distinto de cero es $a_1 = (2\pi)^{12}$. Por lo tanto $\Delta \neq 0$ y $\Delta \in S_{12}(\mathrm{SL}_2(\mathbb{Z}))$.

Δ satisface la siguiente fórmula debida a Ramanujan [Ram16]:

$$\Delta(z) = \eta(z)^{24} = q\prod_{n=1}^{\infty}(1-q^n)^{24}, \qquad q = e^{2\pi iz}, \tag{3.3.3}$$

donde $\eta(z)$ es la función η de Dedekind. De (3.3.3) es claro que $\Delta(z) \neq 0$ para toda $z \in \mathbb{H}$.

Ahora definimos una forma automorfa muy importante:

Definición 3.3.9. El *invariante modular* $j : \mathbb{H} \to \mathbb{C}$ se define como

$$j(z) = 1728\frac{g_2(z)^3}{\Delta(z)}.$$

Como $g_2^3, \Delta \in M_{12}(\mathrm{SL}_2(\mathbb{Z}))$, tenemos que para toda $\gamma \in \mathrm{SL}_2(\mathbb{Z})$

$$\frac{g_2(\gamma z)^3}{\Delta(\gamma z)} = \frac{(cz+d)^{12}g_2(z)^3}{(cz+d)^{12}\Delta(z)} = (cz+d)^0\frac{g_2(z)^3}{\Delta(z)},$$

y por lo tanto j es débilmente modular de peso 0 con respecto de $\mathrm{SL}_2(\mathbb{Z})$. Como $\Delta(z) \neq 0$ sobre $\mathbb{H}$, entonces j es holomorfo sobre $\mathbb{H}$. Para ver el comportamiento de j en ∞, sustituimos las series de Fourier de g_2 y Δ en la definición de j:

$$j(z) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} a_n(j)q^n, \qquad q = e^{2\pi iz},$$

donde $a_n(j) \in \mathbb{Z}$ para toda $n \geq -1$ (cf. [DS05]). Por lo tanto j tiene un polo simple en ∞. De esta manera tenemos que j es una forma automorfa de peso 0 con respecto de $\mathrm{SL}_2(\mathbb{Z})$, i.e. $j \in \mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z}))$. De hecho j genera a todas las formas automorfas de peso 0:

Proposición 3.3.10. *Todas las formas automorfas de peso 0 con respecto de* $\mathrm{SL}_2(\mathbb{Z})$ *son funciones racionales en* j*, más precisamente, tenemos la siguiente igualdad de campos:*

$$\mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}(j).$$

Por lo tanto el campo de funciones meromorfas de la superficie de Riemann $\mathbb{H}^*/\mathrm{SL}_2(\mathbb{Z})$ *es* $\mathbb{C}(j)$*.*

Esta proposición se sigue del siguiente lema:

Lema 3.3.11. *La función* $j : \mathbb{H} \to \mathbb{C}$ *es biyectiva y* $j(\infty) = \infty$*. Por lo tanto* j *se extiende de manera única a una biyección* $j : X_0(1) \to \mathbb{C} \cup \{\infty\}$*.*

Demostración. Sea $z_0 \in \mathbb{H}$. Entonces $j - z_0 \in \mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z}))$ y por lo tanto $j - z_0 : \mathbb{H} \to \mathbb{C}$ se factoriza a través de $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ y se extiende a una función meromorfa $j - z_0 : X_0(1) \to \mathbb{C} \cup \{\infty\}$. El divisor principal asociado a $j - z_0$ tiene grado igual a 0. Como $j - z_0$ solamente tiene un polo simple en la cúspide $\infty\mathrm{SL}_2(\mathbb{Z})$, necesariamente $j - z_0$ tiene un cero simple en un punto $z_1 \in X_0(1) - \{\infty\mathrm{SL}_2(\mathbb{Z})\}$. En particular $j(z_1) = z_0$ y solamente sucede en z_1, porque $j - z_0$ tiene un cero simple en $z_1 \in X_0(1) - \{\infty\mathrm{SL}_2(\mathbb{Z})\}$. Por lo tanto $j : \mathbb{H} \to \mathbb{C}$ es biyectiva y como $j(\infty) = \infty$, tenemos que $j : X_0(1) \to \mathbb{C} \cup \{\infty\}$ es biyectiva. □

Demostración. (de la proposición 3.3.10) Primero observamos que $\mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z}))$ es un campo porque si $f \in \mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z}))$ es distinta de 0, entonces claramente $1/f \in \mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z}))$. De hecho, $\mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z}))$ contiene a $\mathbb{C}$ y por lo tanto, como $j \in \mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z}))$ entonces inmediatamente tenemos $\mathbb{C}(j) \subseteq \mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z}))$.

Ahora sea $f \in \mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z}))$ con ceros $p_1, \ldots, p_n \in \mathbb{H}$ y polos $q_1 \ldots, q_m \in \mathbb{H}$, enumerados con multiplicidad. Entonces el divisor principal (f) tiene grado:

$$\deg(f) = n - m + \nu_\infty(f),$$

donde $\nu_\infty(f)$ es el orden de f en ∞.

La función

$$g(z) := \frac{(j(z) - j(p_1)) \cdots (j(z) - j(p_n))}{(j(z) - j(q_1)) \cdots (j(z) - j(q_m))} \in \mathbb{C}(j),$$

tiene exactamente los mismos ceros y polos que f sobre $\mathbb{H}$, gracias al lema anterior. Por lo tanto $\deg(g) = n - m + \nu_\infty(f)$. Como $\mathbb{H}^*/\mathrm{SL}_2(\mathbb{Z})$ es una superficie de Riemann compacta, los grados de los divisores principales (f) y (g) son 0 (cf. la proposición 2.1.11) y por lo tanto $\nu_\infty(f) = \nu_\infty(g)$, i.e. f y g tienen el mismo comportamiento en la cúspide ∞. Por lo tanto $f/g : \mathbb{H}^*/\mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C} \cup \{\infty\}$ es una función meromorfa entre superficies de Riemann compactas que no tiene ceros ni polos y por lo tanto es constante. Como $g \in \mathbb{C}(j)$, concluimos que $f \in \mathbb{C}(j)$ y terminamos con la prueba. □

3.4. Operadores de Hecke

Para definir los operadores de Hecke que son operadores de los espacios vectoriales $M_k(\Gamma)$. Necesitamos estudiar 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 3.4.1. 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 [DS05]), más precisamente:

$$\exists\, \beta_1, \ldots, \beta_n \in \Gamma\alpha\Gamma' \text{ tal que } \Gamma\alpha\Gamma' = \bigsqcup_{i=1}^{n} \Gamma\beta_i, \tag{3.4.1}$$

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

Definición 3.4.2. 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 (3.4.1).

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 observe 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:

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

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:

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

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

Lema 3.4.3. *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 ∞.*

Demostración. Sea $h \in \mathbb{Z}^+$ el mínimo común múltiplo de $h_1, \ldots, h_m$. Entonces $f := f_1 + \cdots + f_m$ es $h\mathbb{Z}-$periódica. 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 $M_k(\Gamma')$.

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

$$\alpha_p = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}), \tag{3.4.2}$$

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

Definición 3.4.4. 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 (3.4.2) 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 3.4.7 más adelante). Entonces si pudiéramos 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 $\Gamma_1(N)$ (cf. la sección 3.2). 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, restringida 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 3.4.5. 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 $\langle d\rangle : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$ definida 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 3.4.6. *Sea G el grupo dual de Pontryagin del grupo finito $\mathbb{Z}/N\mathbb{Z}$, es decir*

$$G = \mathrm{Hom}((\mathbb{Z}/N\mathbb{Z})^*, \mathbb{C}^*).$$

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

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

Demostración. 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 3.4.7 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[10] 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

$$\pi_\chi^2 = \pi_\chi \quad \text{y} \quad \pi_{\chi'}\pi_\chi = 0 \quad (\chi \neq \chi'). \tag{3.4.3}$$

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 $d \neq 1$.[11] Estas dos igualdades implican respectivamente que

$$\pi_\chi(M_k(\Gamma_1(N))) \subseteq M_k(\Gamma_1(N),\chi) \quad \text{y} \quad \sum_{\chi\in G}\pi_\chi = \mathrm{Id}. \tag{3.4.4}$$

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

$$\pi_\chi|_{M_k(\Gamma_1(N),\chi)} = \mathrm{Id}. \tag{3.4.5}$$

De (3.4.3), (3.4.4) y (3.4.5) se sigue que $M_k(\Gamma_1(N),\chi)$ es un sumando directo de $M_k(\Gamma_1(N))$. De la segunda parte de (3.4.4) se sigue que los subespacios $M_k(\Gamma_1(N),\chi)$ generan a $M_k(\Gamma_1(N))$ y de la segunda parte de (3.4.3) 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 3.4.7. *Sean $e, d \in (\mathbb{Z}/N\mathbb{Z})^*$ y $p, q \in \mathbb{Z}$ primos. Entonces:*

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

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

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

[10] Véase, por ejemplo, el capítulo 16, §3 de [IR90] y en particular la proposición 16.3.1.

[11] Como $d \neq 1$, d determina un caracter no trivial del grupo finito G y es conocido que la suma de todos los valores de un caracter no trivial es 0. Este argumento está en la prueba de la proposición 16.3.1 de [IR90].

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

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

Demostración. Esto es exactamente la proposición 5.2.4 de [DS05]. □

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 3.4.8. 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:

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

Notas. El operador $\langle n \rangle$ es completamente multiplicativo, 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 3.4.7.*i*:

$$T_m \langle n \rangle = \langle n \rangle T_m \qquad \forall\, n, m \in \mathbb{Z}^+. \tag{3.4.6}$$

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

$$T_m T_n = T_{nm} = T_n T_m \qquad \forall\, (n, m) = 1 \tag{3.4.7}$$

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 $\langle p^{-1} \rangle T_p$ (cf. el teorema 5.5.3 de [DS05]). Por lo tanto la proposición 3.4.7 nos garantiza que $\langle p \rangle$ y T_p son operadores normales (i.e. conmutan con su operador adjunto) de lo cual se sigue el siguiente resultado:

Proposición 3.4.9. *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 3.4.10. *El espacio $S_k(\Gamma_1(N))$ tiene una base ortogonal de vectores propios simultáneos para los operadores de Hecke $\{\langle n \rangle, T_n \mid (n, N) = 1\}$.*

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

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

Proposición 3.4.11. *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:

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

Demostración. Véase la proposición 5.3.1 de [DS05]. □

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 ver a $S_k(\Gamma_0(M))$ como subespacio de $S_k(\Gamma_0(N))$. 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 ver a $S_k(\Gamma_0(M))$ como subespacio de $S_k(\Gamma_0(N))$ 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 3.4.12. *Si $f \in S_k(\Gamma_0(M))$ y $g(z) = f(dz)$, entonces $g \in S_k(\Gamma_0(Md))$.*

Demostración. 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 $\gamma' \in \Gamma_0(M)$ porque $Md \mid c$. 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 inyectiva porque si $f[\beta_d]_k = 0$ claramente $f = 0$; esta es la segunda manera de ver a $S_k(\Gamma_0(M))$ como subespacio de $S_k(\Gamma_0(N))$.

Si d es un divisor de N definimos la función:

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

Definimos:

Definición 3.4.13. 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 formas 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 3.4.14. *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 $\{T_n, \langle n\rangle \mid (n, N) = 1\}$.*

Demostración. [DS05, §5.7] □

Definición 3.4.15. Sea $f \in S_k(\Gamma_0(N))$ distinta de 0. Decimos que es una *eigenforma* si es un vector propio simultáneo 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 3.4.16. *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 3.4.6), en particular $\langle n\rangle f = \chi(n)f$ para toda $(n, N) = 1$. 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.

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

$$T_n f = b_n f \quad \text{y} \quad \langle n\rangle f = c_n f \qquad \text{donde } (n, N) = 1. \tag{3.4.8}$$

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 3.4.11. Por esta vía tenemos:

$$a_1(T_n f) = a_n(f) = \lambda_n \qquad \forall n > 0. \tag{3.4.9}$$

Por otro lado, f es una eigenforma fuera de N, entonces por (3.4.8) tenemos

$$\lambda_n = a_1(T_n f) = a_1(b_n f) = b_n a_1(f) = b_n \lambda_1. \tag{3.4.10}$$

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

$$\frac{\lambda_n}{\lambda_1} = b_n \qquad \forall\ (n, N) = 1. \tag{3.4.11}$$

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 1970, f necesariamente es una forma vieja, i.e. $f \in S_k^{\text{old}}(\Gamma_0(N))$, [AL70]. En [DS05, §5.7] viene una prueba detallada debida a David Carlton. □

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

Proposición 3.4.17. *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.

Demostración. Para una prueba con geometría algebraica, consulte [DS74, proposición 2.7.3 de §2] o [DS05, §6.5]. En seguida escribimos una prueba elemental debida a Serre que aparece en [Ser77b, §2.5].

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 una combinación algebraica 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 3.4.10). 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 grupo 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:

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

o en otras palabras, $a_m(g^\sigma) = a_m(g)^\sigma$. Además, si escribimos $h := \chi(n)g$, 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 [DS05, teorema 6.5.4] y el caso $k \geq 2$ se encuentra en [Shi94, §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:

$$\langle n \rangle g^\sigma = \chi^\sigma(n)g^\sigma = \chi(n)g^\sigma = (\chi(n)g)^\sigma = (\langle n \rangle g)^\sigma. \tag{3.4.12}$$

Con esta notación y con la fórmula para calcular coeficientes de Fourier de $T_p g$ (la proposición 3.4.11), tenemos que para $\sigma \in G$

$$\begin{aligned}
a_m(T_p g)^\sigma &= \left(\sum_{d|(m,p)} d^{k-1} a_{pm/d^2}(\langle d \rangle g) \right)^\sigma = \sum_d (d^{k-1})^\sigma \chi^\sigma(d) \big(a_{pm/d^2}(g)\big)^\sigma \\
&= \sum_d d^{k-1} \chi(d) \big(a_{pm/d^2}(g)\big)^\sigma \qquad \big(\text{porque } \chi^\sigma = \chi\big) \\
&= \sum_d d^{k-1} \chi(d) a_{pm/d^2}(g^\sigma) = \sum_d d^{k-1} a_{pm/d^2}(\chi(d)g^\sigma) \\
&\overset{(3.4.12)}{=} \sum_d d^{k-1} a_{pm/d^2}(\langle d \rangle g^\sigma) \\
&= a_m(T_p g^\sigma) \quad \forall m \geq 1. \\
\therefore \quad T_p g^\sigma = (T_p g)^\sigma &= \big(a_p(g)g\big)^\sigma = a_p(g)^\sigma g^\sigma.
\end{aligned}$$

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 $G \curvearrowright \Lambda$ definida 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 [DS74], 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 6.2. En este trabajo solamente probamos que $K_f/\mathbb{Q}$ es finita 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 [DS05].

Capítulo 4

Curvas Modulares

4.1. Modelos de curvas modulares

En esta sección vamos a describir el método de Shimura en [Shi94] para encontrar un *modelo* sobre un campo numérico para cada curva modular $X(\Gamma)$. Primero definimos el concepto de modelo de una curva sobre un subcampo del campo de definición.

Definición 4.1.1. Sea $\mathcal{C}'$ una curva proyectiva definida sobre un campo K y sea $k \subseteq K$ un subcampo. Decimos que una pareja $(\mathcal{C}, \varphi) = (\mathcal{C}/k, \varphi)$ es un *modelo* de $\mathcal{C}'$ sobre k si $\mathcal{C}$ es una curva proyectiva definida sobre k y $\varphi : \mathcal{C}' \to \mathcal{C}$ es una función birracional definido sobre K.

Recuerde que cuando $\Gamma \subseteq \mathrm{SL}_2(\mathbb{R})$ es un subgrupo discreto y de índice finito, entonces el cociente $X(\Gamma) := \mathbb{H}^*/\Gamma$ es una superficie de Riemann compacta gracias al teorema 3.1.5. Por el teorema de Riemann, $X(\Gamma)$ admite una estructura de curva proyectiva sobre $\mathbb{C}$. Por lo tanto podemos calcular modelos de $X(\Gamma)$ sobre subcampos de $\mathbb{C}$. Hacemos la siguiente convención cuando trabajamos con curvas modulares:

> En el caso cuando $\mathcal{C}' = \mathbb{H}^*/\Gamma$ es una curva modular, entonces si $(\mathcal{C}, \varphi)$ es un modelo de $\mathbb{H}^*/\Gamma$ sobre $\mathbb{C}$, vamos a asumir sin pérdida de generalidad que $\varphi : \mathbb{H}^* \to \mathcal{C}$ es una función holomorfo $\Gamma-$invariante, en lugar de que el dominio de φ sea $\mathbb{H}^*/\Gamma$.

Ejemplo 4.1.2. Si $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ y $\mathbb{P}^1(\mathbb{C})$ es la esfera de Riemann definida sobre $\mathbb{C}$, entonces $(\mathbb{P}^1(\mathbb{C}), j)$ es un modelo de $X(1) = \mathbb{H}^*/\mathrm{SL}_2(\mathbb{Z})$ sobre $\mathbb{C}$ (cf. el lema 3.3.11).

El propósito de esta sección es describir la prueba de Shimura del problema de encontrar modelos de las curvas modulares:

Teorema 4.1.3. *(Shimura) Sea Γ un subgrupo de congruencia*[1]*, entonces existe un modelo $(\mathcal{C}_\Gamma, \varphi_\Gamma)$ de $X(\Gamma)$ sobre una extensión finita k_Γ de $\mathbb{Q}$. Además, la asignación $\Gamma \mapsto (\mathcal{C}_\Gamma/k_\Gamma, \varphi_\Gamma)$ cumple las siguientes dos propiedades. Sean Γ y Γ' dos subgrupos de congruencia y $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$ tal que $\gamma\Gamma\gamma^{-1} \subseteq \Gamma'$, entonces:*

1. $k_{\Gamma'} \subseteq k_\Gamma$,

[1]Shimura no se restringe al caso cuando Γ es de congruencia; él toma $\Gamma \subset \mathrm{PSL}_2(\mathbb{Q})$ como cualquier grupo Fuchsiano de primer tipo tal que contiene a $\Gamma(N)$ para alguna N, cf. el párrafo después del teorema 3.1.5.

2. La función racional $T : \mathcal{C}_\Gamma \to \mathcal{C}_{\Gamma'}$ inducida por la contención $\gamma\Gamma\gamma^{-1} \subseteq \Gamma'$,

$$\begin{array}{ccc} \mathbb{H}^* & \xrightarrow{z\mapsto\gamma z} & \mathbb{H}^* \\ {\scriptstyle\varphi_\Gamma}\downarrow & & \downarrow{\scriptstyle\varphi_{\Gamma'}} \\ \mathcal{C}_\Gamma & \xrightarrow[T/k_\Gamma]{} & \mathcal{C}_{\Gamma'} \end{array} \qquad T(\varphi_\Gamma(z)) := \varphi_{\Gamma'}(\gamma z). \tag{4.1.1}$$

está definida sobre k_Γ.

Demostración. cf. §6.7 de [Shi94], en particular las proposiciones 6.27 y 6.30. □

La idea clave para probar el teorema anterior es que dado $(\mathcal{C}_\Gamma, \varphi_\Gamma)$, un modelo de $X(\Gamma)$ sobre el campo numérico k_Γ, entonces el campo $\mathfrak{F}_\Gamma$, definido por

$$\mathfrak{F}_\Gamma = \{f \circ \varphi_\Gamma \mid f \in k_\Gamma(\mathcal{C}_\Gamma)\}, \tag{4.1.2}$$

donde $k_\Gamma(\mathcal{C}_\Gamma)$ es el campo de funciones racionales de $\mathcal{C}_\Gamma$, corresponde a un subconjunto abierto y compacto de $G_{\mathfrak{F}/\mathbb{Q}}$, el grupo de Galois de un campo $\mathfrak{F}$ que contiene a $\mathfrak{F}_\Gamma$ (cf. la definición 4.1.5 más adelante). De esta manera el problema se reduce a estudiar la estructura de $G_{\mathfrak{F}/\mathbb{Q}}$. Shimura prueba que $G_{\mathfrak{F}/\mathbb{Q}}$ es topológicamente isomorfo al cociente entre dos subgrupos de la "adelización" de GL_2 y por lo tanto $\mathfrak{F}_\Gamma$ corresponde a algún subgrupo abierto y compacto de la adelización de GL_2. De esta manera podemos reducir los resultados del teorema 4.1.3 a propiedades sobre los subrupos abiertos y compactos de la adelización de GL_2.

Para hacer más precisas estas ideas, primero definimos el campo $\mathfrak{F}$, repasamos sus propiedades básicas y luego construimos el grupo $\mathbb{A}_{\mathrm{GL}_2}$, la adelización de GL_2, y estudiamos sus propiedades básicas. Al final de la sección, explicamos cómo estas ideas se combinan para probar el teorema 4.1.3.

Vamos a definir el campo $\mathfrak{F}$ como una unión infinita de campos $\mathfrak{F}_N$ que generan a las formas automorfas de peso 0 y nivel N, i.e. $\mathbb{C}\otimes\mathfrak{F}_N = \mathcal{A}_0(\Gamma(N))$ donde $\Gamma(N)$ es el subgrupo de congruencia principal de nivel N. Para definir $\mathfrak{F}_N$, necesitamos las siguientes funciones auxiliares: sea a un vector en $\mathbb{Q}^2$ cuyas entradas no son ambas enteras, i.e. $a \notin \mathbb{Z}^2$, entonces definimos para $z \in \mathbb{H}$,

$$f_a(z) := \frac{g_2(z)g_3(z)}{\Delta(z)}\wp_\Lambda\big(a \cdot (z, 1)\big)$$

donde $\Lambda = z\mathbb{Z} \oplus \mathbb{Z}$ es una retícula y $\wp_\Lambda$ es la función de Weierstrass asociada a la retícula Λ.[2] Véase §6.1 de [Shi94].

Proposición 4.1.4. *Si definimos $\mathfrak{F}_1 := \mathbb{Q}(j)$ y:*

$$\mathfrak{F}_N := \mathbb{Q}\big(j, f_a \mid a \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}^2\big), \qquad (N > 1)$$

entonces $\mathfrak{F}_N/\mathbb{Q}(j)$ es una extensión de Galois que contiene a todas las raíces primitivas $N-$ésimas de la unidad. El grupo de Galois es:

$$\mathrm{Gal}(\mathfrak{F}_N/\mathfrak{F}_1) \cong \mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Por último, $\mathbb{C} \otimes \mathfrak{F}_N = \mathcal{A}_0(\Gamma(N))$ donde $\Gamma(N)$ es el subgrupo de congruencia principal de nivel N.

[2] Si fijamos z y variamos a, el conjunto de valores $\{f_a(z)\}$ es el conjunto de valores de la función de Weber asociado a la retícula Λ aplicada a los puntos de torsión de $\mathbb{C}/\Lambda$. Cuando z genera un campo cuadrático K el teorema de Weber-Feuter nos dice que la abelianización del campo cuadrático es igual al campo generado por $j(z)$ y los valores de la función de Weber. Véase el II.5 de [Sil99] y en particular el corolario 5.7

Demostración. Véase el teorema 6.6 de [Shi94] y la proposición 6.1 para la última afirmación. □

Este resultado es una generalización de Weber-Feuter a formas modulares y el grupo de Galois es una generalización dos dimensional del grupo de Galois del teorema de Kronecker-Weber. Con esto en mente, $\mathfrak{F}$ es el análogo modular de la extensión maximal abeliana:

Definición 4.1.5.

$$\mathfrak{F} := \bigcup_{N=1}^{\infty} \mathfrak{F}_N$$

Nota. Si $N \mid M$, entonces $\mathfrak{F}_N \subseteq \mathfrak{F}_M$, entonces por la proposición anterior, $\mathfrak{F}$ es una extensión de Galois de $\mathfrak{F}_1$ y $\mathbb{C} \otimes \mathfrak{F}$ es el espacio de todas las formas automorfas de peso 0 con respecto de cualquier subgrupo de congruencia.

Sea Γ un subgrupo de congruencia y retomemos el campo $\mathfrak{F}_\Gamma$ de (4.1.2). Como Γ es de congruencia, existe una N tal que $\Gamma(N) \subseteq \Gamma$, entonces si tomamos $\gamma = 1$ en el teorema 4.1.3 obtenemos $\mathfrak{F}_\Gamma \subseteq \mathfrak{F}_{\Gamma(N)} = \mathfrak{F}_N$ y por lo tanto $\mathfrak{F}_\Gamma \subseteq \mathfrak{F}$. Si la extensión $\mathfrak{F}/\mathfrak{F}_\Gamma$ es de Galois, entonces $\mathfrak{F}_\Gamma$ corresponde a un subgrupo abierto y compacto del grupo de Galois $G_{\mathfrak{F}/\mathbb{Q}}$.

Esta observación motiva a Shimura a estudiar el grupo de Galois $G_{\mathfrak{F}/\mathbb{Q}}$ y en particular sus subgrupos abiertos y compactos. En §6.6 de [Shi94], Shimura da una descripción explícita del grupo de Galois usando la "adelización" de GL_2 y notemos que esto sigue la analogía de Kronecker-Weber porque el grupo de Galois $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ está contenido en GL_1 de la adelización de $\mathrm{GL}_1(\mathbb{Q})$. Primero repasamos el concepto del grupo de *idèles* de un campo numérico y luego explicamos la generalización de Shimura de esta construcción al grupo GL_2.

Sea K un campo numérico y sea M_K el conjunto de clases de equivalencias de valores absolutos de K (cf. la notación de la sección 2.5). Para todo valor absoluto $|\cdot|_\nu$, con valuación asociada ν,de K, denotamos por K_ν a la completación de K con respecto de $|\cdot|_\nu$. Si $|\cdot|_\nu$ es no arquimediano (i.e. $|\cdot|_\nu \in M_K^0$), entonces denotamos por $\mathcal{O}_\nu$ al anillo de enteros de K_ν. Entonces definimos el grupo (topológico) de idèles de K como:

$$\mathbb{A}_K^* := \left\{ x = (x_\nu) \in \prod_{|\cdot|_\nu \in M_K} K_\nu^* \;\middle|\; x_\nu \in \mathcal{O}_\nu^* \text{ para casi toda } |\cdot|_\nu \in M_K \right\}$$

donde la topología es la del *producto restringido de* $\{K_\nu^*\}$ *con respecto de* $\{\mathcal{O}_\nu^*\}$. Más precisamente tomamos como base topológica a todos los conjuntos de la forma $\prod V_\nu$ donde $V_\nu \subseteq K_\nu^*$ es abierto para todo $|\cdot|_\nu$ y $V_\nu = \mathcal{O}_\nu^*$ para casi todo $|\cdot|_\nu$. Véase §13 de [Cas67] para un repaso de las propiedades de esta topología en este contexto.

La función diagonal $K^* \to \mathbb{A}_K^*$ definida por $\alpha \mapsto (\alpha, \alpha, \ldots)$ es inyectiva con imagen discreta y por lo tanto podemos identificar el grupo multiplicativo K^* con un subgrupo de $\mathbb{A}_K^*$. Otro subgrupo importante es $K_{\infty+}^*$ que definimos como la componente conexa de la identidad en K_∞^*, la componente arquimediana de $\mathbb{A}_K^*$.

Por la teoría de campos de clases,[3] hay una sucesión exacta:

$$1 \longrightarrow \overline{K^* K_{\infty+}^*} \longrightarrow \mathbb{A}_K^* \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K) \longrightarrow 1, \tag{4.1.3}$$

[3]Más precisamente, estamos usando el teorema 6, §9, del capítulo XIII de [Wei74] que es un ejemplo de los teoremas principales de la teoría de campos de clases sobre extensiones abelianas. Véase también [Tat67, §5] para otra formulación de estos teoremas.

donde $\overline{K^*K^*_{\infty+}}$ es la cerradura topológica del subgrupo $K^*K^*_{\infty+}$ en $\mathbb{A}_K^*$ y K^{ab} es la máxima extensión abeliana de K. Siguiendo a Shimura, denotamos por $[x, K] \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$ a un elemento que corresponde a $x \in \mathbb{A}_K^*$ bajo (4.1.3).

Ahora que hemos construido el grupo de idèles de un campo numérico K, revisamos una construcción similar que Shimura llama la "adelización" de GL_2. Nos especializamos al caso $K = \mathbb{Q}$, donde $M_{\mathbb{Q}}$ se puede identificar con $\{p \in \mathbb{Z} \mid p \text{ es primo}\} \cup \{\infty\}$. En este caso, a los elementos de $M_{\mathbb{Q}}$ los denotamos por p, donde p es primo o $p = \infty$. Con esta notación $p \in M_{\mathbb{Q}}$ es en realidad el valor absoluto $p-$ádico si $p < \infty$ y es el valor absoluto usual si $p = \infty$. En particular $\mathbb{Q}_p$ denota a los racionales $p-$ádicos si $p < \infty$ y $\mathbb{Q}_\infty = \mathbb{R}$.

Definición 4.1.6. Si denotamos $G_p := \mathrm{GL}_2(\mathbb{Q}_p)$, entonces la adelización de GL_2 es el grupo topológico

$$\mathrm{GL}_2(\mathbb{A}) := \Big\{ x = (x_p) \in \prod_{p \leq \infty} G_p \;\Big|\; x_p \in \mathrm{GL}_2(\mathbb{Z}_p) \text{ para casi toda } p \Big\}$$

con la topología del producto restringido de $\{G_p\}$ con respecto de $\{\mathrm{GL}_2(\mathbb{Z}_p)\}$.

Esta construcción es un ejemplo de un fenómeno general sobre la adelización de grupos algebraicos debida a Weil [Wei12].

Nota. El conjunto

$$U := \prod_{p<\infty} \mathrm{GL}_2(\mathbb{Z}_p) \times \mathrm{GL}_2^+(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{A}),$$

es un abierto de $\mathrm{GL}_2(\mathbb{A})$. En general, para toda $N > 1$, definimos:

$$U_N := \{x \in U \mid x_p \equiv \mathrm{Id} \pmod N,\ \forall p < \infty\},$$

donde $x_p \equiv \mathrm{Id} \pmod N$ significa $x_p = \mathrm{Id} + N\gamma$ para alguna $\gamma \in NM_{2\times 2}(\mathbb{Z}_p)$. Observe que $U_1 = U$ y que si $N \mid M$, entonces $U_M \subseteq U_N$. De esta manera, la familia $\{U_N\}_{N>0}$ es una base para la topología de $\mathrm{GL}_2(\mathbb{A})$ (cf. §6.4 de [Shi94]).

Las proyecciones $\pi_p : \mathrm{GL}_2(\mathbb{A}) \twoheadrightarrow G_p$ son homomorfismos continuos. El núcleo de la proyección π_∞ es un subgrupo normal que denotamos por G^0, la notación viene de la notación $M^0_{\mathbb{Q}}$; de hecho

$$G^0 := \ker\big(\mathrm{GL}_2(\mathbb{A}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{R})\big) = \{x \in \mathrm{GL}_2(\mathbb{A}) \mid x_\infty = 1\}.$$

Si multiplicamos G^0 por el factor $\mathrm{GL}_2^+(\mathbb{R})$ de U, obtenemos los elementos de $\mathrm{GL}_2(\mathbb{A})$ que son positivos en la componente infinita:

$$\mathrm{GL}_2^+(\mathbb{A}) := \prod_{p<\infty} G_p \times \mathrm{GL}_2^+(\mathbb{R}) = G^0 \cdot \mathrm{GL}_2^+(\mathbb{R}).$$

Como en el caso $K^* \hookrightarrow \mathbb{A}_K^* = \mathrm{GL}_1(\mathbb{A}_K)$, podemos identificar $\mathrm{GL}_2(\mathbb{Q})$ con un subgrupo de $\mathrm{GL}_2(\mathbb{A})$ mediante el encaje diagonal:

$$\mathrm{GL}_2(\mathbb{Q}) \lhook\joinrel\longrightarrow \mathrm{GL}_2(\mathbb{A}) \qquad \gamma \mapsto (\gamma, \gamma, \ldots)$$

En particular $\mathrm{GL}_2^+(\mathbb{Q}) = \{\gamma \in \mathrm{GL}_2(\mathbb{Q}) \mid \det\gamma > 0\}$ es un subgrupo de $\mathrm{GL}_2(\mathbb{A})$ y cumple:

$$\mathrm{GL}_2^+(\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Q}) \cap \mathrm{GL}_2^+(\mathbb{A}).$$

Por otro lado, en cada componente G_p de $\mathrm{GL}_2(\mathbb{A})$, tenemos la función continua $\det : G_p \to \mathbb{Q}_p^*$. Por la propiedad universal del producto, la familia de homomorfismos continuos $\{\det \circ \pi_p : \mathrm{GL}_2(\mathbb{A}) \to \mathbb{Q}_p^*\}$ induce un homomorfismo continuo y abierto:[4]

$$\det : \mathrm{GL}_2(\mathbb{A}) \longrightarrow \mathbb{A}_{\mathbb{Q}}^*, \qquad \det(x_p) = (\det x_p).$$

Si $V \subseteq \mathrm{GL}_2(\mathbb{A})$ es un abierto, entonces $\det(V) \subseteq \mathbb{A}_{\mathbb{Q}}^*$ es abierto y por lo tanto $\mathbb{Q}^* \cdot \det(V) \subseteq \mathbb{A}_{\mathbb{Q}}^*$ es un abierto que contiene a $\mathbb{Q}^* \cdot \mathbb{Q}_{\infty+}^*$. Gracias a la teoría de campos de clases y en particular a la sucesión exacta (4.1.3), tenemos que $\mathbb{Q}^* \cdot \det(V)$ corresponde a una extensión abeliana finita de $\mathbb{Q}$ que denotamos por k_V. En general se tiene:

Proposición 4.1.7. *Para todo abierto $V \subseteq \mathrm{GL}_2(\mathbb{A})$, existe una extensión abeliana finita $k_V/\mathbb{Q}$ que cumple las siguientes propiedades:*

1. *Para toda $x \in \mathrm{GL}_2(\mathbb{A})$ tenemos que $k_V = k_{xVx^{-1}}$.*
2. *Si $V \subseteq V'$ entonces $k_{V'} \subseteq k_V$.*
3. *Para los abiertos básicos U_N, tenemos $k_N := k_{U_N} = \mathbb{Q}(\zeta)$, donde ζ es una raíz $N-$ésima primitiva de la unidad.*

Demostración. Véase §6.4 de [Shi94] y en particular las fórmulas (6.4.4) y (6.4.5). □

Ahora estamos en posición para relacionar $\mathrm{Gal}(\mathfrak{F}/\mathbb{Q})$ con $\mathrm{GL}_2(\mathbb{A})$. El teorema principal sobre esta relación es:

Teorema 4.1.8. *Si denotamos $H := \mathbb{Q}^* \cdot \mathrm{GL}_2^+(\mathbb{R}) \subset \mathrm{GL}_2^+(\mathbb{A})$, entonces existe un homomorfismo $\tau : \mathrm{GL}_2^+(\mathbb{A}) \to \mathrm{Gal}(\mathfrak{F}/\mathbb{Q})$ que cabe en la sucesión exacta:*

$$1 \longrightarrow H \longrightarrow \mathrm{GL}_2^+(\mathbb{A}) \xrightarrow{\tau} \mathrm{Gal}(\mathfrak{F}/\mathbb{Q}) \longrightarrow 1$$

y además tenemos que $\mathrm{Gal}(\mathfrak{F}/\mathbb{Q}) \cong \mathrm{GL}_2^+(\mathbb{A})/H$ como grupos topológicos.

Demostración. Esto es exactamente el teorema 6.23 de [Shi94], la existencia de la sucesión exacta la prueba en §6.6 y el isomorfismo lo prueba en el mismo teorema. □

Nota. Este teorema es un análogo a la sucesión exacta (4.1.3) de la teoría de campos de clases, entonces a veces τ se llama el "mapeo de reciprocidad de Shimura", véase también el capítulo 11 de [Lan87].

Recuerde que los subgrupos cerrados (y por lo tanto compactos) de $\mathrm{Gal}(\mathfrak{F}/\mathbb{Q})$ corresponden a los subcampos intermedios de la extensión $\mathfrak{F}/\mathbb{Q}$. Los subgrupos abiertos corresponden a las subextensiones finitas. Gracias al teorema anterior, esto significa que los campos numéricos contenidos en $\mathfrak{F}$ corresponden a los subconjuntos abiertos V de $\mathrm{GL}_2^+(\mathbb{A})$ que contienen a H y cuyo cociente V/H es compacto.

Escribimos:

$$\mathcal{Z} := \{V \subseteq \mathrm{GL}_2^+(\mathbb{A}) \mid V \text{ es abierto, } H \subseteq V \text{ y } V/H \text{ es compacto}\},$$

[4] En cada componente $\det : G_p \to \mathbb{Q}_p^*$ es una función abierta. De esto junto con la topología del producto restringido, concluimos que $\det : \mathrm{GL}_2(\mathbb{A}) \to \mathrm{GL}_2(\mathbb{A})_{\mathbb{Q}}$ es abierta.

y para toda $V \in \mathcal{Z}$ definimos:

$$\Gamma_V := V \cap \mathrm{GL}_2^+(\mathbb{Q}), \qquad \mathfrak{F}_V := \{f \in \mathfrak{F} \mid f^{\tau(x)} = f,\ \forall x \in V\},$$

es decir $\mathfrak{F}_V$ es el campo fijo de $\tau(V) \subseteq \mathrm{Gal}(\mathfrak{F}/\mathbb{Q})$ que es abierto y por lo tanto $\mathfrak{F}_V$ es una extensión finita de $\mathbb{Q}$, no necesariamente abeliana.[5] Entonces los subgrupos $\Gamma_V \subset \mathrm{GL}_2^+(\mathbb{A})$ tienen las siguientes propiedades:

Proposición 4.1.9. *Para toda $V \in \mathcal{Z}$ tenemos que $\Gamma_V/\mathbb{Q}^*$ es (isomorfo a) un subgrupo de congruencia Γ y $\mathbb{C} \otimes \mathfrak{F}_V \cong \mathcal{A}_0(\Gamma)$. Por último, k_V es algebraicamente cerrado en $\mathfrak{F}_V$.*

Demostración. Véase la proposición 6.27 de [Shi94]. □

Nota. $\Gamma_V/\mathbb{Q}^*$ denota el cociente de la acción natural $\mathbb{Q}^* \curvearrowright \mathrm{GL}_2^+(\mathbb{Q})$ restringida a Γ_V.

Por último, tenemos:

Proposición 4.1.10. *Sea Γ un subgrupo de congruencia. Entonces existe una $V \in \mathcal{Z}$ tal que $\Gamma = \Gamma_V/\mathbb{Q}^*$.*

Demostración. Véase la proposición 6.30 de [Shi94]. □

Las proposiciones 4.1.9 y 4.1.10 nos da la existencia del modelo en el teorema 4.1.3. Para las otras propiedades enunciadas nos referimos a la discusión que sigue de la proposición 6.30 de §6.8 de [Shi94].

Para terminar la sección aplicamos el teorema 4.1.3 a los subgrupos de congruencia $\Gamma_0(N)$ y $\Gamma(N)$ (véase los últimos dos párrafos de §6.8 de [Shi94] para una prueba de los siguientes corolarios).

Corolario 4.1.11. *Para la curva modular $X_0(N)$ asociada a $\Gamma_0(N)$, tenemos que $k_{\Gamma_0(N)} = \mathbb{Q}$, entonces el modelo $(\mathcal{C}_{\Gamma_0(N)}, \varphi_{\Gamma_0(N)})$ está definido sobre $\mathbb{Q}$ y el campo de funciones de $\mathcal{C}_{\Gamma_0(N)}$ es $\mathfrak{F}_{\Gamma_0(N)} = \mathbb{Q}(j, j_N)$ donde $j_N(z) := j(Nz)$.*

Corolario 4.1.12. *Para la curva modular $X(N)$ asociada a $\Gamma(N)$, tenemos que $k_{\Gamma(N)} = \mathbb{Q}(e^{2\pi i/N})$, entonces el modelo $(\mathcal{C}_{\Gamma(N)}, \varphi_{\Gamma(N)})$ está definido sobre $\mathbb{Q}(e^{2\pi i/N})$ y el campo de funciones de $\mathcal{C}_{\Gamma(N)}$ es $\mathfrak{F}_N$ de la proposición 4.1.4.*

Nota. Para $N \geq 1$, tenemos que $\Gamma_0(N) \subseteq \Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$, entonces por el teorema 4.1.3, la proyección natural $X_0(N) \to X_0(1)$ induce un morfismo $\mathcal{C}_{\Gamma_0(N)} \to \mathcal{C}_{\Gamma_0(1)}$ definido sobre $\mathbb{Q}$.

4.2. El polinomio modular

En esta sección revisamos la parte de construir explícitamente un modelo de $X_0(N)$ sobre $\mathbb{Q}$. Más precisamente definimos un polinomio Φ_N con coeficientes en el campo $\mathbb{C}(j)$, donde j es el $j-$invariante de la sección 3.3. Luego vamos a probar que Φ_N es el polinomio mínimo de j_N, que está definido por $j_N(z) := j(Nz)$. Después veremos que Φ_N realmente tiene coeficientes en $\mathbb{Z}[j]$ y por lo tanto, visto como polinomio en $\mathbb{Z}[X, Y] \cong \mathbb{Z}[j][t]$, define una curva proyectiva sobre $\mathbb{Q}$.

[5] Uno puede pensar en $\mathfrak{F}_V$ como una generalización no abeliana del campo de clases asociado a V.

El polinomio modular lo vamos a definir como un producto de términos lineales de la forma $t - j \circ \gamma$ donde γ corre sobre el conjunto de matrices primitivas con determinante N que definimos en seguida:

$$M'_{\det=N} := \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}) \middle| \det \gamma = N, \text{ y } (a,b,c,d) = 1 \right\}.$$

La descomposición de $M'_{\det=N}$ en conjuntos disjuntos es:

Lema 4.2.1. *El conjunto de matrices primitivas de determinante N se puede descomponer como una unión finita disjunta*

$$M'_{\det=N} = \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \mathrm{SL}_2(\mathbb{Z}) = \bigcup_{\gamma} \mathrm{SL}_2(\mathbb{Z})\gamma \tag{4.2.1}$$

donde γ corre sobre el conjunto finito:

$$\gamma \in \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}) \;\middle|\; ad = N,\ 0 \le b < d \text{ y } (a,b,d) = 1 \right\}.$$

Demostración. Esto es parte del lema 9.1 de [Kna92], véase también el lema 8.15 que trata de esta descomposición en matrices no necesariamente primitivas. □

Nota. Hay

$$\psi(N) := N \prod_{p|N} \left(1 + \tfrac{1}{p}\right)$$

términos en la descomposición de $M'_{\det=N}$ en (4.2.1). A veces se le conoce como la función ψ de Dedekind. Con esto en mente, reescribimos la descomposición como:

$$M'_{\det=N} = \bigcup_{i=1}^{\psi(N)} \mathrm{SL}_2(\mathbb{Z})\gamma_i. \tag{4.2.2}$$

No es coincidencia que $\psi(N)$ es exactamente el índice de $\Gamma_0(N)$ en $\mathrm{SL}_2(\mathbb{Z})$ (cf. la formula (3.2.4) de la sección 3.2), de hecho la fórmula (4.2.1) se puede usar para calcular independientemente el índice $(\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N))$. Véase en particular la proposición 9.3 de [Kna92] para el cálculo de este índice con este método.

Para facilitar la notación, denotaremos

$$\gamma_1 := \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}.$$

De esta manera, podemos escribir $M'_{\det=N} = \mathrm{SL}_2(\mathbb{Z})\gamma_1\mathrm{SL}_2(\mathbb{Z})$. Esto prueba que $M'_{\det=N}$ es invariante bajo multiplicación por elementos de $\mathrm{SL}_2(\mathbb{Z})$. Más precisamente, si $\gamma \in M'_{\det=N}$, entonces existen $\sigma, \sigma' \in \mathrm{SL}_2(\mathbb{Z})$ tales que $\gamma = \sigma\gamma_1\sigma'$ y por lo tanto, para toda $\tau \in \mathrm{SL}_2(\mathbb{Z})$, tenemos que $\tau\gamma = (\tau\sigma)\gamma_1\sigma' \in \mathrm{SL}_2(\mathbb{Z})\gamma_1\mathrm{SL}_2(\mathbb{Z}) = M'_{\det=N}$ y similarmente $\gamma\tau \in M'_{\det=N}$.

Con esto, ya podemos definir el polinomio modular:

Definición 4.2.2. El *polinomio modular de orden* N es el polinomio en una variable t definido por:

$$\Phi_N(t) = \prod_{i=1}^{\psi(N)} (t - j \circ \gamma_i),$$

donde $j \circ \gamma_i = j[\gamma_i]_0$ donde $[\gamma_i]_0$ es el operador de peso 0 de la sección 3.3.

Nota. Como $j_N = j \circ \gamma_1$, tenemos j_N es una raíz de $\Phi_N(t)$.

El propósito de esta sección es probar que Φ_N es un polinomio irreducible sobre $\mathbb{C}(j)$ y que tiene coeficientes en $\mathbb{Z}[j]$, pero primero necesitamos estudiar las raíces del polinomio modular con más detalle. Específicamente, tenemos:

Proposición 4.2.3. *El conjunto* $\{j \circ \gamma_1, \ldots, j \circ \gamma_{\psi(N)}\}$ *de raíces de* $\Phi_N(t)$ *cumple las siguientes propiedades:*

1. *Todas las raíces son distintas, i.e.* $j \circ \gamma_i \neq j \circ \gamma_j$ *para toda* $i \neq j$.
2. *Cada* $j \circ \gamma_i : \mathbb{H} \to \mathbb{C}$ *admite una serie de Fourier meromorfa en* $q_N = e^{2\pi i z/N}$ *alrededor de* ∞.
3. *Existe una acción transitiva* $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \{j \circ \gamma_1, \ldots, j \circ \gamma_{\psi(N)}\}$ *definida por* $(\sigma, j \circ \gamma_i) \mapsto j \circ \gamma_i \sigma$ *donde* $\sigma \in \mathrm{SL}_2(\mathbb{Z})$.

Demostración. Para toda $i \in \{1, \ldots, \psi(N)\}$, escribimos la matriz $\gamma_i \in M'_{\det=N}$ como

$$\gamma_i = \begin{pmatrix} a_i & b_i \\ 0 & d_i \end{pmatrix}, \qquad \big(a_i d_i = N,\ 0 \leq b_i < d_i \text{ y } (a_i, b_i, d_i) = 1\big).$$

También escribimos $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

1. Para probar que las raíces son distintas, supongamos que $j \circ \gamma_i = j \circ \gamma_j$ para algunas i, j. Si escribimos la serie de Fourier de j como $j(z) = q^{-1} + F(q)$ donde $F \in \mathbb{Z}[[q]]$ es una serie de potencias, entonces para toda $z \in \mathbb{H}$ tenemos:

$$\begin{aligned}(j \circ \gamma_i)(z) = j\left(\frac{a_i z + b_i}{d_i}\right) &= e^{-2\pi i a_i z/d_i} e^{-2\pi i b_i/d_i} + F(e^{2\pi i a_i z/d_i} e^{2\pi i b_i/d_i}) \\ &= q_{d_i}^{-a_i} \zeta_{d_i}^{-b_i} + F(q_{d_i}^{a_i} \zeta_{d_i}^{b_i}), \quad \big(q_{d_i} = e^{2\pi i z/d_i},\ \zeta_{d_i} = e^{2\pi i/d_i}\big). \end{aligned} \tag{4.2.3}$$

   De la misma manera obtenemos una fórmula análoga para $j \circ \gamma_j$. Si invertimos formalmente la serie de potencias, obtenemos:

$$\frac{1}{(j \circ \gamma_i)(z)} = q_{d_i}^{a_i} \zeta_{d_i}^{b_i} + G(q_{d_i}^{a_i} \zeta_{d_i}^{b_i}),$$

   donde $G \in \mathbb{Z}[[q]]$ es una serie formal sin término constante ni lineal. Por lo tanto

$$1 = \frac{(j \circ \gamma_i)(z)}{(j \circ \gamma_j)(z)} = \frac{q_{d_i}^{-a_i} \zeta_{d_i}^{-b_i}}{q_{d_j}^{-a_j} \zeta_{d_j}^{-b_j}} + H(q_{d_i}^{a_i} \zeta_{d_i}^{b_i}, q_{d_j}^{a_j} \zeta_{d_j}^{b_j}),$$

donde H es una serie de potencias en dos variables sin término constante. Si hacemos $\Im(z) \to \infty$ en la ecuación anterior obtenemos:

$$q_{d_i}^{a_i}\zeta_{d_i}^{b_i} = q_{d_j}^{a_j}\zeta_{d_j}^{b_j} \quad \Longrightarrow \quad e^{2\pi iz\left(\frac{a_i}{d_i}-\frac{a_j}{d_j}\right)} = e^{2\pi i\left(\frac{b_j}{d_j}-\frac{b_i}{d_i}\right)}, \quad (z \in \mathbb{H}). \tag{4.2.4}$$

Esto sucede para toda $z \in \mathbb{H}$ solamente cuando $a_i/d_i = a_j/d_j$ que, después de multiplicar por $a_i d_i = N = a_j d_j$, implica que $a_j^2 = a_i^2$ y $d_j^2 = d_i^2$. Como a_i, a_j, d_i, d_j son todos no negativos por elección, concluimos que $a_i = a_j$ y $d_i = d_j$. Si sustituimos estas igualdades en (4.2.4) deducimos que $b_i = b_j$ y por lo tanto las matrices γ_i y γ_j son iguales. Hemos probado que si $j \circ \gamma_i = j \circ \gamma_j$, entonces $\gamma_i = \gamma_j$, es decir que todos los factores $(t - j \circ \gamma_i)$ del polinomio modular $\Phi_N(t)$ son distintos.

2. Para calcular la q_N-expansión de $j \circ \gamma_i$ alrededor de ∞, retomamos (4.2.3). Primero observemos que $1/d_i = a_i/N$ y por lo tanto

$$q_{d_i} = e^{2\pi iz/d_i} = e^{2\pi iza_i/N} = q_N^{a_i}, \qquad \zeta_{d_i} = \zeta_N^{a_i}.$$

Si escribimos la serie de potencias F como $F(q) = \sum_{n\geq 0} d_n q^n$ donde $d_n \in \mathbb{Z}$, entonces (4.2.3) se convierte en una serie de potencias en q_N con coeficientes en $\mathbb{C}$:

$$(j \circ \gamma_i)(z) = q_N^{-a_i^2}\zeta_N^{-a_i b_i} + \sum_{n=0}^{\infty} d_n (q_N^{a_i^2}\zeta_N^{a_i b_i})^n = \sum_{n=-1}^{\infty} D_n q_N^{na_i^2} \in \mathbb{C}[[q_N]], \tag{4.2.5}$$

donde $D_{-1} = \zeta_N^{-a_i b_i}$ y $D_n = d_n \zeta_N^{na_i b_i}$ para toda $n \geq 0$. Por lo tanto $j \circ \gamma_i$ admite una expansión en serie de Fourier alrededor de ∞ y así $j \circ \gamma_i$ es meromorfa en ∞.

3. Por último probamos que la acción de Γ sobre el conjunto de raíces $R := \{j \circ \gamma_1, \ldots, j \circ \gamma_{\psi(N)}\}$ está bien definida y es transitiva. Sea $\tau \in \Gamma$ arbitraria y $j \circ \gamma_i \in R$. Entonces, por la primera nota después del lema 4.2.1, tenemos que $\gamma_i \tau \in M'_{\det=N}$. Por la fórmula (4.2.1) del mismo lema, tenemos que existe una $j \in \{1, \ldots, \psi(N)\}$ tal que $\gamma_i \tau = \gamma_j$ y por lo tanto la acción $\Gamma \curvearrowright R$ hace

$$(\tau, j \circ \gamma_i) \mapsto = j \circ \gamma_i \tau = j \circ \gamma_j \in R.$$

Esto prueba que la acción $\Gamma \curvearrowright R$ está bien definida y permuta los elementos de R.

Para probar la transitividad de $\Gamma \curvearrowright R$, sea $j \circ \gamma_i \in R$ arbitrario. Como $\gamma_i \in \Gamma\gamma_1\Gamma$, existen $\sigma, \sigma' \in \Gamma$ tales que $\gamma_i = \sigma\gamma_1\sigma'$ o equivalentemente $\sigma^{-1}\gamma_i = \gamma_1\sigma'$. Por otro lado, la $\Gamma-$invarianza de j nos garantiza que:

$$(\sigma, j \circ \gamma_1) \mapsto j \circ \gamma_1\sigma = j \circ \sigma^{-1}\gamma_i = \left(j \circ \sigma^{-1}\right) \circ \gamma_i = j \circ \gamma_i.$$

Por lo tanto todas las raíces $j \circ \gamma_i$ están en la órbita de $j \circ \gamma_1$ y concluimos que la acción es transitiva.

□

Con estas propiedades sobre las raíces de $\Phi_N(t)$ podemos probar el teorema principal de esta sección:

Teorema 4.2.4. *El polinomio $\Phi_N(t)$ tiene coeficientes en $\mathbb{Z}[j]$ y es irreducible sobre $\mathbb{C}(j)$.*

Demostración. Otra vez escribimos $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. La prueba la haremos en cuatro pasos:

1. Los coeficientes de $\Phi_N(t)$ son funciones racionales de j, es decir $\Phi_N(t) \in \mathbb{C}(j)[t]$. Para ver esto, observe que por definición de Φ_N, sus coeficientes son polinomios simétricos en $\psi(N)$ variables evaluados en las raíces $j \circ \gamma_i$. Más precisamente, si escribimos:

$$\Phi_N(t) = c_{\psi(N)} + c_{\psi(N)-1}t + \cdots + c_1 t^{\psi(N)-1} + t^{\psi(N)},$$

entonces el coeficiente c_n de Φ_N es de la forma $\pm f_n(j \circ \gamma_1, \ldots, j \circ \gamma_{\psi(N)})$ donde f_n es el $n-$ésimo polinomio simétrico elemental[6]. En particular, como cada $j \circ \gamma_i$ es holomorfo sobre $\mathbb{H}$ (ya que las matrices γ_i son triangulares superiores), entonces cada coeficiente c_n de Φ_N es holomorfo sobre $\mathbb{H}$. Por el lema 4.2.3, cada $j \circ \gamma_i$ admite una q_N-expansión de Fourier meromorfa alrededor de ∞ y de esta manera c_n también admite una q_N-expansión de Fourier meromorfa alrededor de ∞. Por último tenemos que para toda $\sigma \in \Gamma$,

$$\begin{aligned} c_n[\sigma]_0 &= \pm f_n\big(j \circ \gamma_1, \ldots, j \circ \gamma_{\psi(N)}\big)[\sigma]_0 = \pm f_n\big(j \circ \gamma_1[\sigma]_0, \ldots, j \circ \gamma_{\psi(N)}[\sigma]_0\big) \\ &= \pm f_n(j \circ \gamma_1, \ldots, j \circ \gamma_{\psi(N)}) = c_n, \end{aligned}$$

porque la acción de Γ sobre las raíces las permuta y f_n es un polinomio simétrico, i.e. invariante bajo permutaciones de las variables. Por lo tanto c_n es automorfa de peso 0 con respecto de Γ. Por la proposición 3.3.10, concluimos que $c_n \in \mathbb{C}(j)$ para toda n y así obtenemos que $\Phi_N(t) \in \mathbb{C}(j)[t]$.

2. $\Phi_N(t)$ es irreducible sobre $\mathbb{C}(j)$. Sea $K = \mathbb{C}(j \circ \gamma_1, \ldots, j \circ \gamma_{\psi(N)})$ el campo de descomposición de $\Phi_N(t)$ sobre $\mathbb{C}(j)$ y supongamos que $\Phi_N(t)$ es reducible sobre $\mathbb{C}(j)$. Por el lema 4.2.3, las raíces de Φ_N son distintas, por lo tanto Φ_N no es una potencia de un polinomio irreducible y así tiene al menos dos factores $f, g \in \mathbb{C}(j)[t]$ irreducibles *distintos*.

   Como Γ actúa sobre K como automorfismos de K que fijan a $\mathbb{C}(j)$, entonces si $j \circ \gamma_i$ es una raíz de f, tenemos que para toda $\sigma \in \Gamma$, $j \circ \gamma_i\sigma$ sigue siendo una raíz de f. Como $f \neq g$, entonces no comparten raíces en el campo de descomposición K porque son polinomios irreducibles distintos. Por lo tanto las raíces de f pertenecen a una órbita de la acción de Γ sobre K y las raíces de g pertenecen a otra órbita distinta. Esto contradice la transitividad de la acción de Γ en las raíces de Φ_N. Con esto concluimos que Φ_N es irreducible sobre $\mathbb{C}(j)$.

3. Los coeficientes de Fourier de c_n son enteros. Retomamos la fórmula (4.2.3) de la prueba del lema 4.2.3 sin el subíndice i:

$$\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \quad \Longrightarrow \quad (j \circ \gamma)(z) = \zeta_d^{-a} q_d^{-a} + F(\zeta_d^b q_d^a),$$

[6]Los polinomios simétricos elementales en m variables con coeficientes en un campo k, se definen como:

$$\begin{aligned} f_1(x_1, \ldots, x_m) &= x_1 + \cdots + x_m, \\ f_2(x_1, \ldots, x_m) &= x_1x_2 + \cdots + x_{m-1}x_m, \\ &\vdots \\ f_m(x_1, \ldots, x_m) &= x_1 \cdots x_m. \end{aligned}$$

En general, si Σ es el grupo de permutaciones de m elementos, entonces los polinomios $f(x_1, \ldots, x_m)$ invariantes bajo la acción de permutar las variables, i.e. $(\sigma, f) \mapsto f(x_{\sigma(1)}, \ldots, f_{\sigma(m)})$, forman un subanillo S de $k[x_1, \ldots, x_m]$ que es generado como $k-$álgebra por los polinomios simétricos elementales, es decir $S \cong k[f_1, \ldots, f_m]$ como $k-$álgebras.

donde $F \in \mathbb{Z}[[q]]$. Como $d \mid N$, tenemos que $\zeta_d = \zeta_N^{N/d}$ y $q_d = q_N^{N/d}$ y por lo tanto el lado derecho de la fórmula de arriba es una serie de potencias en q_N con coeficientes en $\mathbb{Z}[\zeta_N]$. Además, como $c_n = \pm f_n(j \circ \gamma_1, \ldots, j \circ \gamma_{\psi(N)})$, entonces los coeficientes de Fourier de la q_N-expansión de c_n también pertenecen a $\mathbb{Z}[\zeta_N]$. Esto lo escribimos como:

$$c_n \in \mathbb{Z}[\zeta_N][[q_N]]. \tag{4.2.6}$$

Por otro lado consideremos los coeficientes de Fourier de c_n como elementos de la extensión ciclotómica $\mathbb{Q}(\zeta_N)$. Los $\mathbb{Q}-$automorfismos de $\mathbb{Q}(\zeta_N)$ están dados por $\zeta_N \mapsto \zeta_N^r$ donde $(r, N) = 1$. Bajo este automorfismo tenemos que:

$$(j \circ \gamma)(z) \mapsto \zeta_d^{-br} q_d^{-a} + F(\zeta_d^{br} q_d^a).$$

Si escribimos b' como el mínimo residuo no negativo de br módulo d, entonces $b' \equiv br \pmod{d}$ y así $\zeta_d^{br} = \zeta_d^{b'}$. Por lo tanto tenemos que bajo el $\mathbb{Q}-$automorfismo $\zeta_N \mapsto \zeta_N^r$, tenemos que

$$(j \circ \gamma)(z) \mapsto \zeta_d^{-b'} q_d^{-a} + F(\zeta_d^{b'} q_d^a) = (j \circ \gamma')(z), \quad \text{donde } \gamma' = \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}.$$

Observe que por la descripción de $M'_{\det=N}$ del lema 4.2.3, tenemos que $\gamma' = \gamma_i$ para alguna $i \in \{1, \ldots, \psi(N)\}$. Esto significa que el $\mathbb{Q}-$automorfismo $\zeta_N \mapsto \zeta_N^r$ induce la siguiente permutación de las matrices $\{\gamma_1, \ldots, \gamma_{\psi(N)}\}$:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}, \quad \text{donde } b' \equiv br \pmod{d} \text{ y } 0 \leq b' < d.$$

En efecto, como $(r, N) = 1$, la función $b \mapsto b'$ es una permutación del conjunto de residuos $\{0, 1, \ldots, d-1\}$ y por lo tanto la acción de arriba permuta las matrices $\{\gamma_1, \ldots, \gamma_{\psi(N)}\}$.

Concluimos que el $\mathbb{Q}-$automorfismo $\zeta_N \mapsto \zeta_N^r$, donde $(r, N) = 1$, permuta el conjunto $\{j \circ \gamma_1, \ldots, j \circ \gamma_{\psi(N)}\}$ y por lo tanto fija a los coeficientes de la q_N-expansión de c_n, porque éste es un polinomio simétrico en las q_N-expansiones de las series de Fourier de las $j \circ \gamma_i$s. Como $\mathbb{Q}(\zeta_N)$ es una extensión de Galois de $\mathbb{Q}$, esto implica que los coeficientes de la q_N-expansión de c_n son racionales, i.e. $c_n \in \mathbb{Q}[[q_N]]$. Gracias a (4.2.6) y a que $\mathbb{Z} = \mathbb{Q} \cap \mathbb{Z}[\zeta_N]$,[7] podemos concluir que $c_n \in \mathbb{Z}[[q]]$.

4. Los coeficientes de $\Phi_N(t)$, están contenidos en $\mathbb{Z}[j]$. Este hecho se sigue del siguiente resultado general: sea $f \in \mathcal{A}_0(\Gamma)$ con expansión de Fourier $f(z) = \sum_{n=-M}^{\infty} a_n(f) q^n$ meromorfa alrededor de ∞ ($M \geq 0$), entonces:

$$f \in \mathcal{A}_0(\Gamma) \text{ es holomorfo sobre } \mathbb{H} \implies f \in \big(\mathbb{Z}[a_{-M}(f), a_{-M+1}(f), \ldots]\big)[j], \tag{4.2.7}$$

es decir que f es un polinomio en j con coeficientes en el $\mathbb{Z}-$módulo generado por los coeficientes de Fourier de f.

Por el momento, supongamos que (4.2.7) es cierto. Como cada coeficiente $c_n \in \mathbb{C}(j) = \mathcal{A}_0(\Gamma)$ es un polinomio simétrico evaluado en las funciones holomorfas $j \circ \gamma_i$, entonces cada c_n

[7] Los elementos de $\mathbb{Z}[\zeta_N]$ son raíces de polinomios mónicos y los únicos elementos de $\mathbb{Q}$ que son raíces de polinomios mónicos son los enteros, porque $\mathbb{Z}$ es un dominio de factorización única y por lo tanto íntegramente cerrado en su campo de fracciones.

es holomorfo en $\mathbb{H}$. Por (4.2.7) concluimos que $c_n \in (\mathbb{Z}[a_{-M}(c_n), a_{-M+1}(c_n), \ldots])[j]$, pero por el paso anterior, todos los coeficientes de Fourier $a_n(c_n)$ son enteros y por lo tanto $\mathbb{Z}[a_{-M}(c_n), a_{-M+1}(c_n), \ldots] = \mathbb{Z}$. Concluimos que $c_n \in \mathbb{Z}[j]$ para todo coeficiente de $\Phi_N(t)$.

Entonces solamente falta probar (4.2.7). Esto lo hacemos por inducción sobre M. Cuando $M = 0$, entonces f es holomorfo en ∞ y por lo tanto induce una función holomorfa sobre la superficie de Riemann compacta $X_0(1)$, es decir f es constante y vale $a_0(f)$. En particular $f \in (\mathbb{Z}[a_0(f), a_1(f), \ldots])[j]$. Ahora supongamos que (4.2.7) es cierto para $M-1$. La idea es cancelar el primer término $a_{-M}(f)q^{-M}$ de la serie de Fourier de f con una potencia adecuada de j. Más precisamente:

$$(f - a_{-M}(f)j^M)(z) = \sum_{n=-M}^{\infty} a_n(f)q^n - a_{-M}(f)\left(\frac{1}{q} + F(q)\right)^M := \sum_{n=-(M-1)}^{\infty} d_n q^n,$$

donde $F(q) \in \mathbb{Z}[[q]]$. Los coeficientes d_n pertenecen a $a_n(f) + a_{-M}(f)\mathbb{Z}$ por construcción, y por hipótesis de inducción, pertenecen al $\mathbb{Z}-$módulo generado por $d_{-M+1}, d_{-M+2}, \ldots$, es decir:

$$\begin{aligned} d_n \in \mathbb{Z}[d_{-M+1}, d_{-M+2}, \ldots] &\subseteq \mathbb{Z}[a_{-M+1}(f) + a_{-M}(f)\mathbb{Z}, a_{-M+2}(f) + a_{-M}(f)\mathbb{Z}, \ldots] \\ &\subseteq \mathbb{Z}[a_{-M}(f), a_{-M+1}(f), a_{-M+2}(f), \ldots]. \end{aligned}$$

Con esto concluimos que $f - a_{-M}(f)j^M \in (\mathbb{Z}[a_{-M}(f), a_{-M+1}(f), \ldots])[j]$ y por lo tanto $f \in (\mathbb{Z}[a_{-M}(f), a_{-M+1}(f), \ldots])[j]$. Esto termina la inducción y la prueba de (4.2.7).

□

Para cerrar la sección mencionamos algunas consecuencias directas de las propiedades del polinomio modular.

Primero recuerde que los coeficientes $c_n \in \mathbb{Z}[j]$, entonces para cada $n \geq 0$, existe un polinomio $f_n(X) \in \mathbb{Z}[X]$ tal que $c_n = f_n(j)$. Por lo tanto el polinomio modular lo podemos reescribir como $\Phi_N(t) = f(j, t)$ donde $f(X, Y)$ es el polinomio

$$f_{\psi(N)}(X) + f_{\psi(N)-1}(X)Y + \cdots + f_1(X)Y^{\psi(N)-1} + f_0(X)Y^{\psi(N)} \in \mathbb{Z}[X, Y].$$

También denotamos por $\Phi_N(X, Y)$ al polinomio de arriba y observamos que no debe causar confusión con el polinomio modular porque no tienen la misma cantidad de variables.

Como $\Phi_N(X, Y)$ es irreducible, define una curva algebraica afín sobre $\mathbb{Q}$, más precisamente

Definición 4.2.5. Sea $N \geq 1$. El *modelo afín de* la curva modular $X_0(N)$ lo definimos como la curva sobre $\mathbb{Q}$ definida por la ecuación $\Phi_N(X, Y) = 0$ y la denotamos por $\mathcal{C}_N$.

Escribimos $\overline{\mathcal{C}}_N$ como la proyectivización de $\mathcal{C}_N$ definida sobre $\mathbb{Q}$, i.e. los ceros de la homogenización de Φ_N. Tomamos $X/\mathbb{Q}$, junto con un morfismo birracional $f : X \to \overline{\mathcal{C}}_N$ como la desingularización de $\overline{\mathcal{C}}_N$, i.e. X es proyectiva, lisa y única entre las curvas proyectivas y lisas que admiten morfismos birracionales a $\overline{\mathcal{C}}_N$ (cf. el teorema 3 de §7.5 de [Ful08]). Observe que en los $\mathbb{C}-$puntos de X y $\overline{\mathcal{C}}_N$ tenemos una función birracional $X(\mathbb{C}) \to \overline{\mathcal{C}}_N(\mathbb{C})$.

Definición 4.2.6. Con la notación de arriba, decimos que X es el *modelo racional* de $X_0(N) = \mathbb{H}/\Gamma_0(N)$ y lo denotamos por $X_0^{\mathbb{Q}}(N)$.

Con esto podemos definir la modularidad de curvas elípticas:

Definición 4.2.7. Sea $E/\mathbb{Q}$ una curva elíptica. Decimos que E es *modular* si existe un entero $N > 0$ y un morfismo no constante $X_0^{\mathbb{Q}}(N) \to E$. A este morfismo lo llamamos una *parametrización modular* de E de *nivel* N.

Nota. Si $N \mid M$, entonces vimos que hay una proyección natural $X_0(M) \to X_0(N)$ de superficies de Riemann. Gracias a la teoría de modelos de Shimura, esta proyección induce un morfismo $X_0^{\mathbb{Q}}(M) \to X_0^{\mathbb{Q}}(N)$ definido sobre $\mathbb{Q}$ (cf. el teorema 4.1.3). Por lo tanto la existencia de una parametrización modular $X_0^{\mathbb{Q}}(N) \to E$ implica que existen una infinidad de otras parametrizaciones modulares, una para cada múltiplo positivo de N.

Definición 4.2.8. Sea $E/\mathbb{Q}$ una curva elíptica modular. Decimos que N_0 es el *conductor analítico* de E si es el nivel más pequeño de las parametrizaciones modulares que admite E.

4.3. Curvas modulares como espacios moduli

En esta sección vamos a ver que ciertas curvas modulares $X(\Gamma) := \mathbb{H}^*/\Gamma$ (o más precisamente la subvariedad abierta $Y(\Gamma) = \mathbb{H}/\Gamma$) parametrizan clases de isomorfismo entre curvas elípticas cuyos ismorfismos preservan cierta información de torsión determinada por el subgrupo de congruencia Γ.

Para precisar esta idea, primero definimos el espacio de curvas elípticas como

$$\mathcal{E}(K) = \{E/K \text{ es curva elíptica}\}.$$

Decimos que dos curvas $E, E' \in \mathcal{E}(K)$ son *isomorfas* si existe un isomorfismo $f : E \to E'$ definido sobre K. Esto define una relación de equivalencia y denotamos a las clases de equivalencia por $[E]$. En el caso $K = \mathbb{C}$, el espacio cociente $\mathcal{E}(\mathbb{C})/_{\cong}$ es el primer ejemplo de curva modular como espacio moduli.

Ejemplo 4.3.1. Definimos $\mathcal{J} : \mathcal{E}(\mathbb{C})/_{\cong} \to \mathbb{C}$ con $[E] \mapsto j(E)$. Gracias al teorema 2.1.5, $E \cong E'$ sobre $\mathbb{C}$ si y solo si $j(E) = j(E)$, entonces $\mathcal{J}$ está bien definida y es inyectiva. Como dado un valor $j_0 \in \mathbb{C}$ podemos construir una curva $E_0/\mathbb{C}$ tal que $j(E) = j_0$, entonces $\mathcal{J}$ es biyectiva. Por último componemos con la función inversa $j^{-1} : \mathbb{C} \to \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ del lema 3.3.11, para obtener una biyección:

$$\mathcal{E}(\mathbb{C})/_{\cong} \longleftrightarrow Y(\mathrm{SL}_2(\mathbb{Z})), \qquad [E] \mapsto \tau\mathrm{SL}_2(\mathbb{Z}) \text{ tal que } j(E) = j\big(\tau\mathrm{SL}_2(\mathbb{Z})\big),$$

donde la j del lado izquierdo es el invariante de la curva elíptica E y la j del lado derecho es la forma automorfa de peso 0.

En general, vamos a estar interesados en los subgrupos de congruencia principales: $\Gamma(N), \Gamma_1(N)$ y $\Gamma_0(N)$. En esta sección vamos a asumir que todo subgrupo de congruencia Γ es de uno de los tres tipos anteriores.

Resulta que el ejemplo anterior se puede generalizar: dado Γ existe una biyección entre $Y(\Gamma)$ y un espacio de clases de isomorfismos de curvas elípticas, donde los isomorfismo preservan cierta información de torsión. Para cada forma de Γ de nuestro interés describimos un espacio de curvas elípticas sobre $\mathbb{C}$, definimos una noción de isomorfismo en ese espacio y damos una biyección entre $Y(\Gamma)$ y las clases de isomorfismo.

Para los diferentes posibles valores de Γ, definimos:

Definición 4.3.2. Sea $K \subseteq \mathbb{C}$. Para $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ de una de las siguientes formas, definimos una categoría de curvas elípticas sobre K cuyos isomorfismos preservan cierta información de torsión que depende de Γ:

1. $\big(\Gamma = \Gamma_0(N)\big)$

$$\mathcal{E}_0(N)(K) := \left\{ (E, C) \;:\; \begin{array}{c} E/K \text{ curva elíptica,} \\ C \subseteq E(\overline{K}) \text{ subgrupo cíclico} \\ \text{de orden } N \text{ y } G_K - \text{estable} \end{array} \right\}, \quad \begin{array}{c} (E,C) \cong (E',C') \text{ si :} \\ \exists f : E \xrightarrow{\sim} E' \text{ sobre } K, \\ f(C) = C' \end{array}$$

2. $\big(\Gamma = \Gamma_1(N)\big)$

$$\mathcal{E}_1(N)(K) := \left\{ (E, P) \;:\; \begin{array}{c} E/K \text{ curva elíptica,} \\ P \in E[N] \text{ es de orden } N \\ \text{y es } G_K - \text{estable} \end{array} \right\}, \quad \begin{array}{c} (E,P) \cong (E',P') \text{ si :} \\ \exists f : E \xrightarrow{\sim} E' \text{ sobre } K, \\ f(P) = P' \end{array}$$

3. $\big(\Gamma = \Gamma(N)\big)$

$$\mathcal{E}(N)(K) := \left\{ (E, P, Q) \;:\; \begin{array}{c} E/K \text{ curva elíptica,} \\ P, Q \in E[N],\ G_K - \text{estables,} \\ \text{tales que } \langle P, Q\rangle_{\mathbb{Z}/N\mathbb{Z}} = E[N] \end{array} \right\}, \quad \begin{array}{c} (E,P,Q) \cong (E',P',Q') \text{ si :} \\ \exists f : E \xrightarrow{\sim} E' \text{ sobre } K, \\ f(P) = P',\ f(Q) = Q' \end{array}$$

Nota. Si nos queremos referir a alguna de estas categorías asociada a un Γ de la forma $\Gamma_0(N)$, $\Gamma_1(N)$ o $\Gamma(N)$, escribimos $\mathcal{E}(\Gamma)(K)$ en lugar de $\mathcal{E}_0(N)(K)$, $\mathcal{E}_1(N)(K)$ o $\mathcal{E}(N)(K)$ respectivamente.

Nota. Si K es algebraicamente cerrado (e.g. $\mathbb{C}$ o $\overline{\mathbb{Q}}$), la condición de G_K-estabilidad se cumple automáticamente.

Nota. Si $N = 1$, entonces tenemos que $\mathcal{E}(K) = \mathcal{E}_0(1)(K) = \mathcal{E}_1(1)(K) = \mathcal{E}(1)(K)$, o más precisamente, las categorías son todas equivalentes a $\mathcal{E}(K)$, la clase de curvas elípticas sobre K. En particular, para toda $N \geq 1$, tenemos un funtor que olvida la estructura $\mathcal{E}(\Gamma)(K) \to \mathcal{E}(K)$, por ejemplo $(E, C) \mapsto E$ o $(E, P, Q) \mapsto E$.

Definición 4.3.3. Dado $\Gamma = \Gamma_0(N), \Gamma_1(N)$ o $\Gamma(N)$, al conjunto de clases de isomorfismo en $\mathcal{E}(\Gamma)(K)$ lo denotamos por

$$S(\Gamma)(K) = \mathcal{E}(\Gamma)(K)/_{\cong},$$

y a sus elementos los denotamos por $[E, C]$ (resp. $[E, P]$ o $[E, P, Q]$) para los elementos de $S_0(N)(K)$ (resp. $S_1(N)(K)$ o $S(N)(K)$).

Para el caso $K = \mathbb{C}$, los conjuntos $S(\Gamma)(\mathbb{C})$ se pueden identificar con el cociente $\mathbb{H}/\Gamma$ de manera explícita. Gracias al teorema de uniformización (cf. el teorema 2.2.3), para toda curva elíptica $E/\mathbb{C}$ existe una $\tau \in \mathbb{H}$ 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 $E_\tau := \mathbb{C}/\Lambda_\tau$. De esta manera las clases de isomorfismo de $S_0(\mathbb{C})$ (resp. $S_1(N)(\mathbb{C})$ o $S(N)(\mathbb{C})$ son de la forma $[E_\tau, \langle N^{-1} + \Lambda_\tau\rangle]$ (resp. $[E_\tau, N^{-1} + \Lambda_\tau]$ o $[E_\tau, \tau N^{-1} + \Lambda_\tau, N^{-1} + \Lambda_\tau]$). Verificamos esto en seguida para el caso $\Gamma = \Gamma_0(N)$:

Primero probamos que toda $[E, C] \in S_0(N)$ es de la forma $[E_\tau, \langle N^{-1} + \Lambda_\tau \rangle]$ para alguna $\tau \in \mathbb{H}$. Fijamos $[E, C] \in S_0(N)$ y sea $Q \in C$ un generador de C, 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 suprayectiva, se 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

$$\tau' = \sigma'\tau = \frac{a'\tau + b'}{c'\tau + d'} \tag{4.3.1}$$

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

$$m\Lambda_{\tau'} = m(\tau'\mathbb{Z} \oplus \mathbb{Z}) = m\tau'\mathbb{Z} \oplus m\mathbb{Z} = (a'\tau + b')\mathbb{Z} \oplus (c'\tau + d')\mathbb{Z}. \tag{4.3.2}$$

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 $\mathrm{PSL}_2(\mathbb{Z}) \curvearrowright \mathbb{H}$.[8] 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 (4.3.2) 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 (cf. el corolario 1.3.3 de [DS05]). 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 $\tau' \in \mathbb{H}$.

Observamos que este argumento se puede generalizar fácilmente a los demás subgrupos de congruencia con los que estamos trabajando, i.e. $\Gamma_1(N)$ y $\Gamma(N)$. Por lo tanto podemos asumir que las clases de isomorfismo $[E,C]$ (resp. $[E,P]$ y $[E,P,Q]$) están representadas por $[E_\tau, \langle N^{-1}+\Lambda_\tau\rangle]$ (resp. $[E_\tau, N^{-1}+\Lambda_\tau]$ o $[E_\tau, \tau N^{-1}+\Lambda_\tau, N^{-1}+\Lambda_\tau]$) para alguna $\tau \in \mathbb{H}$. De esta manera podemos definir biyecciones entre $S(\Gamma)(N)$ y $Y(\Gamma) = \mathbb{H}/\Gamma$.

Proposición 4.3.4. *Para cada Γ de la forma $\Gamma_0(N), \Gamma_1(N)$ o $\Gamma(N)$, tenemos las siguientes funciones:*

I) *La función $S_0(N)(\mathbb{C}) \to Y_0(N)$ definida por $[E_\tau, \langle N^{-1}+\Lambda_\tau\rangle] \mapsto \tau\Gamma_0(N)$ es biyectiva.*

II) *La función $S_1(N)(\mathbb{C}) \to Y_1(N)$ definida por $[E_\tau, N^{-1}+\Lambda_\tau] \mapsto \tau\Gamma_1(N)$ es biyectiva.*

III) *La función $S(N)(\mathbb{C}) \to Y(N)$ definida por $[E_\tau, \tau N^{-1}+\Lambda_\tau, N^{-1}+\Lambda_\tau] \mapsto \tau\Gamma(N)$ es biyectiva.*

Demostración. Solamente probamos el caso $\Gamma = \Gamma_0(N)$ y nos referimos a [Hus04, §2, capítulo 11] para los otros dos casos. Si escribimos ψ como la función $S_0(N)(\mathbb{C}) \to \mathbb{H}/\Gamma_0(N)$, tenemos que probar que ψ cumple tres cosas:

I) ψ 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 una $m \in \mathbb{C}^*$ 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 8). 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

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

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 8.

[8] 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 [Ser73]). En particular tenemos que

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

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 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 (4.3.1). De manera análoga a (4.3.2) 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 $\psi_{\Gamma_0(N)}$ es inyectiva.

III) ψ es suprayectiva.

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. $\psi_{\Gamma_0(N)}[E_\tau,\langle N^{-1}+\Lambda_\tau\rangle]=\tau\Gamma_0(N)$ y Ψ_N es suprayectiva.

□

Nota. Decimos que $S(\Gamma)(\mathbb{C})$ es un *espacio moduli* de clases de isomorfismo de curvas elípticas complejas con datos de $N-$torsión.

Ahora describimos $S_0(N)(\mathbb{C})$ con clases de isogenias de núcleo cíclico y de orden N. En el caso de $\Gamma=\Gamma_0(N)$, podemos identificar $S_0(N)(K)$ con otro conjunto de clases de equivalencia. Los objetos son isogenias $\varphi:E\to E'$ definidas sobre K con núcleo cíclico de orden N; a éstas se les llama $N-$*isogenias*. Al conjunto de estas isogenias lo denotamos por

$$\mathrm{Isog}_N(K):=\left\{\varphi:E\longrightarrow E'\;\middle|\;\varphi\text{ es una }N-\text{isogenia sobre }K\right\}$$

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:

$$\begin{array}{ccc} E_1 & \xrightarrow{\sim} & E_2 \\ {\scriptstyle\varphi_1}\downarrow & & \downarrow{\scriptstyle\varphi_2} \\ E_1' & \xrightarrow{\sim} & E_2' \end{array} \tag{4.3.3}$$

A la clase de isomorfismo de $N-$isogenias, la denotamos por $\mathrm{Isog}_N(K)/_{\cong}$ y sus elementos por $[\varphi : E \to E']$.

La función

$$\mathrm{Isog}_N(K) \longrightarrow S_0(N)(K) \quad \text{definida por} \quad [E \xrightarrow{\varphi} E'] \mapsto [E, \ker\varphi] \tag{4.3.4}$$

es una biyección. Claramente está bien definida por la conmutatividad del diagrama (4.3.3).

Para construir su inverso, recuerde que para todo subgrupo finito C de E, existe una única curva elíptica definida sobre K, denotada por E/C, y una isogenia $E \to E/C$ definida sobre K con núcleo C (cf. teorema 2.1.8), i.e. una $N-$isogenia. Esta asignación sugiere que el inverso de (4.3.4) 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 (4.3.4) y por lo tanto es una biyección.

Cuando $K = \mathbb{C}$, la clase $[E_\tau, \langle N^{-1} + \Lambda_\tau\rangle] \in S_0(N)(\mathbb{C})$ corresponde a la clase $[E_\tau \xrightarrow{\varphi} E_{N\tau}] \in \mathrm{Isog}_N(\mathbb{C})$ 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 la proposición 4.3.4, nos produce las siguientes dos biyecciones:

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

De esta manera, tenemos la función $Y_0(N) \to \mathrm{Isog}_N(\mathbb{C})$ definida por $\tau\Gamma_0(N) \mapsto [E_\tau \to E_{N\tau}]$. Si componemos esto con la función $[E \to E'] \mapsto (j(E), j(E')) \in \mathbb{A}^2_{\mathbb{C}}$, obtenemos la siguiente función:

$$Y_0(N) \longrightarrow \mathbb{A}^2_{\mathbb{C}} \quad \text{definida por} \quad \tau\Gamma_0(N) \mapsto \big(j(E_\tau), j(E_{N\tau})\big) = (j(\tau), j_N(\tau)). \tag{4.3.5}$$

Observe que la función anterior está bien definida porque j y j_N son $\Gamma_0(N)-$invariantes. Por definición, la imagen está contenida en los ceros del polinomio modular Φ_N visto como un polinomio en $\Phi_N \in \mathbb{Q}[X, Y]$. Más precisamente, si tomamos $\mathcal{C}_N \subset \mathbb{A}^2_{\mathbb{C}}$ como la curva afín definida por la ecuación $\Phi_N(X, Y) = 0$, los resultados de la sección anterior nos dicen que la imagen de $\tau\Gamma_0(N) \mapsto (j(\tau), j_N(\tau))$ está contenida en $\mathcal{C}_N(\mathbb{C})$.

Si componemos (4.3.5) con la biyección de la proposición 4.3.4 obtenemos una función explícita:

$$S_0(N)(\mathbb{C}) \longrightarrow \mathcal{C}_N(\mathbb{C}) \quad \text{definida por} \quad [E, C] \mapsto \big(j(E), j(E/C)\big).$$

De hecho como j es invariante bajo isomorfismos, podemos extender esta función a $\mathcal{E}_0(N)(\mathbb{C})$, i.e. tenemos el siguiente diagrama:

$$\begin{array}{ccccc} \mathcal{E}_0(N)(\mathbb{C}) & & & & \\ \downarrow & \searrow & & & \\ S_0(N)(\mathbb{C}) & \longrightarrow & Y_0(N) & \longrightarrow & \mathcal{C}_N(\mathbb{C}) \end{array}$$

Por lo tanto existe una función de $\mathcal{E}_0(N)(\mathbb{C})$ a $Y_0(N)$, tal que su composición con $Y_0(N) \to \mathcal{C}_N(\mathbb{C})$ de (4.3.5), es $(E, C) \mapsto (j(E), j(E/C))$.

En general para $K \subseteq \mathbb{C}$ y para $[E, C] \in S_0(N)(K)$, entonces $j(E) \in K$ por definición de j y por lo tanto la imagen de $S_0(N)(K) \to \mathbb{A}^2_K$ está contenida en los $K-$puntos de $\mathcal{C}_N$, es decir tenemos la función

$$S_0(N)(K) \longrightarrow \mathcal{C}_N(K) \quad \text{definida por} \quad [E, C] \mapsto (j(E), j(E/C)).$$

Cuando $K \supseteq \mathbb{Q}$ es arbitrario obtenemos un resultado más general. Denotamos por $Y_0^{\mathbb{Q}}(N)$ por la subvariedad abierta del modelo $X_0^{\mathbb{Q}}(N)$ de $X_0(N)$ sobre $\mathbb{Q}$, obtenida al quitar las cúspides, i.e. quitar la preimagen de ∞ bajo el morfismo $X_0^{\mathbb{Q}}(N) \longrightarrow X_0^{\mathbb{Q}}(1) \xrightarrow{j} \mathbb{P}^1(\mathbb{Q})$ definido sobre $\mathbb{Q}$. De esta manera ya no podemos describir una función $S_0(N)(K) \to Y_0^{\mathbb{Q}}(N)(K)$ de manera explícita como lo hicimos en el caso $K = \mathbb{C}$, pero sí podemos afirmar lo siguiente:

Teorema 4.3.5. *Sea $K \supseteq \mathbb{Q}$ un campo arbitrario. Entonces existe una función $\psi : \mathcal{E}_0(N)(K) \to Y_0^{\mathbb{Q}}(N)(K)$ tal que la composición con $Y_0^{\mathbb{Q}}(N)(K) \to \mathcal{C}_N(K)$ es $(E, C) \mapsto (j(E), j(E/C))$. Además esta función se factoriza a través de una función suprayectiva $S_0(N)(K) \to Y_0^{\mathbb{Q}}(N)(K)$ que es biyectiva si K es algebraicamente cerrado.*

$$\begin{array}{ccccc} \mathcal{E}_0(N)(K) & & & & \\ \downarrow & \overset{\exists\psi}{\searrow} & & & \\ S_0(N)(K) & \longrightarrow & Y_0^{\mathbb{Q}}(N)(K) & \longrightarrow & \mathcal{C}_N(K) \\ [E, C] & & \longrightarrow & & \big(j(E), j(E/C)\big) \end{array}$$

Esta versión del teorema la citamos de [Mil06] que viene probado en el capítulo 16 de [Mil17a]. La prueba usa el método de descenso de Weil que primero aparece en [Wei56] bajo condiciones más generales para encontrar modelos de curvas sobre subcampos del campo de definición. El lenguaje de Weil lo modernizaron Deligne y Rapaport en [DR73], en particular en §IV.

Para los demás subgrupos de congruencia $\Gamma_1(N)$ y $\Gamma(N)$ tenemos:

Teorema 4.3.6. *Para toda $N \geq 3$, existen curvas afines y lisas $Y_0^{\mathbb{Q}}(N)$, $Y_1^{\mathbb{Q}}(N)$ y $Y^{\mathbb{Q}}(N)$ tales que:*

1. *Si $K \supseteq \mathbb{Q}$, entonces hay una biyección*

$$Y^{\mathbb{Q}}(N)(K) \longrightarrow S(N)(K),$$

y un isomorfismo de superficies de Riemann:

$$Y^{\mathbb{Q}}(N)(\mathbb{C}) \cong \bigcup_{i=1}^{\phi(N)} \mathbb{H}/\Gamma(N)$$

donde la unión es disjunta.

2. *Si $K \supseteq \mathbb{Q}$, entonces hay una biyección*

$$Y_1^{\mathbb{Q}}(N)(K) \longrightarrow S_1(N)(K),$$

y un isomorfismo de superficies de Riemann:

$$Y_1^{\mathbb{Q}}(N)(\mathbb{C}) \cong \mathbb{H}/\Gamma_1(N).$$

3. *Si $K \supseteq \mathbb{Q}$ es algebraicamente cerrado, entonces hay una biyección*

$$Y_0^{\mathbb{Q}}(N)(K) \longrightarrow S_0(N)(K),$$

y un isomorfismo de superficies de Riemann:

$$Y_0^{\mathbb{Q}}(N)(\mathbb{C}) \cong \mathbb{H}/\Gamma_0(N).$$

La prueba de este teorema requiere teoría de esquemas aplicada a espacios moduli de curvas elípticas desarrollada por Deligne y Rapaport en [DR73]. En este caso, el teorema es el el teorema 3.7.1 y los corolarios 4.7.1 y 4.7.2 de [KM85] donde Katz y Mazur recopilan los resultados más importantes de la teoría de espacios moduli de curvas elípticas.

Capítulo 5

Representaciones de Galois

5.1. 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 $G_{L|K} = \mathrm{Gal}(L/K)$) que, con la topología de Krull [Neu99, capítulo IV, §1], es un grupo topológico compacto y Hausdorff, de hecho:

$$G_{\mathbb{Q}} = \varprojlim_{K} \mathrm{Gal}(K/\overline{\mathbb{Q}})$$

donde K corre sobre todas las extensiones de Galois de $\mathbb{Q}$. En particular $G_{\mathbb{Q}}$ es un grupo profinito y admite una base local del $1 \in G_{\mathbb{Q}}$ de subgrupos normales abiertos de la forma $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ (donde $K/\mathbb{Q}$ es finita y de Galois).

Definición 5.1.1. 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 propiedades de las representaciones de grupos finitos como el lema de Schur [Ser77a, 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 $|\cdot|_\lambda$ 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 $\mathrm{GL}_n(A)$ dada 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 la completación de una extensión finita 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 5.1.2. *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 $\rho \cong i \circ \rho'$.*

Demostración. 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 [DS05] 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 contenida 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 5.1.3. 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 5.1.9), la irreducibilidad y la irreducibilidad absoluta coinciden en dimensión 2 y característica 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 6.2.

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 $K/\mathbb{Q}$ 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

$$D_{p,\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Hay un epimorfismo natural $D_{p,\mathfrak{P}} \twoheadrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{P} \mid \mathbb{F}_p)$ definido por $\sigma \mapsto \big(x + \mathfrak{P} \mapsto \sigma(x) + \mathfrak{P}\big)$. El núcleo de este morfismo, denotado por $I_{p,\mathfrak{P}}$, es el *grupo de inercia*. Entonces tenemos el isomorfismo:

$$\frac{D_{p,\mathfrak{P}}}{I_{p,\mathfrak{P}}} \cong \mathrm{Gal}(\mathcal{O}_K/\mathfrak{P} \mid \mathbb{F}_p). \tag{5.1.1}$$

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 definida módulo el grupo de inercia $I_{p,\mathfrak{P}}$.

En el caso de la extensión $\overline{\mathbb{Q}}/\mathbb{Q}$, 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

$$D_{\mathfrak{p}} \cong \varprojlim_{K} D_{\mathfrak{p}\cap\mathcal{O}_K,p}, \qquad (\mathfrak{p} \subset \overline{\mathbb{Z}})$$

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 $\varprojlim D_{\mathfrak{p}\cap\mathcal{O}_K,p}$ 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 núcleo $\mathfrak{p}$.

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 núcleo 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 $I_{\mathfrak{p}\cap\mathcal{O}_K,p}$ donde K corre sobre todas las subextensiones finitas de Galois, i.e.

$$I_{\mathfrak{p}} \cong \varprojlim_{K} I_{\mathfrak{p}\cap\mathcal{O}_K,p} \qquad (\mathfrak{p} \subset \overline{\mathbb{Z}})$$

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. [Neu99, 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:

[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 $\{\mathbb{Z}/m\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}\}_{n|m}$ forma un sistema proyectivo; su límite inverso es $\widehat{\mathbb{Z}}$.

Definición 5.1.4. Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(A)$ una representación de Galois. Entonces ρ es *no-ramificada* 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-ramificada 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 $\rho' : \mathrm{Gal}(K_\rho/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ donde K_ρ es una extensión finita igual al campo fijo 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 ramificada en p.[1]

Ejemplo 5.1.5. 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 asociada a χ. Afirmamos que ρ_χ es no-ramificada 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-ramificada en un primo p. En este caso se 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:

[1] Una extensión $K_\rho/\mathbb{Q}$ es no ramificada en p si la factorización del ideal $p\mathcal{O}_\rho$ del anillo de enteros de K_ρ es un producto lineal de ideales primos distintos.

Definición 5.1.6. 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 definida.

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 n es el entero que cumple $f(\zeta) = \zeta^n$ para alguna raíz 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 5.1.7. *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 $q \nmid N$.*

Demostración. c.f. [KKS11, §5.2 proposición 5.12 y §8.1 teorema 8.7] □

Ahora, si fijamos un número primo ℓ, tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} & & (\mathbb{Z}/\ell^{n+1}\mathbb{Z})^* \\ & \overset{\bar{\chi}_{\ell^{n+1}}}{\nearrow} & \downarrow \text{ mód } \ell^n \\ G_{\mathbb{Q}} & \xrightarrow[\bar{\chi}_{\ell^n}]{} & (\mathbb{Z}/\ell^n\mathbb{Z})^* \end{array}$$

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 5.1.8. *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* $q \neq \ell$.

Demostración. Las propiedades de $\bar{\chi}_{\ell^n}$ de la proposición 5.1.7 se preservan al pasar al límite inverso. □

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 5.1.9. *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.*

Demostración. 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. □

Ahora repasamos las condiciones sobre las representaciones $\bar{\rho}_{E,p}$ y $\rho_{E,\ell}$ análogas a la semiestabilidad de E. Las definiciones precisas y técnicas no se usan en este trabajo, entonces nos referimos a [Tat97] o [Sha86] para los detalles técnicos de la teoría de esquemas de grupos. Realmente lo único que necesitamos es la relación entre la semiestabilidad de curvas elípticas y la semiestabilidad de sus representaciones asociadas (cf. el teorema 5.1.13).

Definición 5.1.10. Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ una representación de Galois módulo ℓ, donde $q = \ell^f$. Entonces:

1. Sea X un esquema sobre $\mathbb{Z}_{(p)}$ finito plano de grupos. Entonces $X(\overline{\mathbb{Q}})$ es un $G_{\mathbb{Q}}-$módulo de modo natural. Si existe X tal que $X(\overline{\mathbb{Q}}) \cong \mathbb{F}_q \times \mathbb{F}_q$ como $G_{\mathbb{Q}}-$módulos (donde $\mathbb{F}_q \times \mathbb{F}_q$ es un $G_{\mathbb{Q}}-$módulo mediante la acción de ρ), entonces decimos que ρ es *buena* en p.

2. ρ es *ordinaria* en p si existen una matriz $Q \in \mathrm{GL}_2(\mathbb{F}_q)$ y una función $f : I_{p,\mathfrak{P}} \to \mathbb{F}_q^*$ tal que

$$Q\rho(\sigma)Q^{-1} = \begin{pmatrix} \chi(\sigma) & f(\sigma) \\ 0 & 1 \end{pmatrix} \qquad (\forall \sigma \in I_{p,\mathfrak{P}})$$

   donde χ es la restricción del caracter $G_{\mathbb{Q}} \xrightarrow{\bar{\chi}_p} \mathbb{F}_p^* \hookrightarrow \mathbb{F}_q^*$ al grupo de inercia.

Definición 5.1.11. Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ una representación de Galois ℓ-ádica. Entonces:

1. ρ es *buena* en p si para cada natural $n > 0$ existe un esquema X_n sobre $\mathbb{Z}_{(p)}$ finito plano de grupos tal que $X(\overline{\mathbb{Q}}) \cong (R/\mathfrak{m}^n) \times (R/\mathfrak{m}^n)$.

2. ρ es *ordinaria* en p si existe una matriz $Q \in \mathrm{GL}_2(R)$ y una función $f : I_{p,\mathfrak{P}} \to R^*$ tal que

$$Q\rho(\sigma)Q^{-1} = \begin{pmatrix} \chi(\sigma) & f(\sigma) \\ 0 & 1 \end{pmatrix} \qquad (\forall \sigma \in I_{p,\mathfrak{P}})$$

   donde χ es la restricción del caracter $G_{\mathbb{Q}} \xrightarrow{\chi_\ell} \mathbb{Z}_\ell^* \to R^*$ al grupo de inercia.

Resumimos estas definiciones con:

Definición 5.1.12. Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$ una representación de Galois (donde A es $\mathbb{F}_q$ o un anillo de coeficientes). Entonces decimos que ρ es *semiestable en p* si ρ es buena u ordinaria en p. En general decimos que ρ es *semiestable* si es no-ramificada casi donde sea y semiestable en los primos donde ramifica.

La importancia de estas definiciones para el estudio de las representaciones de Galois asociadas a curvas elípticas se resume en el siguiente teorema:

Teorema 5.1.13. *Sea E una curva elíptica sobre $\mathbb{Q}$ y $\rho_{E,\ell}$ su representación ℓ-ádica asociada. Entonces:*

1. *E tiene buena reducción módulo $p \iff \rho_{E,\ell}$ es buena en p.*

2. *E es semiestable en $p \iff \rho_{E,\ell}$ es semiestable en p.*

Demostración. Véase la proposición 3.46 de §3.7 de [Sai13a]. □

5.2. 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. Observe 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 [Sil09, §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 2.1.13 de la sección 2.1), entonces $\mathrm{Aut}(E[N])$ es simplemente $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Así definimos:

Definición 5.2.1. 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 5.2.2. *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-ramificada en q y en particular, $\bar{\rho}_{E,p}$ es no-ramificada 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 2.3.1).

Demostración. Véase la proposición 3.15 de §3.3 de [Sai13a]. □

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:

$$\begin{array}{ccccc} & & \mathrm{GL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) & \xrightarrow{\cong} & \mathrm{Aut}(E[\ell^{n+1}]) \\ & \overset{\bar{\rho}_{E,\ell^{n+1}}}{\nearrow} & \downarrow \text{mód } \ell^n & & \vdots \\ G_{\mathbb{Q}} & \xrightarrow[\bar{\rho}_{E,\ell^n}]{} & \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) & \xrightarrow{\cong} & \mathrm{Aut}(E[\ell^n]) \end{array} \tag{5.2.1}$$

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 5.2.3. Sea E una curva elíptica sobre $\mathbb{Q}$, entonces la *representación de Galois ℓ-ádica* asociada a E, es la representación

$$\rho_{E,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \cong \mathrm{Aut}(T_\ell(E))$$

Nota. La representación $\bar{\rho}_{E,\ell}$ asociada a los puntos de $\ell-$torsión de E se puede recuperar de la representación $\ell-$ádica $\rho_{E,\ell}$. Más precisamente, la conmutatividad del diagrama (5.2.1) y la definición del límite inverso nos implican que

$$\begin{array}{ccc} & & \mathrm{GL}_2(\mathbb{Z}_\ell) \\ & \overset{\rho_{E,\ell}}{\nearrow} & \big\downarrow \text{ mód } \ell \\ G_{\mathbb{Q}} & \xrightarrow[\bar{\rho}_{E,\ell}]{} & \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \end{array} \tag{5.2.2}$$

conmuta.

Esta representación cumple casi las mismas propiedades que $\bar{\rho}_{E,p}$. La siguiente proposición sobre $\rho_{E,\ell}$ se obtiene esencialmente aplicando el límite inverso a la proposición 5.2.2.

Proposición 5.2.4. *Sea ℓ un primo fijo y sea E una curva elíptica sobre $\mathbb{Q}$. Entonces*

I) *$\rho_{E,\ell}$ es no-ramificada en q para todo primo distinto de ℓ donde E tenga buena reducción. En particular, $\rho_{E,\ell}$ es no-ramificada 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-ramificada casi donde sea. Entonces, como consecuencia de las proposiciones 5.1.7, 5.1.8, 5.2.2 y 5.2.4, tenemos el siguiente corolario:

Corolario 5.2.5. *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.*

Si juntamos esto con la proposición 5.1.9, tenemos el siguiente resultado

Corolario 5.2.6. *Sea E una curva elíptica sobre $\mathbb{Q}$. Entonces para todo primo $p \geq 3$, tenemos que*

$$\bar{\rho}_{E,p} \text{ es irreducible} \iff \bar{\rho}_{E,p} \text{ es absolutamente irreducible.}$$

Para terminar esta sección enunciamos un teorema importante debido a Serre y algunas consecuencias de este teorema.

Teorema 5.2.7. *(Serre) Sea E una curva elíptica sobre $\mathbb{Q}$, entonces la representación $\bar{\rho}_{E,p}$ asociada a sus puntos de $p-$torsión cumple un de las siguientes dos propiedades:*

1. $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ *es suprayectiva,*

2. $\bar{\rho}_{E,p}$ es reducible.

Demostración. Cuando $p \geq 7$, el teorema se sigue de la proposición 21 (§4.5) de [Ser72] y cuando $p = 3, 5$, la prueba aparece en la proposición 3.1 de [Ser96]. □

Corolario 5.2.8. *Sea $E/\mathbb{Q}$ una curva elíptica. En el caso $p = 3$, tenemos que*

$$\bar{\rho}_{E,3} \text{ es irreducible} \implies \bar{\rho}_{E,3}|_{G_{\mathbb{Q}(\sqrt{-3})}} \text{ es absolutamente irreducible,}$$

En el caso $p = 5$, tenemos que

$$\bar{\rho}_{E,5} \text{ es irreducible} \implies \bar{\rho}_{E,5}|_{G_{\mathbb{Q}(\sqrt{5})}} \text{ es absolutamente irreducible,}$$

5.3. La modularidad de representaciones de Galois

En esta sección estudiamos las representaciones de Galois que surgen de las formas modulares. Gracias al trabajo de Eichler y Shimura, cada forma primitiva de peso 2 tiene asociada una representación de Galois. Para describir este resultado, introducimos un poco de notación.

Como en la sección 3.4, denotamos por $S_2(\Gamma_0(N))$ al espacio de formas cuspidales de peso 2 y nivel N. También denotamos por $S_2^{\text{new}}(\Gamma_0(N))$ al subespacio de formas primitivas (cf. la definición 3.4.15). 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 3.4.17). Denotamos por $\mathcal{O}_f$ al anillo de enteros de K_f.

Todo ideal primo $\lambda \subset \mathcal{O}_f$ tiene asociada una valuación no arquimediana discreta $\nu_\lambda : K_f^* \to \mathbb{Z}$. La completación de K con respecto de esta valuación la denotamos por $K_{f,\lambda}$. Recuerde que ν_λ se extiende de manera única a una valuación no arquimediana de $K_{f,\lambda}$ (denotamos igual por ν_λ) y que, como K_f es un campo numérico, $K_{f,\lambda}$ es una extensión finita de $\mathbb{Q}_\ell$ donde ℓ es el primo que cumple $\ell\mathbb{Z} = \ell \cap \mathbb{Z}$, i.e. $\lambda \mid \ell$.

Teorema 5.3.1. *(Eichler-Shimura) Sea ℓ un número primo. Para toda forma primitiva $f \in S_2^{\text{new}}(\Gamma_0(N))$ y para todo ideal primo $\lambda \subset \mathcal{O}_f$ sobre ℓ, 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-ramificada en q para todo primo $q \nmid N\ell$.*

II) *$\det \rho_{f,\lambda} = \chi_\ell$ el caracter ciclotómico $\ell-$ádico (esta igualdad se justifica en la nota después de la proposición 5.1.8).*

III) *$\mathrm{tr}(\rho_{f,\lambda}(\mathrm{Frob}_q)) = a_q(f)$ para todo primo $q \nmid N\ell$.*

Demostración. Esto es el teorema 9.5.4 en §9.5 de [DS05], o véase §7.6 de [Shi94]. □

Nota. Cuando el contexto no requiere del ideal primo $\lambda \subset \mathcal{O}_f$, vamos a denotar la representación como ρ_f en lugar de $\rho_{f,\lambda}$. Esto es sensato porque λ depende de f.

Este teorema tiene una generalización a otros pesos distintos de 2 (c.f. el teorema 9.6.5 de [DS05]). El teorema anterior para pesos mayores que 2 es debido a Deligne [Del71] y para peso 1 es debido a Deligne y Serre [DS74]. 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 6.2 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 5.3.2. 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 $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ 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 $G_{\mathbb{Q}} \xrightarrow{\rho_{f,\lambda}} \mathrm{GL}_2(K_{f,\lambda}) \hookrightarrow \mathrm{GL}_2(K)$).

Esta definición es difícil de aplicar, entonces queremos una condición suficiente para modularidad que sea más práctica 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 5.3.3. *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:*

$$\rho \text{ es irreducible y } \operatorname{tr}\rho(\mathrm{Frob}_q) = \operatorname{tr}\rho'(\mathrm{Frob}_q) \text{ para casi todo primo } q \quad \Longrightarrow \quad \rho \cong \rho'.$$

Demostración. Esto es la proposición 3.4 de §3,1 en [Sai13b]. □

Corolario 5.3.4. *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.*

Demostración. Por la proposición 5.2.4 y el Teorema 5.3.1, 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 5.1.9 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 5.2.5 y el teorema 5.3.1 respectivamente. Con esto aplicamos la proposición 5.3.3 para concluir que $\rho_{E,\ell} \cong \rho_{f,\ell}$ y que $\rho_{E,\ell}$ es modular. □

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 5.1.2. 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 $f \in S_2^{\text{new}}(\Gamma_0(N))$ 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 $\mathfrak{m}_{f,\lambda} = \lambda\mathcal{O}_{f,\lambda}$, el ideal maximal del anillo local $\mathcal{O}_{f,\lambda}$. El cociente $\mathcal{O}_{f,\lambda}/\mathfrak{m}_{f,\lambda}$ es una extensión finita de $\mathbb{F}_\ell$ y lo denotamos por $k_{f,\lambda}$.

Resumimos estos dos párrafos con el siguiente diagrama conmutativo:

$$\begin{array}{ccccc} & & & & \mathrm{GL}_n(K_{f,\lambda}) \\ & \overset{\rho_{f,\lambda}}{\nearrow} & & & \uparrow \\ G_{\mathbb{Q}} & & \xrightarrow{\rho'} & \mathrm{GL}_n(\mathcal{O}_{f,\lambda}) & \xrightarrow{\mathrm{mod}\,\mathfrak{m}_{f,\lambda}} \mathrm{GL}_n(k_{f,\lambda}). \\ & \underset{\exists\,\bar{\rho}_{f,\lambda}}{\searrow} & & & \end{array} \tag{5.3.1}$$

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 $\bar{\rho}_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k_{f,\lambda})$ donde $k_{f,\lambda}$ es una extensión finita de $\mathbb{F}_\ell$.

Ahora definimos la modularidad de representaciones de Galois sobre $\bar{\mathbb{F}}_\ell$.

Definición 5.3.5. Sea K una extensión finita de un $\mathbb{F}_\ell$. Una representación de Galois $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(K)$ 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 que $\rho \cong \bar{\rho}_{f,\lambda}$ (donde estamos identificando $\bar{\rho}_{f,\lambda}$ con la composición $G_{\mathbb{Q}} \xrightarrow{\bar{\rho}_{f,\lambda}} \mathrm{GL}_2(k_{f,\lambda}) \hookrightarrow \mathrm{GL}_2(K)$).

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 $G_{\mathbb{Q}} \xrightarrow{\rho} \mathrm{GL}_2(F) \hookrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$. Por otro lado, si tenemos una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$, la imagen de ρ es finita 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 contenida 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 viceversa. Por lo tanto, sin pérdida de generalidad podemos cambiar K por $\bar{\mathbb{F}}_\ell$ en la definición anterior.

En el caso de representaciones de Galois asociadas a los puntos de torsión de una curva elíptica, las dos definiciones de modularidad se relacionan de la siguiente manera:

Proposición 5.3.6. *Sea $E/\mathbb{Q}$ una curva elíptica y p un primo fijo. Sean $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_p)$ y $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ sus representaciones de Galois asociadas. Entonces*

$$\rho_{E,p} \text{ es modular} \quad \Longrightarrow \quad \bar{\rho}_{E,p} \text{ es modular.}$$

Demostración. Por definición existe $f \in S_2^{\text{new}}(\Gamma_0(N))$ y un ideal primo $\lambda \subset \mathcal{O}_f$ sobre p tal que $K_{f,\lambda} \hookrightarrow \mathbb{Q}_p$ y $\rho_{E,p} \cong \rho_{f,\lambda}$. Por definición de $K_{f,\lambda}$, necesariamente tenemos que $K_f = \mathbb{Q}$ y $\lambda = p\mathbb{Z}$. Por otro lado, podemos asumir que la imagen de $\rho_{f,\lambda}$ está contenida en $\mathrm{GL}_2(\mathbb{Z}_p)$, entonces existe una matriz $M \in \mathrm{GL}_2(\mathbb{Z}_p)$ tal que

$$\rho_{E,p}(s) = M\rho_{f,\lambda}(s)M^{-1}, \qquad \forall s \in G_{\mathbb{Q}}. \tag{5.3.2}$$

Observe que podemos multiplicar M por una constante sin alterar la igualdad, entonces podemos asumir sin pérdida de generalidad que $\det M \notin p\mathbb{Z}_p$. También podemos asumir sin pérdida de generalidad que la imagen de $\rho_{f,\lambda}$ está contenida en $\mathrm{GL}_2(\mathbb{Z}_p)$.

Si componemos ambos lados de (5.3.2) con el morfismo $\mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ de reducción módulo $\lambda = p\mathbb{Z}$, obtenemos

$$\bar{\rho}_{E,p}(s) = \overline{M}\bar{\rho}_{f,\lambda}\overline{M}^{-1}, \qquad \forall s \in G_{\mathbb{Q}},$$

gracias a los diagramas (5.2.2) y (5.3.1). Como $\overline{M} \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ por construcción, concluimos que $\bar{\rho}_{E,p} \cong \bar{\rho}_{f,\lambda}$ y por lo tanto $\bar{\rho}_{E,p}$ es modular. □

La implicación inversa de esta última proposición, i.e. que la modularidad de $\bar{\rho}_{E,p}$ implica la modularidad de $\rho_{E,p}$, es el paso crucial para la prueba del teorema de modularidad de Wiles.

Como con la definición 5.3.2, la definición de modularidad de representaciones sobre campos finitos no es práctica, pero también tenemos un resultado análogo al corolario 5.3.4 para establecer una condición suficiente para la modularidad de una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$.

Proposición 5.3.7. *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.

Nota. La prueba de la proposición anterior es muy similar a la prueba del corolario 5.3.4 pero se basa en una versión distinta de la proposición 5.3.3. Esa versión viene en la misma proposición de [Sai13a] citada en la prueba y de hecho no requiere la hipótesis sobre la ramificación como lo pide la proposición 5.3.3.

La modularidad de una curva elíptica está codificada en la modularidad de las representaciones ℓ-ádicas asociadas a la curva:

Teorema 5.3.8. *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.*

Demostración. Véase la proposición 3.23 de §3.4 de [Sai13a] □

Este teorema es un paso importante en la prueba de el teorema de modularidad para curvas modulares semiestables porque traduce la modularidad de curvas elípticas a la modularidad de representaciones de Galois.

5.4. Deformaciones de Galois

Recuerde la notación al principio de la sección 5.1: A es un anillo de coeficientes, i.e. $A = (A, \mathfrak{m}, k)$ es un anillo local, completo y noetheriano con ideal maximal $\mathfrak{m}$ y campo residual k finito; denotamos por $\mathcal{O}$ a su anillo de enteros. Como A es completo, el isomorfismo $A \cong \varprojlim A/\mathfrak{m}^N$ induce el isomorfismo $\mathrm{GL}_n(A) \cong \varprojlim \mathrm{GL}_n(A/\mathfrak{m}^N)$ y por lo tanto $\mathrm{GL}_n(A)$ es un grupo profinito. Si $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(A)$ es una representación, podemos asumir que la imagen de ρ está contenida en $\mathrm{GL}_n(\mathcal{O})$ (cf. la proposición 5.1.2).

En la sección pasada vimos cómo la representación $\ell-$ádica $\rho_{E,\ell}$ se reduce módulo ℓ a la representación $\bar{\rho}_{E,\ell}$ sobre los puntos de $\ell-$torsión de una curva elíptica $E/\mathbb{Q}$ (cf. el diagrama 5.2.2). Esto es un ejemplo particular de un fenómeno general:

Definición 5.4.1. Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(A)$ una representación de Galois, entonces la *representación residual de* ρ se define como la composición:

$$\bar{\rho} : G_{\mathbb{Q}} \xrightarrow{\quad\rho\quad} \mathrm{GL}_n(\mathcal{O}) \xrightarrow{\mod \mathfrak{m}} \mathrm{GL}_n(k).$$

Ejemplo 5.4.2. Si $E/\mathbb{Q}$ es una curva elíptica y p es un primo, entonces $\bar{\rho}_{E,p}$ es la representación residual de $\rho_{E,p}$.

Hay una construcción inversa a la representación residual:

Definición 5.4.3. Sea $\rho_0 : G_{\mathbb{Q}} \to \mathrm{GL}_n(k)$ una representación de Galois donde k es un campo finito. Un *levantamiento de* ρ_0 *a* A es una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(A)$ cuya representación residual es ρ_0, es decir que satisface el siguiente diagrama conmutativo:

$$\begin{array}{ccc} & & \mathrm{GL}_n(A) \\ & \overset{\rho}{\nearrow} & \big\downarrow \mod \mathfrak{m} \\ G_{\mathbb{Q}} & \xrightarrow[\rho_0]{} & \mathrm{GL}_n(k) \end{array}$$

Decimos que dos levantamientos ρ y ρ' son *estrictamente equivalentes* si existe una matriz $M \in \mathrm{GL}_n(A)$ tal que $\rho = M\rho' M^{-1}$ donde $M \equiv \mathrm{Id} \mod \mathfrak{m}$. A una clase de equivalencia de levantamientos de ρ_0 módulo equivalencia estricta, la llamamos una *deformación de* ρ_0 *a* A.

Nota. Como es común en la literatura, vamos a referirnos a la deformación $[\rho]$ simplemente por ρ.

Ejemplo 5.4.4. La representación $\rho_{E,p}$ es una deformación de $\bar{\rho}_{E,p}$ y en general, una representación ρ es una deformación de su representación residual $\bar{\rho}$.

En la prueba de modularidad vamos a estar interesados en deformaciones de un tipo específico. Para definir estas deformaciones, fijamos la representación residual $\rho_0 : G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$ donde k es finito de característica p y definimos el conjunto de primos donde ρ_0 se ramifica:

$$S := S_{\rho_0} = \{\ell \text{ primo} \mid \rho_0 \text{ es ramificada en } \ell\}.$$

Entonces definimos una clase de deformaciones importantes para la prueba del teorema de modularidad para curvas elípticas semiestables:

Definición 5.4.5. Sea Σ un conjunto finito de primos (posiblemente vacío[2]) tales que $\Sigma \cap S = \emptyset$. Decimos que una deformación de ρ es de *tipo* $\mathcal{D}_\Sigma$ si ρ cumple las siguientes propiedades:

1. $\det \rho = \chi_p$, donde χ_p es el caracter ciclotómico $p-$ádico (cf. la nota después de la proposición 5.1.8),
2. ρ es no ramificada afuera de $S \cup \Sigma \cup \{p\}$,
3. ρ es semiestable en ℓ para todo primo $\ell \notin \Sigma$,
4. ρ es buena u ordinaria en p (cf. la definición 5.1.11).

En general decimos que ρ es una *deformación admisible* de ρ_0 si ρ es una deformación de tipo $\mathcal{D}_\Sigma$ para algún conjunto finito de primos Σ tal que $\Sigma \cap S = \emptyset$.

Ejemplo 5.4.6. Si $E/\mathbb{Q}$ es una curva elíptica semiestable, entonces $\rho_{E,p}$ es una deformación de $\bar{\rho}_{E,p}$ de tipo $\mathcal{D}_\emptyset$ (cf. corolario 5.2.5, proposición 5.2.4 y el teorema 5.1.13).

Podemos reescribir el problema de encontrar deformaciones en lenguaje categórico. Más precisamente, sea A un anillo de coeficientes fijo con campo residual k y definimos $\mathcal{C}(k)$ como la categoría cuyos objetos son anillos de coeficientes A' con campo residual k y cuyos morfismos son homomorfismos de anillos de coeficientes, i.e. homomorfismos de anillos $f : A' \to A''$ que hacen conmutar el siguiente diagrama:

$$\begin{array}{ccc} A' & \xrightarrow{\quad f \quad} & A'' \\ & {\scriptstyle \bmod \mathfrak{m}'} \searrow \quad \swarrow {\scriptstyle \bmod \mathfrak{m}''} & \\ & k & \end{array}$$

Con esto en mente definimos el siguiente funtor: para una representación $\bar{\rho} : G_\mathbb{Q} \to \mathrm{GL}_n(k)$ y un conjunto finito de primos Σ fijo como en la definición anterior, definimos el funtor $\mathrm{DA}_\Sigma : \mathcal{C}(k) \to$ **Conj** entre la categoría $\mathcal{C}(k)$ y la categoría de conjuntos como:

$$A' \mapsto \mathrm{DA}_\Sigma(A') := \{\rho \mid \rho \text{ es una deformación de } \bar{\rho} \text{ de tipo } \mathcal{D}_\Sigma \text{ a } A'\}.$$

También definimos el funtor de deformaciones *modulares*, i.e. definimos el funtor $\mathrm{DM}_\Sigma : \mathcal{C}(k) \to$ **Conj** como

$$A' \mapsto \mathrm{DM}_\Sigma(A') := \{\rho \in \mathrm{DA}_\Sigma(A') \mid \rho \text{ es modular}\}.$$

El teorema principal de Wiles es:

Teorema 5.4.7. *(Teorema del levantamiento modular semiestable, TLMS) Sea $\rho_0 : G_\mathbb{Q} \to \mathrm{GL}_2(k)$ una representación modular sobre un campo finito k de característica p (véase la definición 5.3.2). Si ρ_0 restringido a*

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}))$$

es absolutamente irreducible, entonces

$$\mathrm{DA}_\Sigma(A) = \mathrm{DM}_\Sigma(A),$$

es decir toda deformación admisible de tipo $\mathcal{D}_\Sigma$ es modular.

[2]El caso $\Sigma = \emptyset$ fue donde Wiles tuvo inicialmente un error cuando presentó la prueba en 1993.

Corolario 5.4.8. *Sea $E/\mathbb{Q}$ una curva elíptica semiestable y $p \in \{3, 5\}$. Entonces si $\bar{\rho}_{E,p}$ es irreducible y modular, entonces $\rho_{E,p}$ es modular.*

Demostración. Por el ejemplo 5.4.6, $\rho_{E,p}$ es una deformación admisible de $\bar{\rho}_{E,p}$. Por el corolario 5.2.8 tenemos que $\bar{\rho}_{E,p}|_{G_L}$ es absolutamente irreducible para ambos valores de p, donde $L = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$. Aplicamos el teorema 5.4.7 a $\bar{\rho}_{E,p}$ para concluir que $\rho_{E,p}$ es modular. □

Para probar este teorema, Wiles reescribe este resultado con la representabilidad de funtores.

Cuando ρ_0 es absolutamente irreducible (que se cumple bajo las hipótesis del TLMS), el funtor $\mathrm{DA}_\Sigma(A)$ es representable por un anillo de coeficientes "universal". Más precisamente:

Teorema 5.4.9. *Si $n \geq 1$ y $\rho_0 : G_\mathbb{Q} \to \mathrm{GL}_n(k)$ una representación absolutamente irreducible, entonces existe un anillo de coeficientes universal $R = R_\Sigma(\rho_0)$ con campo residual k y una deformación universal*

$$\rho^{\mathrm{univ}} : G_\mathbb{Q} \longrightarrow \mathrm{GL}_n(R)$$

de ρ_0 a R que cumple la siguiente propiedad universal: si A es un anillo de coeficientes con campo residual k y $\rho \in \mathrm{DA}_\Sigma(A)$, entonces existe un único homomorfismo $h : R \to A$ (en la categoría $\mathcal{C}(k)$) que hace conmutar el siguiente diagrama:

$$\begin{array}{ccc} G_\mathbb{Q} & \xrightarrow{\rho^{\mathrm{univ}}} & \mathrm{GL}_n(R) \\ & \searrow^{\rho} & \downarrow{\scriptstyle h} \\ & & \mathrm{GL}_n(A) \end{array},$$

es decir que el funtor DA_Σ es representable por el objeto R de $\mathcal{C}(k)$, i.e. $\mathrm{DA}_\Sigma \cong \mathrm{Hom}(R, -)$ con $\rho \mapsto h$.

Lo mismo sucede si cambiamos de funtor a $\mathrm{DM}_\Sigma(A)$, i.e. existe un anillo de coeficientes $T := T_\Sigma(\rho_0)$ y una deformación

$$\rho^{\mathrm{univ.mod.}} : G_\mathbb{Q} \longrightarrow \mathrm{GL}_n(T)$$

que cumple la misma propiedad universal.

Hay varias maneras de probar este resultado. El primero en demostrarlo fue Schlessinger al dar criterios suficientes y necesarios para ver cuándo un funtor contravariante $\mathcal{C}(k) \to \mathbf{Conj}$ (e.g DA_Σ o DM_Σ) es representable (estos criterios aparecen en [Sch68]). También hay una prueba constructiva debida a Lenstra y de Smit que viene explicada detalladamente en [LdS97].

Si sustituimos $A = T$, la propiedad universal de la pareja $(R, \rho^{\mathrm{univ}})$ nos da un morfismo canónico $\varphi := \varphi_\Sigma(\rho_0)$ definido como $\varphi : R \to T$. Entonces el teorema del levantamiento modular semiestable se puede reescribir como:

Teorema 5.4.10. *($R = T$) Con la notación de los teoremas 5.4.7 y 5.4.9 tenemos que el morfismo canónico $\varphi := \varphi_\Sigma(\rho_0)$ definido por $\varphi : R_\Sigma(\rho_0) \to T_\Sigma(\rho_0)$ es un isomorfismo en la categoría $\mathcal{C}(k)$.*

Este es la versión del TLMS que probó Wiles en [Wil95].

Capítulo 6

El teorema de modularidad

6.1. Estrategia de la prueba

En este capítulo probamos el teorema de modularidad para curvas elípticas semiestables con los resultados de los capítulos pasados.

Teorema 6.1.1. *(Teorema de Modularidad Semiestable) Sea $E/\mathbb{Q}$ una curva elíptica semiestable. Entonces E es modular.*

La estrategia general para probar el teorema de modularidad es estudiar la representación $3-$ádica de E. Es decir vamos a probar que $\rho_{E,3}$ es modular con el teorema de levantamiento modular semiestable aplicado a $\bar{\rho}_{E,3}$ una vez que establecemos la modularidad de $\bar{\rho}_{E,3}$ con el Teorema de Langlands Tunnell. Ahora, esta estrategia no siempre funciona para $\bar{\rho}_{E,3}$ cuando éste no es irreducible. En el caso cuando $\bar{\rho}_{E,3}$ no es irreducible, usamos un argumento de Wiles para cambiar el primo 3 por el primo 5 llamado el "truco 3-5". En este caso probamos que $\bar{\rho}_{E,5}$ es irreducible y luego encontramos otra curva elíptica E' con la misma representación módulo 5 que tiene representación $\bar{\rho}_{E',3}$ irreducible; aplicamos el Teorema de Langlands-Tunnell y el teorema de levantamiento modular semiestable para garantizar que $\rho_{E',3}$ es modular. Por último, la construcción de E' nos garantiza que la representación original $\rho_{E,3}$ es modular y por lo tanto E es modular.

Escribimos explícitamente los pasos que vamos a usar: fijamos $E/\mathbb{Q}$ una curva elíptica semiestable.

Teorema 6.1.2. *(Consecuencia de Langlands-Tunnell) Si $\bar{\rho}_{E,3}$ es irreducible, entonces $\bar{\rho}_{E,3}$ es modular.*

Teorema 6.1.3. *(Truco 3-5) Si $\bar{\rho}_{E,3}$ es reducible, entonces $\bar{\rho}_{E,5}$ es irreducible.*

Teorema 6.1.4. *(Familias de curvas módulo 5) Si $\bar{\rho}_{E,5}$ es irreducible, existe una curva elíptica semiestable $E'/\mathbb{Q}$ tal que $\bar{\rho}_{E,5} \cong \bar{\rho}_{E',5}$ y $\bar{\rho}_{E',3}$ es irreducible.*

Teorema 6.1.5. *(Teorema del levantamiento modular semiestable, TLMS) Sea $E/\mathbb{Q}$ una curva elíptica semiestable y $p \in \{3, 5\}$. Entonces si $\bar{\rho}_{E,p}$ es irreducible y modular, entonces $\rho_{E,p}$ es modular.*

Teorema 6.1.6. *(Equivalencia de modularidad) Las siguientes propiedades son equivalentes:*

1. *E es modular (i.e admite un morfismo no constante $X_0(N) \to E$ para alguna N),*

2. *Existe un primo ℓ tal que $\rho_{E,\ell}$ es modular,*

3. *$\rho_{E,\ell}$ es modular para todo primo ℓ.*

Estos últimos dos teoremas ya los vimos en las secciones 5.4 y 5.3 respectivamente (cf. el corolario 5.4.8, respectivamente el teorema 5.3.8). Los primeros tres teoremas los vamos a probar en las siguientes tres secciones.

Por el momento asumimos estos tres resultados y probamos el teorema de modularidad. Como vamos a estar haciendo muchas referencias a teoremas pasados, véase el diagrama de la siguiente página para un resumen esquemático de la prueba.

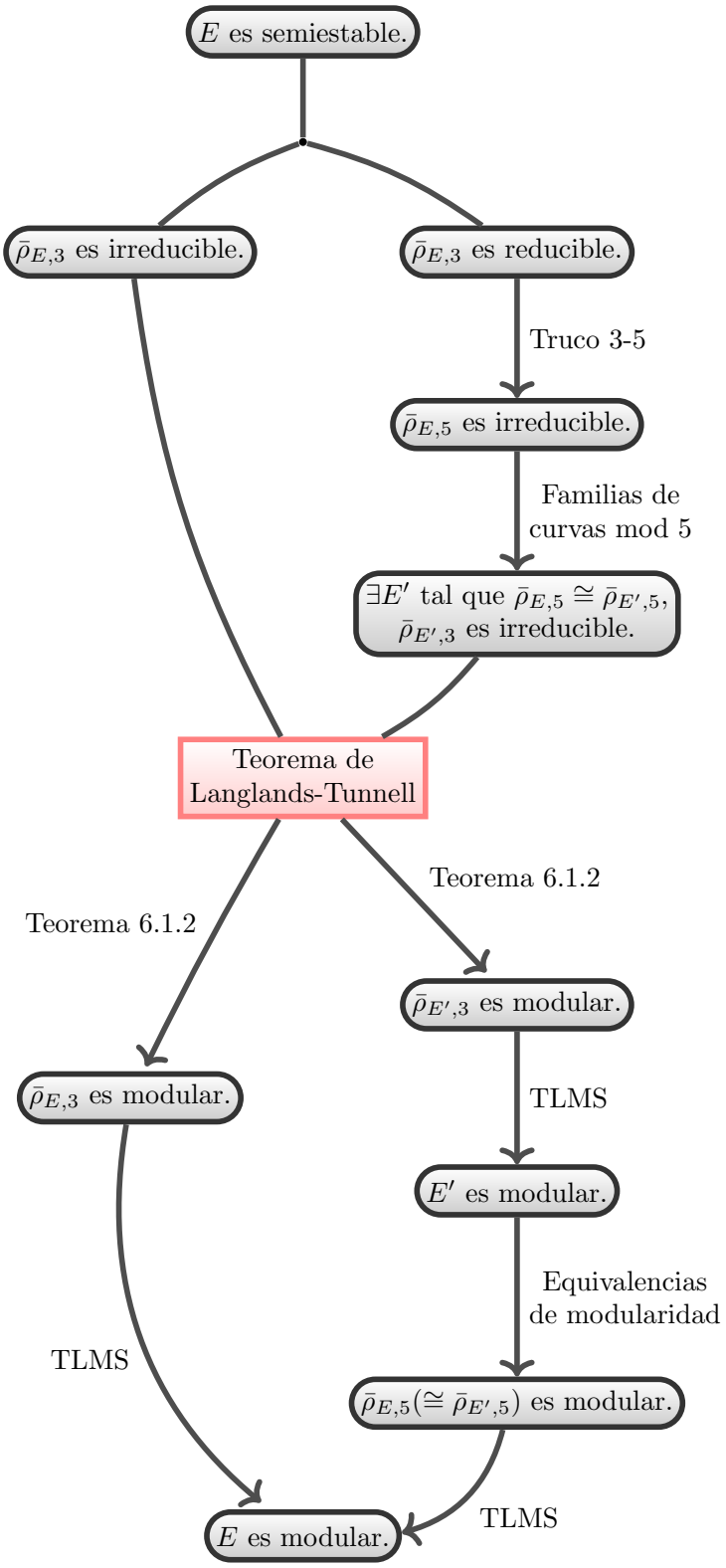
Demostración. (del teorema 6.1.1) Hay dos casos según si $\bar{\rho}_{E,3}$ es irreducible o no:

1. Supongamos que $\bar{\rho}_{E,3}$ es irreducible. Por el teorema 6.1.2 $\bar{\rho}_{E,3}$ es modular. Entonces podemos aplicar el teorema 6.1.5 para deducir que $\rho_{E,3}$ es modular. Por la equivalencia de modularidad (teorema 6.1.6), concluimos que E es modular.

2. Supongamos que $\bar{\rho}_{E,3}$ es reducible. Por el truco 3-5, tenemos que $\bar{\rho}_{E,5}$ es irreducible. Por el teorema 6.1.4, existe una curva $E'/\mathbb{Q}$ tal que $\bar{\rho}_{E,5} \cong \bar{\rho}_{E',5}$ y $\bar{\rho}_{E',3}$ es irreducible. Si aplicamos el teorema 6.1.2 a $\bar{\rho}_{E',3}$ concluimos que $\bar{\rho}_{E',3}$ es modular. Entonces podemos aplicar el teorema 6.1.5 a E' y $\bar{\rho}_{E',3}$ para concluir que E' es modular. Por las equivalencias del teorema 6.1.6 concluimos que $\rho_{E',5}$ es modular lo cual implica que $\bar{\rho}_{E',5}$ es modular (cf. proposición 5.3.6). Como $\bar{\rho}_{E',5} \cong \bar{\rho}_{E,5}$, entonces $\bar{\rho}_{E,5}$ es modular. Como $\bar{\rho}_{E,5}$ es irreducible, aplicamos el teorema 6.1.5, caso $p = 5$, para concluir que E es modular.

□

En vista de la prueba anterior, lo "único" que nos falta ver son los teoremas 6.1.2, 6.1.3 y 6.1.4, i.e. la aplicación del teorema de Langlands, el truco 3-5 y la existencia de familias de curvas módulo 5 respectivamente. Cada una de estos resultados es el enfoque principal de cada uno de las tres secciones siguientes.


E es semiestable.
$\bar{\rho}_{E,3}$ es irreducible.
$\bar{\rho}_{E,3}$ es reducible.
Truco 3-5
$\bar{\rho}_{E,5}$ es irreducible.
Familias de curvas mod 5
$\exists E'$ tal que $\bar{\rho}_{E,5} \cong \bar{\rho}_{E',5}$, $\bar{\rho}_{E',3}$ es irreducible.
Teorema de Langlands-Tunnell
Teorema 6.1.2
Teorema 6.1.2
$\bar{\rho}_{E',3}$ es modular.
$\bar{\rho}_{E,3}$ es modular.
TLMS
E' es modular.
Equivalencias de modularidad
TLMS
$\bar{\rho}_{E,5}(\cong \bar{\rho}_{E',5})$ es modular.
TLMS
E es modular.

6.2. El teorema de Langlands-Tunnell 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 5.2). En esta sección, probamos cómo la modularidad de $\bar{\rho}_{E,3}$ se sigue de un teorema celebrado de Langlands [Lan80] y Tunnell [Tun81]. La versión de su teorema que vamos a usar es:

Teorema 6.2.1. *(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 octaedro), A_4 (las simetrías del tetraedro) y D_{2n} (el grupo diédrico). La prueba en el caso diédrico es debida a los trabajos de Hecke y Maass. El caso tetraédrico es debido a Langlands y el caso octaédrico lo empezó Langlands en [Lan80] y lo terminó Tunnell en [Tun81].

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 [Gel97] para más detalles).

El propósito de esta sección es probar el siguiente teorema:

Teorema 6.2.2. *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 describimos 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 6.2.3) para obtener una genuina eigenforma asociada a $\bar{\rho}_{E,3}$ y así concluir que $\bar{\rho}_{E,3}$ es modular.

Demostración. 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 pueden verificar directamente las siguientes relaciones:

$$A^3 = \mathrm{Id} \quad \text{y} \quad B^8 = \mathrm{Id}.$$

Además, estos exponentes son los enteros positivos mínimos 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 $\langle A\rangle\langle B\rangle = \{A^n B^m \mid 1 \le n \le 3, 1 \le m \le 8\}$ 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 3.2), $\langle A, B\rangle$ tiene 48 elementos. Por lo tanto que A y B efectivamente generan a $\mathrm{GL}_2(\mathbb{F}_3)$.

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 homomorfismo 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:

[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 [Neu99], el caso cuando la extensión es de Galois viene en §1.9.

$$\begin{array}{ccc} \mathrm{GL}_2(\mathbb{F}_3) & \xrightarrow{\Psi} & \mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}]) \\ & \searrow^{\mathrm{Id}} & \downarrow{\scriptstyle \nu} \\ & & \mathrm{GL}_2(\mathbb{F}_3) \end{array} \tag{6.2.1}$$

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

$$\mathrm{tr}\big(\Psi(C)\big) \equiv \mathrm{tr}(C) \pmod{1+\sqrt{-2}}. \tag{6.2.2}$$

Para el determinante de Ψ tenemos la congruencia más fuerte

$$\det\big(\Psi(C)\big) \equiv \det(C) \pmod 3, \tag{6.2.3}$$

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, 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, (6.2.3) 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 5.2.5 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 observemos que

$$\mathrm{PGL}_2(\mathbb{F}_3) := \frac{\mathrm{GL}_2(\mathbb{F}_3)}{\{\mathrm{Id}, -\mathrm{Id}\}} \cong S_4, \tag{6.2.4}$$

donde S_4 es el grupo de permutaciones de un conjunto de cuatro elementos.[2] Con esta identidad 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[3]. 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.[4] 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

$$\rho(s) = \begin{pmatrix} \rho_1(s) & 0 \\ 0 & \rho_2(s) \end{pmatrix} \qquad \forall s \in G_{\mathbb{Q}}.$$

[2]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:

$$[1,0] = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = [a_1, a_3], \qquad [0,1] = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = [a_2, a_4].$$

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 un 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.

[3]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.

[4]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. [Ser77a, §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 5.1.5) 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. [Ser77a, §4.3]).

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 5.1.9 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 tenemos 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 $s_0 \in G_{\mathbb{Q}}$ 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 $g \in S_1^{\mathrm{new}}(\Gamma_0(N), \chi)$ para alguna $N \in \mathbb{N}$ y algún caracter $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$, con serie de Fourier

$$g(z) = \sum_{n=1}^{\infty} a_n(g)e^{2\pi inz},$$

cuyos coeficientes cumplen que, para casi todo primo q,

$$a_q(g) = \mathrm{tr}\big(\rho(\mathrm{Frob}_q)\big). \tag{6.2.5}$$

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 3.4.17). 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 (6.2.2)).

Sea $\mathfrak{P} \subset \mathcal{O}_g$ un ideal primo que contiene al ideal $(1+\sqrt{-2})$. Gracias a (6.2.2), para casi todo primo q tenemos:

$$\begin{aligned} a_q(g) &= \operatorname{tr}\big(\rho(\operatorname{Frob}_q)\big) = \operatorname{tr}\big(\Psi(\bar{\rho}_{E,3}(\operatorname{Frob}_q))\big), \\ &\equiv \operatorname{tr}\big(\bar{\rho}_{E,3}(\operatorname{Frob}_q)\big) \pmod{1+\sqrt{-2}}. \end{aligned}$$

Por lo tanto

$$a_q(g) \equiv \operatorname{tr}\big(\bar{\rho}_{E,3}(\operatorname{Frob}_q)\big) \pmod{\mathfrak{P}}, \tag{6.2.6}$$

porque $(1+\sqrt{-2}) \subseteq \mathfrak{P}$.

A primera vista parece que tenemos las condiciones suficientes de la proposición 5.3.7 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:

$$E_{1,\psi} \in M_1(\Gamma_0(3),\psi) \quad \text{y} \quad a_n(E_{1,\psi}) \equiv \begin{cases} 1 \pmod 3 & n = 0 \\ 0 \pmod 3 & n > 0 \end{cases}. \tag{6.2.7}$$

El hecho que $E_{1,\psi}$ es modular no es trivial (véase el ejercicio 9.6.4 de [DS05]). Otra manera de probar la modularidad de $E_{1,\psi}$ es viendo que $E_{1,\psi}$ es la transformada de Mellin inversa de $\zeta(s)\zeta(s,\psi)$ [Wil95].

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 3.3.6.III). Como $E_{1,\psi} \in M_1(\Gamma_0(3),\psi) \subset M_1(\Gamma_0(3N))$ (cf. el lema 3.4.12) 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 3.4.6) o a nivel de coeficientes de Fourier:

$$a_n(\langle d\rangle f) = \chi(d)\psi(d)a_n(f) \qquad \forall d \in (\mathbb{Z}/3N\mathbb{Z})^*,\ n > 0. \tag{6.2.8}$$

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 (6.2.7):

$$a_n(f) = a_n(g) + \sum_{\substack{i+j=n \\ i,j>0}} a_i(g)a_j(E_{1,\chi}) \equiv a_n(g) \pmod 3 \qquad (\forall n > 1),$$

que también es válida para $n = 1$. Es decir

$$a_n(f) \equiv a_n(g) \pmod 3 \qquad (\forall n > 0). \tag{6.2.9}$$

Si juntamos esta congruencia con (6.2.6), obtenemos que para casi todo primo q se tiene

$$a_q(f) \equiv \operatorname{tr}\big(\bar{\rho}_{E,3}(\mathrm{Frob}_q)\big) \pmod{\mathfrak{P}}. \tag{6.2.10}$$

Otra vez parece que estamos en posición de aplicar la proposición 5.3.7 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 (6.2.9) se reescribe como

$$f \equiv g \pmod{\mathfrak{P}[[e^{2\pi iz}]]}, \tag{6.2.11}$$

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 3.4.11 y la fórmula 6.2.8, los coeficientes de $T_n(f)$ cumplen:

$$\begin{aligned} a_m(T_n f) &= \sum_{d|(m,n)} d\chi(d)\psi(d)a_{nm/d^2}(f) \overset{(6.2.9)}{\equiv} \sum_{d|(m,n)} d\chi(d)\psi(d)a_{nm/d^2}(g) \pmod 3 \\ &\equiv \sum_{d|(m,n)} d^2\chi(d)a_{nm/d^2}(g) \equiv \sum_{d|(m,n)} \chi(d)a_{nm/d^2}(g) \\ \therefore\ a_m(T_n f) &\equiv a_m(T_n g) \pmod 3, \end{aligned}$$

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 (6.2.11), las congruencias anteriores se reescriben como

$$T_n f \equiv T_n g \pmod{\mathfrak{P}[[e^{2\pi iz}]]} \qquad \forall (n, 3N) = 1.$$

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 3.4.16). 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 (6.2.6) que es necesaria para deducir 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 6.2.3. *(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 valuación discreta pero la prueba es fácilmente adaptada para dominios de Dedekind porque localmente son anillos de valuación discreta.

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:

$$a'_{T_n} \equiv a_n(f) \pmod{\mathfrak{P}'}. \tag{6.2.12}$$

Como f' es eigenforma sus valores propios son sus coeficientes de Fourier (cf. el teorema 3.4.16). Además, como $\mathfrak{P} \subset \mathfrak{P}'$, podemos juntar las congruencias (6.2.10) y (6.2.12) para concluir que para casi todo primo q (que además cumple $q \nmid N$) tenemos:

$$a_q(f') = a'_{T_q} \equiv a_q(f) \equiv \operatorname{tr}(\bar{\rho}_{E,3}(\mathrm{Frob}_q)) \pmod{\mathfrak{P}'}.$$

Finalmente tenemos las condiciones suficientes para aplicar la proposición 5.3.7 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 6.2.3. 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[5].

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

$$\varepsilon(T) := a_T + \mathfrak{m} \qquad (\forall\, T \in \mathcal{F})$$

Observe que por construcción $\varepsilon|_{\mathfrak{O}} = \mathrm{Id}_{\mathfrak{O}}$, entonces ε es suprayectivo. 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 [AM94, §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, todos 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 estrictamente 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 $x = 0$)

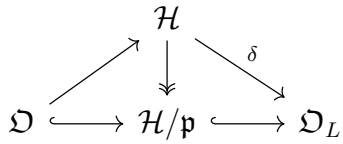
[5]Un $\mathfrak{O}-$módulo $\mathcal{H}$ es plano si el funtor $N \mapsto N \otimes \mathcal{H}$ es exacto izquierdo (recuerde que este funtor siempre es exacto derecho). Gracias a que el producto tensorial y la suma directa conmutan, todo módulo libre es plano.

es distinta 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 [Eis04])

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 [AM94]), 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 [Neu99]). 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

$$\delta(\ker \varepsilon) \subseteq \mathfrak{m}'. \tag{6.2.13}$$

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:

$$\delta(T - a_T \mathrm{Id}_M) = a'_T - a_T \in \mathfrak{m}' \quad \Longrightarrow \quad a'_T \equiv a_T \pmod{\mathfrak{m}'} \tag{6.2.14}$$

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 $T_i T_i' = 0$ para toda $i = 1, \ldots, n$. Además, para cada $1 \otimes T_i \in \mathfrak{P}$ se toma una $f_i \in M$ 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[6] al módulo [Eis04, teorema 3.1, pg 89]. Por lo tanto si denotamos al conjunto de ideales primos asociados a $L \otimes M$ 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 Avoidance" (véase por ejemplo la proposición 1.11 de [AM94]), $\mathfrak{P}$ está contenido en algún $\mathfrak{q} \in \mathcal{A}$. Por lo tanto existe un elemento $f'' \in L \otimes M - \{0\}$ tal que $\mathfrak{q}$ es su anulador, es decir $\mathfrak{P} \subseteq \mathfrak{q} = (f'' : 0)$.

Por último, si $T \in \mathcal{F}$, entonces $(T - a_T')f'' = 0$ o equivalentemente $Thf'' = a_T' f''$; lo mismo sucede si sustituimos f'' por algún múltiplo. En particular, podemos tomar un múltiplo adecuado $f' \in \mathfrak{O}_L \otimes M$ de f'' y obtenemos el vector propio que buscamos. □

6.3. El truco "3-5"

En esta sección estudiamos las propiedades aritméticas de la curva elípitica $X_0(15)$ para probar:

Teorema 6.3.1. *Sea $E/\mathbb{Q}$ una curva elíptica semiestable en 5. Entonces*

$$\bar{\rho}_{E,3} \text{ es reducible} \implies \bar{\rho}_{E,5} \text{ es irreducible.}$$

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 6.2. Si $\bar{\rho}_{E,3}$ no es irreducible, Langlands-Tunnell no se puede aplicar, pero lo que dice el teorema 6.3.1 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 6.3.1. 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, probaremos que E no es semiestable en 5.

El primer paso es probar:

Lema 6.3.2. *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 $G_{\mathbb{Q}}$.*

[6] 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 $\mathfrak{p} = (f : 0) := \{a \in A \mid af = 0\}$.

Demostración. 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 $G_{\mathbb{Q}}$. Recuerde 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 tienen subgrupos cíclicos de orden 15. Vimos en §4.3 que las clases de isomorfismo $[E, C]$ 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 6.3.2) 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 2.1.2 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 órdenes 2 y 3 respectivamente. Por la prueba del teorema 2.1.2, 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 Néron, 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 $N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$ [Lig75]. 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

$$\eta(z) := e^{2\pi i z/24} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z}) = \sum_{n=1}^{\infty} \left(\frac{n}{12}\right) q^{n^2/24}, \tag{6.3.1}$$

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. (6.3.3), 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 [New56] (véase el teorema 1) y el caso $(N, 6) > 1$, e.g. $N = 15$, aparece en la segunda parte [New58]. Ligozat aumentó las condiciones de Newmann para caracterizar cuándo un $\eta-$cociente define una función meromorfa sobre $X_0(15)$. Enunciamos este resultado

Teorema 6.3.3. *(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.

Demostración. Véase la proposición 3.2.1 de [Lig75]. 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 6.3.4. *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*

$$Y^2 + XY + Y = X^3 + X^2 - 10X - 10. \tag{6.3.2}$$

Demostración. 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 (6.3.2) 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 6.3.3 junto con sus series de Fourier que se pueden calcular a partir de (6.3.1):

$$\begin{aligned}
\mathbf{r}_1 &= \{-1,1,5,-5\}, \quad \eta_{\mathbf{r}_1}(z) = q^{-2} + q^{-1} + 2 + 2q + 4q^2 + \cdots \\
\mathbf{r}_2 &= \{7,-1,1,-7\}, \quad \eta_{\mathbf{r}_2}(z) = q^{-4} - 7q^{-3} + 7q^{-2} + 8q^{-1} - 56 + 34q + 51q^2 + \cdots \\
\mathbf{r}_3 &= \{2,4,2,-8\}, \quad \eta_{\mathbf{r}_3}(z) = q^{-4} - 2q^{-3} - q^{-2} - 2q^{-1}9 + 4q - 4q^2 + \cdots
\end{aligned}$$

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:

$$y(z) = q^{-3} + q^{-1} + q^2 + 6q^3 + \cdots$$

Por el teorema 2.1.2, 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 (2.1.4) del teorema 2.1.2 obtenemos la ecuación de Weierstrass buscada:

$$y^2 + xy + y = x^3 + x^2 - 10x - 10.$$

Otra vez por el teorema 2.1.2 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. □

Nota. Lo que hizo Fricke para calcular una ecuación de $X_0(15)$ fue un poco distinto. Él definió el $\eta-$cociente

$$\tau(z) := \frac{\eta(3z)^3\eta(5z)^3}{\eta(z)^3\eta(15z)^3} = q^{-2} + 3 + 9q^2 + O(q^4). \tag{6.3.3}$$

Una vez definida τ, Fricke considera un múltiplo adecuado de la derivada de τ y lo llama σ. De esta manera obtiene el segundo generador de $\mathbb{C}(X_0(15))$ como $\mathbb{C}-$álgebra, es decir $\mathbb{C}(X_0(15)) = \mathbb{C}(\tau, \sigma)$. Después, Fricke calcula y compara coeficientes de Fourier para encontrar la relación algebraica entre τ y σ que resulta ser:

$$\sigma^2 = \tau^4 - 10\tau^3 - 13\tau^2 + 10\tau + 1. \tag{6.3.4}$$

Véase [Fri22, página 439]. Es posible llevar (6.3.4) a una ecuación de Weierstrass mediante el siguiente cambio de variable:

$$\tau = \frac{2y + x + 46}{2(x-8)} + \frac{5}{2}, \quad \sigma = \frac{(2y + x + 46)^2}{4(x-8)^2} - 2(x-8) - \frac{101}{4}, \tag{6.3.5}$$

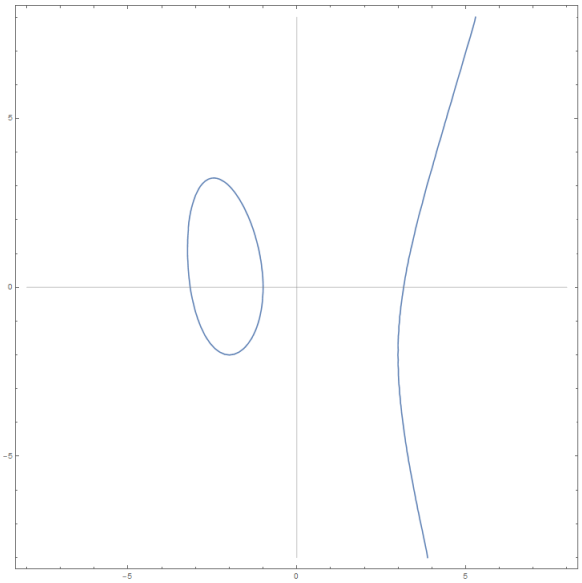


Figura 6.1: La curva real definida por la ecuación $Y^2 + XY + Y = X^3 + X^2 - 10X - 10$.

véase 4.2.5 de [Lig75]. De esta manera obtenemos la ecuación de Weierstrass:

$$y^2 + xy + y = x^3 + x^2 - 10x - 10. \tag{6.3.6}$$

El método de Fricke sirve para calcular ecuaciones de curvas modulares no necesariamente elípticas. Por ejemplo, en $X_0(5)$, Fricke encuentra una función racional τ_5 sobre $X_0(5)$. Usaremos τ_5 más adelante para calcular j como función racional de los $\eta-$cocientes x y y.

Con la ecuación de Weierstrass de $X_0(15)$ podemos calcular sus puntos racionales que denotamos por $G = X_0(15)(\mathbb{Q})$. Por el teorema de Mordell-Weil, tenemos que

$$G \cong G_{\text{tor}} \times \mathbb{Z}^r,$$

donde G_{tor} es el subgrupo de torsión y $r \geq 0$ es el rango de E. 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 (cf. el teorema 2.5.3 de la sección 2.5).

Proposición 6.3.5. *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:*

$$G_{\text{tors}} = \left\{\left(-\tfrac{13}{4}, \tfrac{9}{8}\right), (-1,0), (3,-2), (8,-27), (8,18), (-2,-2), (-2,3)\right\} \cup \{O\}.$$

Demostración. Para aplicar Lutz-Nagell, necesitamos transformar la ecuación de Weierstrass generalizada de $X_0(15)$ dada por el lema 6.3.4 a una ecuación simplificada. El cambio de variable es:

$$x = \frac{x'}{36} - \frac{15}{36}, \qquad y = \frac{y'}{216} - \frac{x'}{72} - \frac{21}{72} \tag{6.3.7}$$

y simplifica la ecuación a

$$y'^2 = x'^3 - 12987x' - 263466 = (x' + 102)(x' + 21)(x' - 123) \tag{6.3.8}$$

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 (6.3.8). Por Lutz-Nagell tenemos que $x_0, y_0 \in \mathbb{Z}$ y el punto P_0 cumple uno de dos casos:

Caso 1: $P_0 + P_0 = O$. En este caso, $P_0 = -P_0$. Por la ecuación (2.1.9), 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 (6.3.8) y obtenemos tres posibles valores para x_0 que corresponden a los siguientes tres puntos racionales de orden 2 en G_{tor}:

$$(-102, 0), \quad (-21, 0) \quad \text{y} \quad (123, 0)$$

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 (6.3.8) 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 (6.3.8):

$$\{(-102, 0), (-21, 0), (123, 0), (303, -4860), (303, 4860), (-57, -540), (-57, 540)\} \cup \{O\}.$$

Bajo el cambio de coordenadas inverso a (6.3.7), 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 nos dice que G_{tor} es isomorfo a una de las siguientes tres posibilidades:

$$\mathbb{Z}/8\mathbb{Z}\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad \text{o} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Para saber cual de estas tres posibilidades es la correcta, necesitamos estudiar el orden de 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 6.2 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

$$G_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. \tag{6.3.9}$$

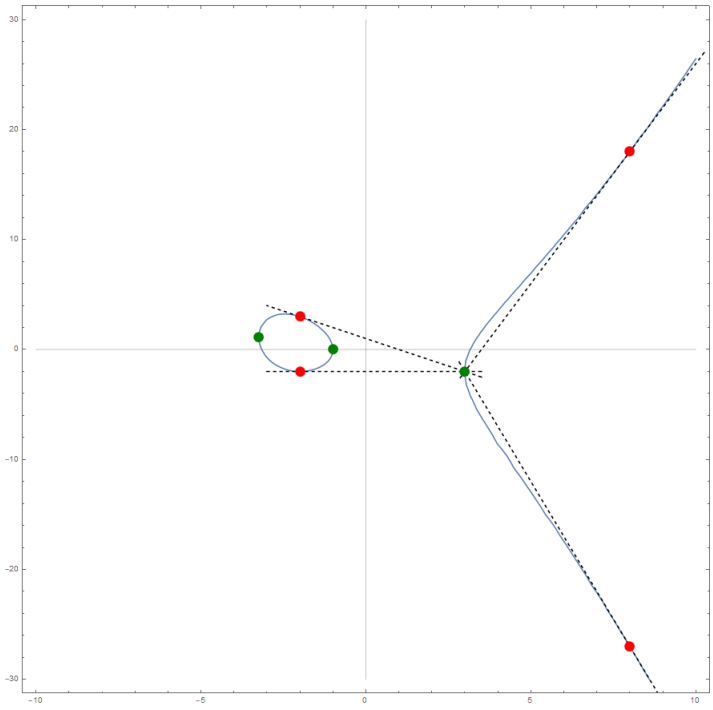


Figura 6.2: Visualización de la duplicación de los puntos racionales de $X_0(15)$. Los puntos verdes son de orden 2 y los puntos rojos son de orden 4.

El próximo paso es probar que el rango de $G \cong \mathbb{Z}^r \times G_{\text{tor}}$ es cero, i.e. $r = 0$. Para esto estudiamos el grupo $G/2G$ para encontrar una fórmula para r. Gracias a (6.3.9) tenemos que

$$\frac{G}{2G} \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^r \times \left(\frac{\mathbb{Z}/2\mathbb{Z}}{2(\mathbb{Z}/2\mathbb{Z})}\right) \times \left(\frac{\mathbb{Z}/4\mathbb{Z}}{2(\mathbb{Z}/4\mathbb{Z})}\right) \quad \Longrightarrow \quad (G : 2G) = 2^{r+2}.$$

Esta fórmula es un caso particular de la fórmula general

$$2^r = \frac{(G : 2G)}{\#\ker[2]}, \tag{6.3.10}$$

donde $[2] : G \to G$ es el homomorfismo de duplicación $P \mapsto P + P$. En efecto, hay tres puntos de orden 2 que junto con el neutro O forman el subgrupo $\ker[2] \subset G$. Esta fórmula se deduce del teorema de estructura de grupos abelianos.[7]

[7] Para un grupo abeliano H finitamente generado tenemos que existen números primos $p_1, \ldots, p_s \in \mathbb{Z}$ y exponentes $n_i > 0$ tales que

$$H \cong \mathbb{Z}^r \times \frac{\mathbb{Z}}{p_1^{n_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_s^{n_s}\mathbb{Z}} \quad \Longrightarrow \quad \frac{H}{2H} \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^r \times \frac{\mathbb{Z}/p_1^{n_1}\mathbb{Z}}{2\mathbb{Z}/p_1^{n_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}/p_s^{n_s}\mathbb{Z}}{2\mathbb{Z}/p_s^{n_s}\mathbb{Z}},$$

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

$$(H : 2H) = 2^{r+\#\{j|p_j=2\}} = 2^r(\#\ker[2]).$$

Para calcular r, necesitamos estudiar con mayor detalle el homomorfismo $[2] : G \to G$. La clave es descomponer $[2]$ 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. Este método se llama $2-$*descenso* (cf. §3 de [ST09] o el capítulo 6 de [Hus04]). Para aplicar este método de manera sencilla, primero consideramos curvas elípticas que tienen al origen del plano afín como un punto 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 también denotamos por

Notación.

$$G = E(\mathbb{Q}).$$

El neutro lo denotamos por O y al origen lo denotamos por $T = (0, 0)$; T es un punto de orden 2. 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 el discriminante $a^2 - 4b$ 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 cuyo órdenes dividen 2, i.e. $\ker[2] = \{O, T, (x_1, 0), (x_2, 0)\}$. Por otro lado, si $a^2 - 4b$ no es un cuadrado perfecto, entonces $(x_1, 0), (x_2, 0) \notin G$ y así solamente hay 2 puntos racionales de orden 2. Resumimos estos dos hechos en la siguiente fórmula:

$$\#\ker[2] = \begin{cases} 4 & a^2 - 4b \text{ es un cuadrado perfecto} \\ 2 & a^2 - 4b \text{ no es un cuadrado perfecto} \end{cases}. \tag{6.3.11}$$

Por lo tanto ya calculamos el término $\#\ker[2]$ de (6.3.10). 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 (6.3.11) 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: $\varphi : E \to \bar{E}$ definida por:

$$\varphi(x, y) := \begin{cases} \left(\frac{y^2}{x^2}, \frac{x^2 - b}{x^2} y\right) & (x, y) \neq O, T \\ \bar{O} & (x, y) = O, T. \end{cases}$$

Si aplicamos φ a $\bar{E}$ obtenemos una función $\bar{E} \to \bar{\bar{E}}$ que junto con el isomorfismo $\bar{\bar{E}} \cong E$, obtenemos la función $\psi : \bar{E} \to E$ definida por

$$\psi(\bar{x}, \bar{y}) := \begin{cases} \left(\frac{\bar{x}^2}{\bar{y}^2}, \frac{\bar{x}^2 - \bar{b}}{\bar{x}^2}\bar{y}\right) & (\bar{x}, \bar{y}) \neq \bar{O}, \bar{T} \\ O & (\bar{x}, \bar{y}) = \bar{O}, \bar{T}. \end{cases}$$

Las funciones φ y ψ son muy útiles para estudiar la isogenia $[2] : E \to E$ ya que cumplen las siguientes propiedades:

Proposición 6.3.6. *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 toda $P \in G$ y $\varphi(\psi(\bar{P})) = [2]\bar{P}$ para toda $\bar{P} \in \bar{G}$. Si abusamos de notación, esto lo podemos denotar por

$$\psi \circ \varphi = [2] = \varphi \circ \psi.$$

(III) $\bar{T} \in \varphi(G)$ (resp. $T \in \psi(\bar{G})$) si y solo si $\bar{b}$ (resp. b) es un cuadrado perfecto.

(IV) 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

$$\bar{P} \in \varphi(G) \ \big(\text{resp. } P \in \psi(\bar{G})\big) \quad \iff \quad \bar{x} \in \mathbb{Q} \ (\text{resp. } x \in \mathbb{Q}) \text{ son cuadrados.}$$

Demostración. Véase la proposición 3.7 de [ST09] para ver que φ y ψ están bien definidas y que cumplen (i) y (ii). Véase §3,5 de [ST09] 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 la fórmula (6.3.10) para el rango se convierte en

$$2^r(\#\ker[2]) \overset{(6.3.10)}{=} (G : 2G) = (G : \psi(\bar{G}))(\psi(\bar{G}) : 2G). \tag{6.3.12}$$

Por otro lado, tenemos que

$$(\psi(\bar{G}) : 2G) = \big(\psi(\bar{G}) : \psi(\varphi(G))\big) \overset{*}{=} \frac{(\bar{G} : \varphi(G))}{(\ker\psi : \varphi(G) \cap \ker\psi)}, \tag{6.3.13}$$

donde el paso (*) se sigue de una propiedad de homomorfismos de grupos abelianos.[8] Por lo tanto si combinamos (6.3.12) y (6.3.13), obtenemos una nueva fórmula para el rango:

$$2^r = \frac{(G : \psi(\bar{G}))(\bar{G} : \varphi(G))}{(\ker\psi : \varphi(G) \cap \ker\psi) \cdot \#\ker[2]}$$

[8] 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 $H = \varphi(G)$.

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 $(\ker\psi : \varphi(G)\cap\ker\psi) = \#\ker\psi = 2$.

Podemos juntar estos dos casos con el inciso (III) de la proposición 6.3.6, 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 (6.3.11) para $\#\ker[2]$ obtenemos $(\ker\psi : \varphi(G)\cap\ker\psi)\cdot\#\ker[2] = 4$ y por lo tanto:

$$2^{r+2} = (G : \psi(\bar{G}))(\bar{G} : \varphi(G)) \tag{6.3.14}$$

y el problema de calcular el rango se reduce a estudiar las imágenes de φ y ψ.

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 6.3.7. *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:

$$2^{2+r} = \#\alpha(G)\cdot\#\bar{\alpha}(\bar{G}).$$

Demostración. 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 2.1 deducimos varias ecuaciones que deben cumplir las coordenadas de P, Q y $P+Q$. En particular la ecuación 2.1.11 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

$$x(P)x(Q)x(P+Q) \equiv 1 \pmod{\mathbb{Q}^{*2}},$$

donde estamos utilizando la notación de congruencia en el contexto multiplicativo. 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 sigue de la definición de α.

Ahora probamos que el núcleo de α es la imagen de ψ. Primero sea $P \in \ker \alpha$. Si $P = O$, trivialmente tenemos que $P \in \psi(\bar{G})$. Si $b \in \mathbb{Q}^{*2}$ entonces puede suceder que $P = T$, pero por el inciso (III), como b es un cuadrado perfecto, entonces $P = T \in \psi(\bar{G})$. Por último si $P \neq O, T$, entonces

$$P \in \ker \alpha \quad \iff \quad x(P) \in \mathbb{Q}^{*2} \quad \overset{*}{\iff} \quad P \in \psi(\bar{G}),$$

donde (*) es exactamente el inciso (IV). 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 (6.3.14) 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

$$\left(\frac{-a \pm d}{2}, 0\right) \in G \quad \Longrightarrow \quad \alpha\left(\frac{-a \pm d}{2}, 0\right) = \frac{-a \pm d}{2}\mathbb{Q}^{*2}. \tag{6.3.15}$$

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 6.3.8. *Sea G el grupo de puntos racionales de una curva elíptica E definida 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:*

$$X^2 = F_\delta(Y, Z), \quad \text{donde por} \quad F_\delta(Y, Z) := \delta Y^4 + aY^2Z^2 + b_0Z^4 \quad (b = \delta b_0)$$

tiene una solución (X_0, Y_0, Z_0), con $Y_0 \neq 0$, y además, cuando $Z_0 \neq 0$:

$$P = \left(\frac{\delta Y_0^2}{Z_0^2}, \frac{\delta X_0 Y_0}{Z_0^3}\right), \qquad \alpha(P) \equiv \delta \pmod{\mathbb{Q}^{*2}}.$$

Si $Z_0 = 0$ tomamos $P = O$ y por lo tanto $\alpha(P) \equiv 1 \pmod{\mathbb{Q}^{*2}}$.

Demostración. 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:

$$\left(\frac{n}{e^3}\right)^2 = \frac{m}{e^2}\left(\frac{m^2}{e^4} + a\frac{m}{e^2} + b\right) \quad \Longrightarrow \quad n^2 = m(m^2 + ame^2 + e^4 b).$$

Por otro lado, sea $\delta = \pm(m, b)$, un máximo común divisor de m y 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:

$$n^2 = \delta m_0(\delta^2 m_0^2 + a\delta m_0 e^2 + e^4 \delta b_0) = \delta^2 m_0(\delta m_0^2 + ae^2 m_0 + e^4 b_0), \tag{6.3.16}$$
$$\therefore \quad \delta^2 \mid n^2 \quad \Longrightarrow \quad \delta \mid n.$$

Con esto, escribimos $n = \delta n_0$ y volvemos a sustituir en la ecuación (6.3.16) para obtener:

$$\delta^2 n_0^2 = \delta^2 m_0(\delta m_0^2 + ae^2 m_0 + e^4 b_0) \quad \Longrightarrow \quad n_0^2 = m_0(\delta m_0^2 + ae^2 m_0 + e^4 b_0). \tag{6.3.17}$$

El siguiente paso es probar que los dos factores del 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:

$$p \mid \delta m_0^2 + ae^2 m_0 + e^4 b_0 \quad \Longrightarrow \quad p \mid e^4 b_0 \quad \overset{p \nmid b_0}{\Longrightarrow} \quad p \mid e^4 \quad \Longrightarrow \quad p \mid e$$
$$\therefore \quad p \mid (m_0, e) \quad \Longrightarrow \quad p \mid (m, e) = 1 \quad \to\leftarrow .$$

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 (6.3.17), 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, (6.3.17) implica que $n_0 = MN$. Si sustituimos estas nuevas expresiones en (6.3.17), 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

$$\alpha(P) = \delta\frac{M^2}{e^2} \equiv \delta \pmod{\mathbb{Q}^{*2}} \quad \Longrightarrow \quad \delta \pmod{\mathbb{Q}^{*2}} \in \alpha(G).$$

□

Observe que la implicación del lema se puede invertir en el siguiente sentido: dado un divisor δ de b, si la ecuación diofantina $X^2 = F_\delta(Y, Z)$ tiene una solución no trivial (X_0, Y_0, Z_0) con $Y_0 \neq 0$, entonces el punto $(\delta Y_0^2 Z_0^{-2}, \delta X_0 Y_0 Z_0^{-3})$ satisface la ecuación $E : y^2 = x^3 + ax^2 + bx$ y por lo tanto es un punto racional de la curva E.

Por lo tanto el lema anterior nos sugiere un algoritmo para calcular la imagen de α: se toman todos los divisores de b y vemos si la ecuación diofantina $X^2 = F_\delta(Y, Z)$ tiene solución; los que tengan solución nos producen elementos en la imagen de la forma $\alpha(\delta Y_0^2 Z_0^{-2}, \delta X_0 Y_0 Z_0^{-3}) \equiv \delta \pmod{\mathbb{Q}^{*2}}$ 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:

$$\begin{aligned}
\delta_2 (dY_0)^4 + a(dY_0)^2 (eZ_0)^2 + \frac{b}{\delta_2}(eZ_0)^4 &= \frac{e^2}{d^2}\delta_1 (dY_0)^4 + a(dY_0)^2 (eZ_0)^2 + \frac{bd^2}{\delta_1 e^2}(eZ_0)^4 \\
&= e^2 d^2 (\delta Y_0^4 + a Y_0^2 Z_0^2 + b_0 Z_0^4) \\
&= e^2 d^2 X_0^2,
\end{aligned}$$

$$\therefore \quad (deX_0)^2 = F_{\delta_2}(dY_0, eZ_0).$$

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 $X^2 = F_\delta(Y, Z)$ para solamente un divisor δ por cada clase de equivalencia. De esta manera tenemos el siguiente algoritmo para calcular la imagen de α:

Algoritmo 6.3.9. 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. Se parte $\mathfrak{D}$ en clases de equivalencia módulo $\mathbb{Q}^{*2}$ y se toma un sistema completo de residuos $\mathfrak{D}' = \{\delta_1, \ldots, \delta_n\}$ módulo $\mathbb{Q}^{*2}$.

2. Se toma un divisor $\delta_i \in \mathfrak{D}'$. Se determina si la ecuación diofantina $X^2 = \delta_i Y^4 + a Y^2 Z^2 + b_i Z^4$ (donde $b = \delta_i b_i$) tiene una solución (X_i, Y_i, Z_i) con $Y_i \neq 0$. Si existe una solución, entonces $\delta \pmod{\mathbb{Q}^{*2}} \in \alpha(G)$ y se cambia de divisor. Si no tiene solución, se cambia de divisor. Se repite hasta terminar los divisores en $\mathfrak{D}'$.

3. La lista de divisores módulo $\mathbb{Q}^{*2}$, que inducen ecuaciones diofantinas con soluciones, es la imagen de α.

Nota. A pesar de que las hipótesis del lema 6.3.8 piden que las coordenadas del punto $P = (x, y)$ sean distintas de cero, el algoritmo alcanza a incluir el caso cuando $y = 0$. En este caso, como $P \in G$, $\bar{b} = a^2 - 4b$ es un cuadrado perfecto, i.e. $\bar{b} = d^2$ para alguna $d \in \mathbb{Z}$, vimos que $\frac{-a \pm d}{2}\mathbb{Q}^{*2}$

son dos elementos de la imagen de α (cf. la ecuación (6.3.15)), pero el algoritmo anterior ya nos produce estos dos elementos. En efecto, b admite la factorización

$$b = \frac{-a+d}{2}\frac{-a-d}{2}.$$

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 6.3.10. *El rango de la curva modular elíptica $X_0(15)$ es 0, por lo tanto, si $G = X_0(15)(\mathbb{Q})$ es su grupo de puntos racionales, entonces $G = G_{\text{tor}}$ y $\#G = 8$.*

Demostración. 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, como el rango es invariante bajo isogenias (cf. la segunda nota después del teorema 2.1.8), vamos a cambiar $X_0(15)$ por una curva isógena que tenga coeficientes más pequeños: $y^2 = x^3 - 27x + 8694$.[9] Con el cambio de variable $(x, y) \to (9x - 21, 27y)$, obtenemos una ecuación de Weierstrass de la forma adecuada para aplicar el algoritmo 6.3.9:

$$E \ : \ y^2 = x^3 - 7x^2 + 16x.$$

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 $\bar{b} = -15$. Primero aplicamos el algoritmo a E:

1. 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.

$$\mathfrak{D}' = \{-2, -1, 1, 2\}.$$

2. 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 $\delta < 0$, en efecto, si $\delta < 0$, todos los coeficientes de $F_\delta(Y, Z)$ son negativos 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

$$(1, 1, 0) \text{ es una solución de } \quad X^2 = Y^4 - 7Y^2Z^2 + 16Z^4.$$

[9] Esta ecuación aparece en las tablas de Cremona [Cre97] en la clase de isogenia de curvas de conductor 15 porque $X_0(15)$ tiene conductor 15 (cf. el ejemplo 2.5.13).

Por lo tanto $1 \pmod{\mathbb{Q}^{*2}} \in \alpha(G)$, pero esto ya lo sabíamos porque $\alpha(O) = 1$ mód $\mathbb{Q}^{*2}$. 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:

$$X_0^2 \equiv 2Y_0^4 + Y_0^2Z_0^2 \equiv Y_0^2(2Y_0^2 + Z_0^2) \pmod 4. \tag{6.3.18}$$

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:

$$Y_0^2 \equiv 1 \pmod 4 \quad \Longrightarrow \quad X_0^2 \equiv 2+Z_0^2 \equiv \begin{cases} 2 \pmod 4 & Z_0^2 \equiv 0 \pmod 4 \\ -1 \pmod 4 & Z_0^2 \equiv 1 \pmod 4 \end{cases} \quad \to\leftarrow . \tag{6.3.19}$$

Por lo tanto necesariamente tenemos $Y_0^2 \equiv 0 \pmod 4$ o equivalentemente $2 \mid Y_0$. Esto, junto con la congruencia (6.3.18), 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:

$$4x_0^2 = 32y_0^4 - 28y_0^2Z_0^2 + 8Z_0^4 = 4(8y_0^4 - 7y_0^2Z_0^2 + 2Z_0^4) \quad \Longrightarrow \quad x_0^2 = 8y_0^4 - 7y_0^2Z_0^2 + 2Z_0^4. \tag{6.3.20}$$

Módulo 4 la ecuación se vuelve

$$x_0^2 \equiv Z_0^2(y_0^2 + 2Z_0^2) \pmod 4.$$

Si $Z_0^2 \equiv 1 \pmod 4$ obtenemos la misma contradicción que en (6.3.19), 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 (6.3.20) 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 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.

3. Por el paso anterior el único divisor cuya ecuación diofantina asociada tenía solución era $\delta = 1$. Por lo tanto
$$\alpha(G) = \{1 \pmod{\mathbb{Q}^{*2}}\} \quad \Longrightarrow \quad \#\alpha(G) = 1 \tag{6.3.21}$$

Ahora aplicamos el algoritmo a $\bar{E}$:

1. 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
$$\bar{\mathfrak{D}}' = \mathfrak{D} = \{-15, -5, -3, -1, 1, 3, 5, 15\}.$$

2. 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

$$F_{\bar{\delta}}(Y, Z) = \bar{\delta}Y^4 + 14Y^2Z^2 - \frac{15}{\bar{\delta}}Z^4.$$

Al tanteo, uno puede encontrar soluciones pequeñas a varias ecuaciones diofantinas. Por ejemplo:

$$\begin{array}{l}(0,1,1) \text{ es una solución de } \quad X^2 = Y^4 + 14Y^2Z^2 - 15Z^4 \text{ y } X^2 = -15Y^4 + 14Y^2Z^2 + 1Z^4, \\ (4,1,1) \text{ es una solución de } \quad X^2 = 5Y^4 + 14Y^2Z^2 - 3Z^4 \text{ y } X^2 = -3Y^4 + 14Y^2Z^2 + 5Z^4.\end{array}$$

Entonces las ecuaciones asociadas a $\bar{\delta} = -15, -3, 1, 5$ tienen soluciones. Por lo tanto:

$$\{-15 \pmod{\mathbb{Q}^{*2}}, -3 \pmod{\mathbb{Q}^{*2}}, 1 \pmod{\mathbb{Q}^{*2}}, 5 \pmod{\mathbb{Q}^{*2}}\} \subseteq \bar{\alpha}(\bar{G}). \tag{6.3.22}$$

El resto de las ecuaciones no tienen soluciones gracias al método de descenso infinito. 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 infinito".

3. Los únicos divisores que inducen ecuaciones diofantinas con soluciones son $\bar{\delta} = -15, -3, 1, 5$, es decir la contención de (6.3.22) es una igualdad:

$$\#\bar{\alpha}(\bar{G}) = 4. \tag{6.3.23}$$

Para terminar juntamos nuestras fórmulas para las imágenes de α, (es decir (6.3.21) y (6.3.23)), y sustituimos en la fórmula del rango de E del lema 6.3.8 para concluir que:

$$2^{2+r} = 4 \quad \Longrightarrow \quad r = 0.$$

□

Como el rango de $X_0(15)(\mathbb{Q})$ es cero, entonces concluimos que tiene 8 elementos. En la sección 3.2 vimos que $\Gamma_0(15)$ tiene las cuatro cúspides $0, \frac{1}{3}, \frac{1}{5}, \infty$ (cf. el ejemplo 3.2.7) que corresponden a puntos racionales sobre $X_0(15)$ y por lo tanto $Y_0(15)(\mathbb{Q}) = X_0(15)(\mathbb{Q}) - \{\text{cúspides}\}$ tiene cuatro puntos racionales no cuspidales.

Sea $X_0^{\mathbb{Q}}(15)$ un modelo de $X_0(15)$ sobre $\mathbb{Q}$ y sea $\mathcal{C}_{15}/\mathbb{Q}$ el modelo afín de $X_0(15)$ construido en la sección 4.2; ambas variedades tienen a $\mathbb{Q}(j, j_{15})$ como campo de funciones racionales. Sea $Y_0^{\mathbb{Q}}(15)$ la subvariedad abierta de $X_0^{\mathbb{Q}}(15)$ que corresponde a $Y_0(15)(\mathbb{Q}) \subset X_0(15)(\mathbb{Q})$.

Gracias al teorema 4.3.5 existe una función suprayectiva de $S_0(15)(\mathbb{Q}) \to Y_0^{\mathbb{Q}}(15)(\mathbb{Q})$ cuya composición con $Y_0^{\mathbb{Q}}(15)(\mathbb{Q}) \to \mathcal{C}_{15}(\mathbb{Q})$ es $[E, C] \mapsto (j(E), j(E/C))$. Como $Y_0^{\mathbb{Q}}(15)(\mathbb{Q})$ tiene cuatro puntos, a los más hay cuatro posibles valores de $j(E)$ para toda $[E, C] \in S_0(15)(\mathbb{Q})$. En seguida calculamos estos posibles valores.

Proposición 6.3.11. *Sea $E/\mathbb{Q}$ una curva elíptica con un subgrupo cíclico de orden N que sea G_K-estable. Entonces $j(E)$ solamente puede tomar uno de cuatro posibles valores racionales:*

$$j(E) \in \{-2^{-1}5^2, -2^{-3}5^2241^3, -2^{-5}5^129^3, 2^{-15}5^1211^3\}.$$

Demostración. Supongamos que $E/\mathbb{Q}$ tiene un subgrupo cíclico $C \subseteq E(\overline{\mathbb{Q}})$ de orden N y $G_{\mathbb{Q}}-$estable. Por definición, esto implica que $[E, C] \in S_0(15)(\mathbb{Q})$ (cf. la sección 4.3). Por el teorema 4.3.5, tenemos que existe una función suprayectiva $S_0(15)(\mathbb{Q}) \to Y_0^{\mathbb{Q}}(15)$ donde $Y_0^{\mathbb{Q}}(15)$ es la subvariedad abierta del modelo racional $X_0^{\mathbb{Q}}(15)$ menos sus puntos cuspidales. La composición con la función $Y_0^{\mathbb{Q}}(15)(\mathbb{Q}) \to \mathcal{C}_{15}(\mathbb{Q})$ nos da la función $[E, C] \mapsto (j(E), j(E/C))$ donde $\mathcal{C}_{15}$ es la curva afín definida por los ceros del polinomio modular Φ_{15} de la sección 4.2.

Cada punto racional (x, y) de $Y_0(15)$ con coordenadas dadas por la ecuación de Weierstrass $y^2 + xy + y = x^3 + x^2 - 10x - 10$ (que calculamos en las proposiciones 6.3.5 y 6.3.10) corresponde a un punto racional $(j(E), j_{15}(E)) \in \mathcal{C}_{15}$. Como $\mathbb{C}(X_0(15)) = \mathbb{C}(x, y)$ donde x y y son los $\eta-$cocientes de la proposición 6.3.4, y como $\mathbb{C}(\mathcal{C}_{15}) = \mathbb{C}(j, j_{15})$ por construcción, se tiene $\mathbb{C}(x, y) = \mathbb{C}(j, j_N)$. Por lo tanto j es una función racional en x y y. Para calcular esta relación uno tiene que comparar la serie de Fourier de j y la serie de Fourier de una expresión racional arbitraria en x y y. Para facilitar la exposición, usamos el truco de Fricke.

Más precisamente usamos el cambio de variable 6.3.5 para convertir un punto racional $P = (x, y)$ con coordenadas de Weierstrass en un punto racional $P' = (\tau, \sigma)$ que satisface la ecuación $\sigma^2 = \tau^4 - 10\tau^3 - 13\tau^2 + 10\tau + 1$. Para hacer recordemos la primera coordenada τ_5 de la ecuación de Fricke para $X_0(5)$, cf. la nota después de la prueba del lema 6.3.4. Una vez en las coordenadas (τ, σ) usamos dos fórmulas de Fricke:

$$\tau_5 = \frac{\tau^4 - 9\tau^3 - 9\tau - 1 - \sigma(\tau^2 - 4\tau - 1)}{2\tau}, \tag{6.3.24}$$

$$j = \frac{(\tau_5^2 + 10\tau_5 + 5)^3}{\tau_5}, \tag{6.3.25}$$

que son respectivamente las fórmulas (9), p. 440, y (13), p. 393 de [Fri22]. Si combinamos ambas fórmulas obtenemos una expresión racional para j en términos de τ y σ. Si hacemos este cálculo para todos los puntos racionales de $X_0(15)$ obtenemos:

1. Para $(x, y) = (-13/4, 9/8)$, $j = 2^{-15}5^1211^3$,
2. Para $(x, y) = (-1, 0)$, $j = \infty$,
3. Para $(x, y) = (3, -2,)$, $j = -2^{-5}5^129^3$,
4. Para $(x, y) = (8, -27)$, $j = \infty$,
5. Para $(x, y) = (8, 18)$, $j = \infty$,
6. Para $(x, y) = (-2, -2)$, $j = -2^{-1}5^2$,
7. Para $(x, y) = (-2, 3)$, $j = \infty$,
8. Para el punto al infinito O tenemos que $j = -2^{-3}5^2241^3$.

Las cuatro veces que $j = \infty$ corresponden a las cuatro cúspides de $X_0(15)$.

Por lo tanto los cuatro puntos racionales no cuspidales $(-2,-2), O, (3,-2)$ y $(-13/4, 9/8)$ de $X_0(15)$ corresponden a los cuatro puntos

$$(-2^{-1}5^2, ...),\ (-2^{-3}5^2241^3, ...),\ (-2^{-5}5^129^3, ...) \text{ y } (2^{-15}5^1211^3, ...)$$

en el modelo $\mathcal{C}_{15}$ de $X_0(15)$ sobre $\mathbb{Q}$. □

Nota. Para cada $j \in \{-2^{-1}5^2, -2^{-3}5^2241^3, -2^{-5}5^129^3, 2^{-15}5^1211^3\}$, construimos la curva E_j definida por:

$$E_j\ :\ y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}.$$

Por construcción $j(E_j) = j$. Ahora llevamos la ecuación de E_j a la versión simplificada donde los cambios de variable admisibles son de la forma $x = u^2x'$ y $y = u^3y'$. Buscamos una $u \in \overline{\mathbb{Q}}$ adecuada para hacer el cambio de variable para simplificar los coeficientes. En seguida describimos este proceso para $j = -25/2$:

$$\begin{aligned} y^2 + xy = x^3 + \frac{72}{3481}x + \frac{2}{3481} \quad &\longrightarrow \quad y^2 = x^3 - \frac{3^35^2}{59^2}x + \frac{2^13^35^2}{59^2} \\ &\longrightarrow \quad y^2 = x^3 - 675x - 79650 \quad (u = 1/\sqrt{-59}). \end{aligned} \tag{6.3.26}$$

Definimos E_1 como la curva dada por la ecuación (6.3.26). Similarmente podemos construir curvas elípticas $E_2, E_3, E_4/\mathbb{Q}$ tales que $j(E_i)$ es el $i-$ésimo valor del conjunto

$$\{-2^{-1}5^2, -2^{-3}5^2241^3, -2^{-5}5^129^3, 2^{-15}5^1211^3\}.$$

En estos casos, solamente mencionamos que los parámetros u_i que se usan en el cambio de variable para simplificar $E_{j(E_i)}$ son, en orden:

$$u_i \in \left\{ \frac{1}{\sqrt{-59}}, \sqrt{-\frac{241}{18707}}, \sqrt{-\frac{29}{2105}}, \sqrt{-\frac{211}{15535}} \right\}.$$

Por lo tanto el cambio de variable que lleva $E_{j(E_i)}$ en E_i está definida sobre $\mathbb{Q}(u_i)$ y en particular $E_{j(E_i)}$ es isomorfa a una E_i sobre una extensión cuadrática de $\mathbb{Q}$.

Estamos en posición de probar el teorema principal de esta sección:

Teorema 6.3.12. *Sea $E/\mathbb{Q}$ una curva elíptica semiestable en 5. Entonces*

$$\bar{\rho}_{E,3} \text{ es reducible} \quad \Longrightarrow \quad \bar{\rho}_{E,5} \text{ es irreducible.}$$

Demostración. Sea $E/\mathbb{Q}$ una curva elíptica semiestable en 5. Sea $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ una ecuación de Weierstrass minimal global (cuya existencia se sigue de la proposición 2.5.5) con discriminante Δ. Supongamos que $\bar{\rho}_{E,3}$ es reducible y por contradicción, supongamos que $\bar{\rho}_{E,5}$ también es reducible. Por el lema 6.3.2, $E(\overline{\mathbb{Q}})$ contiene un subgrupo C cíclico de orden 15 estable bajo la acción de $G_{\mathbb{Q}}$.

Por lo tanto $[E, C] \in S_0(15)(\mathbb{Q})$ y por la proposición 6.3.11, $j(E)$ toma uno de cuatro posibles valores racionales. Aquí solamente consideramos el primer caso $j(E) = -25/2 = j(E_1)$. Por el corolario 2.1.7, tenemos que

$$E \cong E_1 \text{ sobre } K := \mathbb{Q}(\sqrt{59c_6}) \text{ bajo el cambio de variable } \begin{matrix} x \mapsto u^2 x, \\ y \mapsto u^3 y, \end{matrix} \quad \left(u = \frac{c_4\sqrt{59}}{5\sqrt{c_6}}\right)$$

porque $c_6(E_1) = 5^2 \cdot 59$.

Por otro lado consideramos a E_1 definida sobre $\mathbb{Q}_5$. El discriminante de la ecuación de Weierstrass simplificada de E_1 es $\Delta_1 = -2^{13}3^{12}5^4$. Bajo el cambio de variable $x = 36x' + 3$, $y = 216y' - 108x - 108$ la ecuación de Weierstrass se convierte en:

$$y^2 + xy + y = x^3 - x - 2, \tag{6.3.27}$$

con discriminante $\Delta_1 = -2 \cdot 5^4$. Observe que la ecuación es minimal (sobre $\mathbb{Q}_5$) ya que $\nu_5(\Delta_1) < 12$, donde ν_5 es la valuación $5-$ádica de $\mathbb{Q}_5$ (cf. el ejemplo 2.4.2). De hecho, la ecuación se mantiene minimal sobre cualquier extensión finita de $\mathbb{Q}_5$ porque si L es una extensión finita de $\mathbb{Q}_5$ con valuación $\hat{\nu}$ que extiende la valuación $5-$ádica de $\mathbb{Q}_5$, entonces $\hat{\nu}(\Delta_1) = \nu_5(\Delta_1) = 4$ porque $\Delta \in \mathbb{Z} \subset \mathbb{Q}_5$.

Ahora consideremos la extensión cuadrática $K_5 := \mathbb{Q}_5(\sqrt{59c_6})$ de $\mathbb{Q}_5$ donde $\hat{\nu}_5$ es la extensión a K_5 de ν_5. Por hipótesis tenemos que $E/\mathbb{Q}$ es semiestable en 5, i.e. $E/\mathbb{Q}_5$ es semiestable, entonces por el teorema 2.4.6 tenemos que E/K_5 es semiestable en 5. De esta manera $\hat{\nu}_5(\Delta) = 0$ ó $\hat{\nu}_5(\Delta) > 0$ y $\hat{\nu}_5(c_4) = 0$. Con el valor $\hat{\nu}_5(\Delta_1) = \nu_5(-2 \cdot 5^4) = 4$ y las fórmulas de cambio de variable podemos calcular:

$$\begin{aligned} \hat{\nu}_5(\Delta) &= \hat{\nu}_5(\Delta_1 u^{12}) = \hat{\nu}_5(\Delta_1) + 6\hat{\nu}_5(u^2) = 4 + 6\hat{\nu}_5(59c_4^2/25c_6) \\ &= 4 + 6\Big(0 + 2\nu_5(c_4) - 2 - \nu_5(c_6)\Big) = 12\nu_5(c_4) - 6\nu_5(c_6) - 8. \end{aligned} \tag{6.3.28}$$

Observe que si $\hat{\nu}_5(\Delta) = 0$, la fórmula anterior se reduce a $8 = 6(2\nu_5(c_4) - \nu_5(c_6))$ lo cual implica que $6 \mid 8$ porque $\nu_5(c_4), \nu_5(c_6) \in \mathbb{Z}$. Esto es una contradicción y por lo tanto $\hat{\nu}_5(\Delta) > 0$ y $\hat{\nu}_5(c_5) = \nu_5(c_4) = 0$. Sin embargo, estas dos condiciones no pueden suceder simultáneamente con la fórmula (6.3.28). En efecto, si $\nu_5(c_4) = 0$, entonces el lado derecho de (6.3.28) es negativo lo cual contradice que $\hat{\nu}_5(\Delta) > 0$. Por lo tanto concluimos que $\hat{\nu}_5(\Delta) > 0$ y $\hat{\nu}_5(c_4) > 0$, i.e. que E/K_5 tiene reducción aditiva lo cual contradice que E/K_5 es semiestable. Esta contradicción surge de que $\bar{\rho}_{E,5}$ es reducible y por lo tanto terminamos la prueba. □

6.4. Familias de curvas elípticas módulo 5

El propósito de esta sección es probar el siguiente paso crucial en la prueba del teorema de modularidad para curvas semiestables:

Teorema 6.4.1. *Sea $E/\mathbb{Q}$ una curva elíptica semiestable. Si $\bar{\rho}_{E,5}$ es irreducible, entonces existe una curva elíptica $E'/\mathbb{Q}$ semiestable tal que $\bar{\rho}_{E,5} \cong \bar{\rho}_{E',5}$ y $\bar{\rho}_{E',3}$ es irreducible.*

La prueba se divide en tres pasos. El primer paso es realizar a E como una fibra de una superficie elíptica sobre una curva definida sobre $\mathbb{Q}$ y gracias a esta construcción, las demás fibras

(salvo una cantidad finita) corresponden a curvas elípticas cuyas representaciones en los puntos de 5−torsión son isomorfas. El segundo paso es encontrar una fibra, i.e. curva elíptica E', tal que $\bar{\rho}_{E',3}$ sea irreducible. El tercer paso es ver que la semiestabilidad de E se transfiere a E' mediante el isomorfismo $\bar{\rho}_{E,5} \cong \bar{\rho}_{E',5}$.

El primer paso es esencialmente debido a Rubin y Silverberg y aparece de manera completa en [RS97]. Aquí seguiremos esta exposición solamente en el caso $p = 5$ que es el que nos interesa por el momento. El segundo paso, y mucho de esta sección en general, viene en [Rub97]. El tercer paso es esencialmente una proposición que aparece en [Sil97] que se basa en resultados preliminares del trabajo de Grothendieck sobre modelos de Néron en [Gro72].

En seguida enunciamos cada paso como una proposición junto con algunas observaciones (proposiciones 6.4.2, 6.4.3 y 6.4.4 respectivamente). Después probamos el teorema principal usando las tres proposiciones. Cerramos la sección con las pruebas de cada paso.

Las proposiciones son:

Proposición 6.4.2. *Sea $E/\mathbb{Q}$ una curva elíptica con invariante $j = j(E)$. Entonces existen dos polinomios $a(t), b(t) \in \mathbb{Q}(t)$, que dependen de los coeficientes de Weierstrass de E tales que la familia de curvas:*

$$E_t \ : \ y^2 = x^3 + a(t)x + b(t), \qquad (t \in \mathbb{Q})$$

cumplen que $\bar{\rho}_{E,5} \cong \bar{\rho}_{E_t,5}$ para toda $t \in \mathbb{Q}$ salvo una cantidad finita de valores. En particular $E = E_0$.

Proposición 6.4.3. *Sean E y E' dos curvas elípticas sobre $\mathbb{Q}$ tales que $\bar{\rho}_{E,N} \cong \bar{\rho}_{E',N}$ para alguna $N \geq 5$. Si ℓ es un primo tal que $\ell \nmid N$. Entonces tenemos:*

$$E \ \text{ es semiestable en } \ \ell \quad \Longleftrightarrow \quad E' \ \text{ es semiestable en } \ \ell.$$

Nota. Si $N = 2, 3, 4$, entonces el teorema no es cierto porque la hipótesis es muy débil. Se requiere que E tenga reducción buena en ℓ para concluir que E' es semiestable en ℓ. Véase §7 de [Sil97] para ejemplos concretos donde el teorema no es válido para $N < 5$. Como nosotros estamos interesados en el caso $N = 5$, esto no produce problemas para nuestra aplicación.

Proposición 6.4.4. *Sea $\{E_t\}$ la familia de curvas elípticas de la proposición 6.4.2. Entonces para toda $t \in \mathbb{Q}$, salvo posiblemente una cantidad finita de valores, tenemos que $\bar{\rho}_{E_t,3}$ es irreducible.*

Nota. Esta proposición se sigue de un resultado importante, la verificación de la conjetura de Mordell-Weil, debido a Faltings: sea K un campo numérico y L una extensión finita de K, entonces

$$X/K \ \text{ es una variedad proyectiva lisa de género } \geq 2 \quad \Longrightarrow \quad X(L) \ \text{ es finito.} \tag{6.4.1}$$

Véase [Fal83] para una prueba.

Demostración. (del teorema 6.4.1) Sea $E/\mathbb{Q}$ una curva elíptica semiestable, dada por una ecuación $y^2 = x^3+ax+b$ con discriminante $\Delta = -16(4a^3+27b^2)$ y coeficiente $c_4 = -a/27$. Por la proposición 6.4.2 existe una familia de curvas elípticas $\{E_t\}_{t\in\mathbb{Q}}$ tales que $\bar{\rho}_{E,5} \cong \bar{\rho}_{E_t,5}$ para casi toda t. Como E es semiestable, por la proposición 6.4.3, E_t es semiestable en todo primo distinto de 5, para toda t.

Para probar la semiestabilidad de E_t en 5, sea $\{t_n\}$ una sucesión de racionales tales que $\{t_n\} \to 0$ en la topología 5−ádica de $\mathbb{Q}$, donde $E = E_0$. En particular tenemos que los coeficientes $a(t_n)$ y $b(t_n)$ tienden a $a(0) = a$ y $b(0) = b$ respectivamente en la topología 5−ádica.

Por las fórmulas de E_t, tenemos que $\Delta_t = -16(4a(t)^3 + 27b(t)^2)$ y que $c_4(t) = -a(t)/27$, donde $c_4(t)$ es la constante c_4 asociada a la curva E_t. Por lo tanto $\Delta_{t_n} \to \Delta$ y $c_4(t_n) \to c_4$ en la topología $5-$ádica. Como E es semiestable en 5, sucede uno de dos casos (cf. la definición 2.4.4).

Si $\nu_5(\Delta) = 0$, i.e. $|\Delta|_5 = 1$, entonces como $\Delta_{t_n} \to \Delta$ en la topología $5-$ádica, concluimos que $\nu(\Delta_{t_n}) = 0$ para n suficientemente grande ya que ν_5 es discreta. Por lo tanto E_{t_n} es semiestable en 5 para n suficientemente grande.

Si $\nu_5(\Delta) > 0$ y $\nu_5(c_4) = 0$, entonces cuando $t_n \to 0$, concluimos que $\nu_5(\Delta_{t_n}) \to \nu_5(\Delta)$ y $\nu_5(c_4(t_n)) \to \nu_5(c_4)$. Como ν_5 es discreta, los límites anteriores se vuelven constantes a partir de un entero suficientemente grande. Por lo tanto $\nu_5(\Delta_{t_n}) > 0$ y $\nu_5(c_4(t_n)) = 0$ para n suficientemente grande.

Con esto probamos que si tomamos $t \in \mathbb{Q}$ suficientemente cercano a 0 en la topología $5-$ádica, E_t es semiestable en 5 y por lo tanto es semiestable. Si juntamos esto con la proposición 6.4.4, podemos elegir t suficientemente cercano a 0 de tal manera que $\bar{\rho}_{E_t,3}$ es irreducible. Con esto terminamos. □

Ahora solamente nos falta probar las tres proposiciones que usamos en la prueba del teorema 6.4.1. Primero probamos la proposición 6.4.3 que es independiente de las otras dos. Luego probamos la proposición 6.4.2 y por último probamos la proposición 6.4.4.

Primero establecemos notación. Sea $\ell \in \mathbb{Z}$ un número primo y sea ν_ℓ la valuación $\ell-$ádica sobre $\mathbb{Q}$. Definimos el *subgrupo de inercia absoluto* de ℓ, denotado por $\mathcal{I}_\ell$, de la siguiente manera: elige un ideal maximal $\mathfrak{P} \subset \overline{\mathbb{Z}}$ sobre ℓ y se define

$$\mathcal{I}_\ell := \varprojlim_{L \supseteq \mathbb{Q}} I_{\mathfrak{P} \cap \mathcal{O}_L},$$

donde L corre sobre todas las extensiones finitas de Galois que contienen a $\mathbb{Q}$, y donde $I_{\mathfrak{P}\cap\mathcal{O}_L}$ es el subgrupo de inercia usual del ideal primo $\mathfrak{P} \cap \mathcal{O}_L$ de L, i.e.

$$I_{\mathfrak{P}\cap\mathcal{O}_L} = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \mid \sigma(x) \equiv x \pmod{\mathfrak{P} \cap \mathcal{O}_L},\ \forall x \in \mathcal{O}_L\}.$$

Observe que $\mathcal{I}_\ell$ está bien definido módulo conjugación, es decir que si elegimos otro ideal maximal $\mathfrak{P}' \subset \overline{\mathbb{Z}}$ sobre ℓ, entonces

$$\varprojlim I_{\mathfrak{P}'\cap\mathcal{O}_L} = \sigma \varprojlim I_{\mathfrak{P}\cap\mathcal{O}_L} \sigma^{-1},$$

donde $\sigma \in G_\mathbb{Q}$ es tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Esto se vale porque $G_\mathbb{Q}$ actúa transitivamente sobre el conjunto de los ideales maximales de $\overline{\mathbb{Z}}$ sobre ℓ.

Ahora sea K una extensión finita de $\mathbb{Q}$ con anillo de enteros $\mathcal{O}_K$ y sea $\mathfrak{p} \subset \mathcal{O}_K$ un ideal primo sobre ℓ. El subgrupo de inercia absoluto de $\mathfrak{p}$ se define similarmente como:

$$\mathcal{I}_\mathfrak{p} := \varprojlim_{L \supseteq K} I_{\mathfrak{P}\cap\mathcal{O}_L}$$

donde $\mathfrak{P} \subset \overline{\mathbb{Z}}$ es un ideal maximal sobre $\mathfrak{p}$ (y por lo tanto también está sobre ℓ). Similarmente al caso anterior, $\mathcal{I}_\mathfrak{p}$ está bien definido módulo conjugación.

Observe que si elegimos $\mathfrak{P} \subset \overline{\mathbb{Z}}$ sobre $\mathfrak{p}$, entonces podemos identificar $\mathcal{I}_\mathfrak{p}$ con un subgrupo de $\mathcal{I}_\ell$. Más precisamente, gracias a las definiciones con límites inversos, podemos agregarle a $\mathcal{I}_\mathfrak{p}$ un factor 1 para todos los subcampos de L de K para identificar $\mathcal{I}_\mathfrak{p}$ con un subgrupo de $\mathcal{I}_\ell$, es decir:

$$\mathcal{I}_\mathfrak{p} \cong \varprojlim_{L \supseteq \mathbb{Q}} \begin{Bmatrix} I_{\mathfrak{P}\cap\mathcal{O}_L} & L \supseteq K \\ 1 & L \subset K \end{Bmatrix} \subset \prod_{L \subset K} 1 \prod_{L \supseteq K} I_{\mathfrak{P}\cap\mathcal{O}_L} \subset \prod_{L \supseteq \mathbb{Q}} I_{\mathfrak{P}\cap\mathcal{O}_L}.$$

Como K es una extensión finita de $\mathbb{Q}$, solamente estamos agregando una cantidad finita de factores que a su vez son finitos. Por lo tanto el índice $(\mathcal{I}_\ell : \mathcal{I}_\mathfrak{p})$ es finito y podemos concluir que si $\tau \in \mathcal{I}_\ell$, entonces $\tau^M \in \mathcal{I}_\mathfrak{p}$ para alguna $M > 0$.

Ahora enunciamos la siguiente caracterización de semiestabilidad para probar la proposición 6.4.3.

Lema 6.4.5. *Sea E una curva elíptica definida sobre un campo numérico K y p un número primo fijo. Para todo primo $\ell \neq p$ tenemos que las siguientes propiedades son equivalentes:*

1. *E es semiestable en ℓ,*
2. *Para toda $\tau \in \mathcal{I}_\ell$, todos los valores propios de $\rho_{E,p}(\tau)$ son iguales a 1.*
3. *Para toda $\tau \in \mathcal{I}_\ell$ tenemos que $(\rho_{E,p}(\tau) - \mathrm{Id})^2 = 0$.*

Demostración. Véanse la proposición 3.5 y el corolario 3.8 de [Gro72]. □

Nota. Recuerde que $\mathcal{I}_\ell$ está bien definido módulo conjugación, pero esto no afecta las afirmaciones del lema anterior porque las condiciones (2) y (3) solamente dependen de la clase de conjugación del elemento $\tau \in \mathcal{I}_\ell$.

Demostración. (de la proposición 6.4.3) Para facilitar la exposición, solamente vamos a probar la proposición para el caso $N = 5$ que es el caso que necesitamos en esta tesis. Sea $E/\mathbb{Q}$ semiestable en $\ell \neq 5$ y $\bar{\rho}_{E,5} \cong \bar{\rho}_{E',5}$. Gracias al lema anterior, para probar que E' es semiestable en ℓ basta probar que los valores propios de $\rho_{E',5}(\tau)$ son 1 para toda $\tau \in \mathcal{I}_\ell$.

Sea $\tau \in \mathcal{I}_\ell$ y sea λ un valor propio de $\rho_{E',5}(\tau)$. Gracias al teorema de reducción semiestable (cf. la proposición 2.5.9), existe una extensión finita $K/\mathbb{Q}$ tal que E'/K es semiestable en un ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ sobre ℓ. Por el comentario antes del lema 6.4.5, tenemos que

$$\tau \in \mathcal{I}_\ell \quad \Longrightarrow \quad \exists\, M \geq 1 \text{ tal que } \tau^M \in \mathcal{I}_\mathfrak{p}.$$

Observe que podemos tomar M como el mínimo que cumple lo anterior.

Como E'/K es semiestable en $\mathfrak{p}$ y $\tau^M \in \mathcal{I}_\mathfrak{p}$, el lema 6.4.5 implica que

$$0 = \big(\rho_{E',5}(\tau^M) - \mathrm{Id}\big)^2 = \big(\rho_{E',5}(\tau)^M - \mathrm{Id}\big)^2.$$

Por lo tanto el valor propio λ de $\rho_{E',5}(\tau)$ satisface $(\lambda^M - 1)^2 = 0$ y en particular:

$$\lambda \text{ es valor propio de } \rho_{E',5}(\tau) \quad \Longrightarrow \quad \exists\, M > 0 \text{ tal que } \lambda^M = 1. \tag{6.4.2}$$

Por otro lado, tenemos que $\bar{\rho}_{E,5} \cong \bar{\rho}_{E',5}$, entonces si hacemos un cambio de base al espacio vectorial $E'[5] \cong \mathbb{F}_5 \times \mathbb{F}_5$, podemos asumir que $\bar{\rho}_{E,5}(\tau) = \bar{\rho}_{E',5}(\tau)$. Bajo la proyección $\pi : M_{2\times 2}(\mathbb{Z}_5) \twoheadrightarrow M_{2\times 2}(\mathbb{F}_5)$ módulo 5 tenemos que $\pi(\rho_{E,5}(\tau)) = \bar{\rho}_{E,5}(\tau)$ y $\pi(\rho_{E',5}(\tau)) = \bar{\rho}_{E',5}(\tau)$ (cf. el ejemplo 5.4.2). Entonces

$$\pi\big(\rho_{E,5}(\tau) - \rho_{E',5}(\tau)\big) = \bar{\rho}_{E,5}(\tau) - \bar{\rho}_{E',5}(\tau) = 0 \in M_{2\times 2}(\mathbb{F}_5).$$

Por lo tanto $\rho_{E',5}(\tau) - \rho_{E,5}(\tau)$ es una matriz cuyos coeficientes son múltiplos de 5. Si escribimos $B := \rho_{E,5}(\tau)$ y $B' := \rho_{E',5}(\tau)$ tenemos

$$B' - B \in 5M_{2\times 2}(\mathbb{Z}_5). \tag{6.4.3}$$

Como E es semiestable en ℓ y $\tau \in \mathcal{I}_\ell$, el lema 6.4.5 nos garantiza que $(B-\mathrm{Id})^2 = 0$. Esto se combina con (6.4.3) para dar:

$$\begin{aligned}(B'-\mathrm{Id})^2 &= ((B'-B)+(B-\mathrm{Id}))^2 \\ &= \underbrace{(B'-B)^2}_{\in 5M_{2\times 2}(\mathbb{Z}_5)} + 2\underbrace{(B'-B)}_{\in 5M_{2\times 2}(\mathbb{Z}_5)}(B-\mathrm{Id}) + \cancel{(B-\mathrm{Id})^2}.\end{aligned}$$

Por lo tanto $(B'-\mathrm{Id})^2 \in 5M_{2\times 2}(\mathbb{Z}_5)$ y en particular

$$C := \frac{(B'-\mathrm{Id})^2}{5} \in M_{2\times 2}(\mathbb{Z}_5).$$

Ahora sean $\lambda_1, \lambda_2 \in \overline{\mathbb{Q}_5}$ las dos raíces del polinomio característico $f(t)$ de $B' = \rho_{E',5}(\tau) \in \mathrm{GL}_2(\mathbb{Z}_5)$. Este polinomio tiene coeficientes enteros,[10] entonces $\lambda_1, \lambda_2 \in \overline{\mathbb{Z}}$. Como λ_i es un valor propio de B', tenemos $(\lambda_i-1)^2/5$ es un valor propio de $C \in M_{2\times 2}(\mathbb{Z}_5)$. Como $(\lambda_i-1)^2/5 \in \overline{\mathbb{Q}}$ y en $\overline{\mathbb{Z}_5}$ (por ser valor propio), tenemos $(\lambda_i-1)^2/5 \in \overline{\mathbb{Z}}$. Por lo tanto $(\lambda_i-1)^2/5$ satisface un polinomio mónico g con coeficientes en $\mathbb{Z}$ y de esta manera $\Lambda_i := (\lambda_i-1)/\sqrt{5}$ satisface el polinomio mónico $g(t^2) \in \mathbb{Z}[t]$, es decir $\Lambda_i \in \overline{\mathbb{Z}}$.

Con esto construimos los siguientes dos polinomios $h_+, h_- \in \overline{\mathbb{Z}}[t]$:

$$h_+(t) := (t+\Lambda_1)(t+\Lambda_2), \qquad h_-(t) := (t-\Lambda_1)(t-\Lambda_2)$$

Observe que el producto $h := h_+h_-$ es un polinomio mónico en $\overline{\mathbb{Z}}[t]$. Los polinomios h_+ y h_- están relacionados con el polinomio característico f de la siguiente manera:

$$h_\pm(t) = \frac{1}{5}f(1 \pm \sqrt{5}t). \tag{6.4.4}$$

Para probar esto vemos que $1+\sqrt{5}\Lambda_1 = \lambda_1$, entonces $f(1+\sqrt{5}\Lambda_1) = f(\lambda_1) = 0$ y por lo tanto $h_- \mid f(1+\sqrt{5}t)$. Como ambos polinomios son de grado 2, difieren en una constante que resulta ser 5 ya que f es mónico y de grado 2.

Con un cálculo sencillo, deducimos que el producto $h = h_+h_-$ pertenece a $\mathbb{Z}[1/5][t] \subset \mathbb{Q}[t]$. También tenemos que $h \in \overline{\mathbb{Z}}[t]$ por construcción, entonces los coeficientes de h están contenidos en

$$\mathbb{Z}[1/5] \cap \overline{\mathbb{Z}} \subset \mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}.$$

Por lo tanto Λ_1 y Λ_2, que son raíces de $h \in \mathbb{Z}[t]$, son enteros algebraicos. Acabamos de probar que si λ es un valor propio de B' entonces $(\lambda-1)/\sqrt{5} \in \overline{\mathbb{Z}}$. En particular hemos probado que

$$\lambda \text{ es un valor propio de } \rho_{E',5}(\tau) \quad \Longrightarrow \quad (\lambda-1)^2 \in 5\overline{\mathbb{Z}}. \tag{6.4.5}$$

Para terminar la prueba del teorema, vamos a ver cómo (6.4.5) se combina con $\lambda^M = 1$ de (6.4.2) para probar que $M = 1$ y por lo tanto $\lambda = 1$. Una última aplicación del lema 6.4.5 nos da que E' es semiestable en ℓ como buscábamos.

Supongamos que $M > 1$. Entonces existe un divisor primo q de M. Sea q^r la potencia más alta de q que divide a M. Con esto definimos $\zeta := \lambda^{Mq^{-r}}$ que es una raíz q^r-ésima primitiva de la unidad. En particular, ζ es raíz del q^r-ésimo polinomio ciclotómico Φ_{q^r} definido por

$$\Phi_{q^r}(x) := \prod_{\substack{j=1 \\ (j,q^r)=1}}^{q^r} (x-\zeta^j) \tag{6.4.6}$$

[10] Esto se sigue del teorema 4.3, parte a de [Gro72], además los coeficientes son independientes de $p = 5$.

que es irreducible con coeficientes enteros cumple las siguientes propiedades

$$\Phi_{q^r} \text{ tiene } \varphi(q^r) = (q-1)q^{r-1} \text{ raíces y } \Phi_{q^r}(1) = q. \tag{6.4.7}$$

Además, si $\mathcal{O}$ es el anillo de enteros de $\mathbb{Q}(\zeta)$, el ideal $q\mathcal{O}$ se descompone como $q\mathcal{O} = (1-\zeta)^{\varphi(q^r)}$, donde $(1-\zeta)$ es un ideal primo totalmente ramificado sobre $\mathbb{Z}$. Véase el lema 10.1 del capítulo 1 de [Neu99] para más detalles.

Observe que estas propiedades son independientes de qué raíz primitiva ζ elegimos. Por lo tanto $(1-\zeta^j)$ es un ideal primo sobre $q\mathcal{O}$ para toda j primo relativo con q^r. Entonces tenemos que $(1-\zeta) = (1-\zeta^j)$ para toda $(j, q^r) = 1$.

Por otro lado, observe que:

$$\begin{gathered} 1-\zeta = \left(1^{Mq^{-r}} - \lambda^{Mq^{-r}}\right) = (1-\lambda)(1+\cdots+\lambda^{Mq^{-r}-1}) \in (1-\lambda)\overline{\mathbb{Z}}. \\ \therefore \qquad (1-\zeta)^2 \in (1-\lambda)^2\overline{\mathbb{Z}} \subset 5\overline{\mathbb{Z}}, \qquad (j=1). \end{gathered} \tag{6.4.8}$$

Por lo tanto, las propiedades (6.4.7) y (6.4.8) nos implican que:

$$\begin{gathered} q^2 = (\Phi_{q^r}(1))^2 = \prod_{\substack{j=1 \\ (j,q^r)=1}}^{q^r} (1-\zeta^j)^2 \in \prod_j (1-\zeta^j)^2\overline{\mathbb{Z}} = \prod_j (1-\zeta)^2\mathbb{Z} \subset \prod_j (5\overline{\mathbb{Z}}) \\ \therefore \qquad q^2 \in 5^{\varphi(q^r)}\overline{\mathbb{Z}} \quad \Longrightarrow \quad q^2 5^{-\varphi(q^r)} \in \mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z} \end{gathered}$$

De esta manera $5^{\varphi(q^r)} \mid q^2$ lo cual implica que $q = 5$ y que

$$2 \geq \varphi(q^r) = (q-1)q^{r-1} = 4 \cdot 5^{r-1} \qquad \Longrightarrow\Longleftarrow .$$

Por lo tanto q primo y $r > 0$ no pueden existir lo cual implica que $M = 1$. Por lo tanto $\lambda = 1$ y terminamos. □

Ahora probamos la proposición 6.4.2, es decir cada curva $E/\mathbb{Q}$ pertenece a una familia de curvas elípticas con la misma representación módulo 5. Para hacer esto, vamos a construir una superficie elíptica $\mathcal{W}^E$ sobre la curva $\mathbb{P}^1(\mathbb{Q})$, tal que E es (isomorfa sobre $\mathbb{Q}$ a) la fibra de $\mathcal{W}$ sobre 0 y tal que casi todas las fibras $\mathcal{W}_t^E$ tienen la misma estructura de $5-$torsión como $G_{\mathbb{Q}}-$módulos.

La construcción de $\mathcal{W}^E$ depende de una propiedad universal que cumple la curva de Klein $W/\mathbb{Q}(t)$ que definimos en seguida, o más precisamente, la superficie elíptica $\mathcal{W}^E$ sobre $\mathbb{P}^1$ asociada a W. Para poder enunciar la propiedad universal necesitamos definir varias cosas.

Gracias al teorema de clasificación de superficies elípticas (cf. teorema 2.6.3), para definir $\mathcal{W}$, basta definir una curva elíptica W sobre $\mathbb{Q}(t)$. Tomamos la curva de Klein (cf. [Kle45, pg. 130]):

$$W \ : \ y^2 = x^3 + a_4(t)x + a_6(t)$$

donde $a_4, a_6 \in \mathbb{Q}(t)$ están definidos por

$$\begin{aligned} a_4(t) &= -\frac{1}{48}(t^{20} - 228t^{15} + 494t^{10} + 228t^5 + 1), \\ a_6(t) &= \frac{1}{864}(t^{30} + 522t^{25} - 10005t^{20} - 10005t^{10} - 522t^5 + 1). \end{aligned}$$

El $j-$invariante de W es:

$$j(W) = \frac{-(t^{20} - 228t^{15} + 494t^{10} + 228t^5 + 1)^3}{t^5(t^{10} + 11t^5 - 1)^5} \tag{6.4.9}$$

y define una función racional $t \mapsto j(W)$.

La curva de Klein tiene las siguientes propiedades de $5-$torsión:

Lema 6.4.6. *Sea W la curva de Klein definida arriba. Sea $P(t) = (x(t), y(t)) \in W(\mathbb{Q}(t))$ el punto definido por las coordenadas*

$$x(t) = \frac{1}{12}\big(t^{10} + 12t^8 - 12t^7 + 24t^6 + 30t^5 + 60t^4 + 36t^3 + 24t^2 + 12t + 1\big),$$
$$y(t) = \frac{1}{2}\big(t^{13} + t^{12} + 4t^{11} + 5t^9 + 6t^8 + 21t^7 + 29t^6 + 25t^5 + 15t^4 + 9t^3 + 4t^2 + t\big).$$

Entonces:

1. *$P(t), P(\zeta t) \in W[5]$, donde ζ es una raíz $5-$ésima primitiva de la unidad.*
2. *El subgrupo cíclico $C(t) = \langle P(t) - P(\zeta t)\rangle \subset W[5]$ es $G_{\mathbb{Q}}-$invariante y no contiene a $P(t)$.*

Demostración. $P(t), P(\zeta t) \in W[5]$ se verifican simbólicamente en el capítulo 7. Tenemos que $a_i(\zeta t) = a_i(t)$ porque a_i es un polinomio en t^5, por lo tanto las coordenadas de la isogenia $Q \mapsto 5Q$, que también es una función racional en las a_i, es invariante al cambio $t \mapsto \zeta t$. Esto implica que $P(\zeta t)$ también es un elemento de $5-$torsión. Como $P(t) \in W(\mathbb{Q}(t))$ y $P(\zeta t) \notin W(\mathbb{Q}(t))$, tenemos $P(t)$ y $P(\zeta t)$ son vectores independientes en $W[5]$ y así el subgrupo cíclico $C(t) = \langle P(t) - P(\zeta t)\rangle$ no contiene a $P(t)$. Por último, si $\sigma \in G_{\mathbb{Q}}$, entonces

$$\sigma P(\zeta t) = \sigma(x_1(\zeta t), y_1(\zeta t)) = (x_1(\sigma(\zeta)t), y_1(\sigma(\zeta)t)) = P(\sigma(\zeta)t)$$

porque las coordenadas $x_1(t), y_1(t) \in \mathbb{Q}(t)$. Sabemos que $\sigma(\zeta) = \zeta^i$ donde $i = \bar{\chi}_5(\sigma)$ donde $\bar{\chi}_5 : G_{\mathbb{Q}} \to (\mathbb{Z}/5\mathbb{Z})^*$ es el caracter ciclotómico módulo 5. Por lo tanto $\sigma P(\zeta t) = P(\zeta^{\bar{\chi}_5(\sigma)}t)$.

Si $\bar{\chi}_5(\sigma) = 1$, entonces σ actúa como la identidad en $\mathbb{Q}(\zeta)$ y por lo tanto fija a $P(\zeta t)$. Para los demás valores de $\bar{\chi}_5(\sigma)$, tenemos que:

$$\begin{aligned}
(\bar{\chi}_5(\sigma) = 1) \qquad & \sigma P(\zeta t) = P(\zeta t) = P(\zeta t) - 0P(t),\\
(\bar{\chi}_5(\sigma) = 2) \qquad & \sigma P(\zeta t) = P(\zeta^2 t) = 2P(\zeta t) - P(t),\\
(\bar{\chi}_5(\sigma) = 3) \qquad & \sigma P(\zeta t) = P(\zeta^3 t) = 3P(\zeta t) - 2P(t),\\
(\bar{\chi}_5(\sigma) = 4) \qquad & \sigma P(\zeta t) = P(\zeta^4 t) = 4P(\zeta t) - 3P(t).
\end{aligned}$$

(véase el capítulo 7 para los cálculos) Observ3 que estas cuatro ecuaciones, se pueden resumir en la siguiente fórmula:

$$\sigma P(\zeta t) = \bar{\chi}_5(\sigma)P(\zeta t) + \big(1 - \bar{\chi}_5(\sigma)\big)P(t).$$

Esta fórmula prueba que el subgrupo cíclico $C(t) = \langle P(t) - P(\zeta t)\rangle$ es $G_{\mathbb{Q}}-$estable porque si $Q := n(P(t) - P(\zeta t)) \in C(t)$ y $\sigma \in G_{\mathbb{Q}}$, entonces:

$$\sigma Q = n\sigma P(t) - n\sigma P(\zeta t) = nP(t) - n\big(\bar{\chi}_5(\sigma)P(\zeta t) + \big(1 - \bar{\chi}_5(\sigma)\big)P(t)\big)$$
$$\therefore \quad \sigma Q = n\bar{\chi}_5(\sigma)(P(t) - P(\zeta t)) \in C(t).$$

Por lo tanto $C(t)$ es $G_{\mathbb{Q}}-$estable, cíclico de orden 5 y no contiene a $P(t)$. □

Sea $\mathcal{W}$ la superficie elíptica sobre $\mathbb{P}^1$ asociada a W. Definimos la categoría

$$\mathcal{E}'(N)(K) := \left\{ (E,P,C) \ : \ \begin{array}{c} E/K \text{ curva elíptica,} \\ P \in E[N], \text{ de orden } N, \\ C \subset E[N] \text{ cíclico de orden } N \\ G_K - \text{estables tales que } P \notin C. \end{array} \right\}, \quad \begin{array}{c} (E,P,C) \cong (E',P',C') \text{ si:} \\ \exists\, f : E \xrightarrow{\sim} E' \text{ sobre } K, \ , \\ f(P) = P',\ f(C) = C' \end{array}$$

y al conjunto de clases de isomorfismo lo denotamos por

$$S'(N)(K) := \mathcal{E}'(N)(K)/_{\cong}.$$

Con esta notación, las fibras lisas $\mathcal{W}_t$ de $\mathcal{W}$ son elementos de $\mathcal{E}'(5)(\mathbb{Q})$, es decir:

$$\text{para casi toda } \ t \in \mathbb{P}^1 \ \text{ tenemos } \ \big(\mathcal{W}_t, P(t), C(t)\big) \in \mathcal{E}'(5)(\mathbb{Q}). \tag{6.4.10}$$

Esto nos sugiere que $\mathcal{W}$ es una superficie elíptica sobre la curva modular que parametriza los elementos de $S'(5)(\mathbb{Q})$. Vamos a probar más adelante que esta curva modular es isomorfa a $\mathbb{P}^1$.

Podemos caracterizar $S'(N)(K)$ con la forma bilineal de Weil $e_N : E[N] \times E[N] \to \mu_N$ (cf. la proposición 2.1.15). Más precisamente definimos:

$$V_N := \mathbb{Z}/N\mathbb{Z} \times \mu_N, \qquad \eta_N : V_N \times V_N \to \mu_N \quad \text{con} \quad \eta_N\big((a_1,\zeta_1),(a_2,\zeta_2)\big) = \zeta_2^{a_1}/\zeta_1^{a_2},$$

entonces V_N tiene una acción natural de G_K en el segundo factor y η_N es G_K-equivariante bajo esta acción, es decir $\eta((a_1,\sigma\zeta_1),(a_2,\sigma\zeta_2)) = \sigma\eta((a_1,\zeta_1),(a_2,\zeta_2))$ para toda $\sigma \in G_K$. Con esta notación, podemos reescribir $S'(N)(K)$ como clases de isomorfismo de curvas elípticas que preservan un isomorfismo $V_N \xrightarrow{\sim} E[N]$ de G_K-módulos que transfiere la forma bilineal de Weil en η_N. Más precisamente, definimos:

$$\mathcal{E}(e_N)(K) = \left\{ (E,\phi) \ : \ \begin{array}{c} E/K \text{ curva elíptica,} \\ \phi : V_N \xrightarrow{\sim} E[N] \text{ de } G_K - \text{módulos} \\ \eta_N(u,v) = e_N(\phi(u),\phi(v)) \end{array} \right\}, \quad \begin{array}{c} (E,\phi) \cong (E',\phi') \text{ si:} \\ \exists f : E \xrightarrow{\sim} E' \text{ sobre } K, \ , \\ \phi' = f \circ \phi \end{array}$$

y denotamos por $S(e_N)(K)$ al conjunto de clases de isomorfismo. Entonces tenemos una biyección

$$S(e_N)(K) \longleftrightarrow S'(N)(K)$$

definida por $[E,\phi] \mapsto [E,\phi(1,1),\phi(0\times\mu_N)]$ y por otro lado, $[E,P,C] \mapsto [E,\phi]$ donde $\phi(a,\zeta) = aP + Q$ donde Q es el único punto $Q \in C$ tal que $e_N(P,Q) = \zeta$. En efecto, si tomamos $[E,P,C] \mapsto [E,\phi]$, entonces $\phi(1,1) = 1P + O = P$ porque $e_N(P,O) = 1$ y $C = \phi(0 \times \mu_N)$ porque $Q = \phi(0,\zeta) \in C$ implica que $\phi(0 \times \mu_N) \subseteq C$ y tienen la misma cardinalidad. Observe que los comentarios anteriores implican que tenemos los siguientes isomorfismos de G_K-módulos:

$$(E,P,C),(E',P',C') \in \mathcal{E}'(N)(K) \quad \Longrightarrow \quad E[N] \cong V_N \cong E'[N]. \tag{6.4.11}$$

Esto, junto con el lema 6.4.6, o más precisamente (6.4.10), implica que para casi toda fibra $\mathcal{W}_t$, tenemos que $\mathcal{W}_t[5] \cong V_5$ como $G_{\mathbb{Q}}-$módulos y por lo tanto:

Lema 6.4.7. *Existe un conjunto finito $T \subset \mathbb{P}^1$ tal que para todas $t_1, t_2 \in \mathbb{P}^1 - T$ tenemos que $\mathcal{W}_{t_1}[5] \cong \mathcal{W}_{t_2}[5]$ como $G_{\mathbb{Q}}-$módulos o equivalentemente $\bar{\rho}_{\mathcal{W}_{t_1},5} \cong \bar{\rho}_{\mathcal{W}_{t_2},5}$.*

Por la teoría de modelos de Shimura, podemos realizar el conjunto de clases de isomorfismo $S'(5)(\mathbb{Q})$ como el conjunto de puntos racionales de una curva sobre $\mathbb{Q}$:

Lema 6.4.8. *Existe una curva lisa afín Y_5 definida sobre $\mathbb{Q}$ y una biyección $Y_5(\mathbb{Q}) \to S(e_5)(\mathbb{Q})$. Además, si X_5 denota la compactificación de Y_5 en la topología de Zariski, entonces hay un isomorfismo $f : \mathbb{P}^1 \xrightarrow{\sim} X_5$ sobre $\mathbb{Q}$ inducido por $t \mapsto [\mathcal{W}_t, P(t), C(t)]$.*

Demostración. La existencia de Y_5 se sigue de la teoría de Deligne y Rapaport en [DR73] o más precisamente del corolario 4.7.1 de [KM85] (véase el teorema 4.3.6 y el comentario que lo procede).

Si elegimos una raíz 5−ésima de la unidad ζ, tenemos un isomorfismo $Y_5(\mathbb{C}) \to Y(5) = \mathbb{H}/\Gamma(5)$ inducido por la función $[E, \phi] \mapsto [E, \phi(1,1), \phi(0,\zeta)]$ ya que podemos identificar los puntos de $Y(5)$ con el conjunto $S(5)(\mathbb{C})$ (véase el teorema 4.3.6). Por lo tanto, como la proyección $X(5) \to X(1)$ tiene grado:

$$[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma(5)] = \frac{1}{2}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(5)] \overset{(3.2.2)}{=} \frac{5^3 - 5}{2} = 60.$$

El grado de esta proyección en $\mathbb{C}$−puntos implica que la proyección $g : X_5 \to X(1)$, inducido por $[E, P, C] \mapsto [E]$, también es de grado 60. Como $j : X(1) \to \mathbb{P}^1$ es de grado 1, la composición $h : X_5 \to X(1) \to \mathbb{P}^1$ es de grado 60. Observe que $h[E, P, C] = j(E)$.

Ahora componemos h con f para obtener:

$$\begin{array}{ccccc} \mathbb{P}^1 & \xrightarrow{f} & X_5 & \xrightarrow{h} & \mathbb{P}^1 \\ t & & \longrightarrow & & j(W) \end{array}$$

donde $J(W)$ está dado por una función racional cuyo numerador y denominador son de grado 60 por (6.4.9), entonces el grado de la composición es a lo más 60. Por lo tanto, como el grado de h es 60, la composición es de grado exactamente 60. Concluimos que f es de grado 1 y es un isomorfismo. □

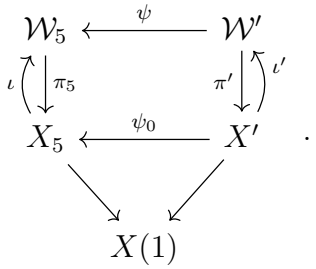
Si identificamos X_5 con $\mathbb{P}^1$, podemos considerar $\mathcal{W}$ como una superficie elíptica sobre X_5 con la proyección $\pi_5 := f \circ \pi$ y sección cero $\iota_5 := \iota \circ h$, donde π y ι son la proyección y sección cero de la superficie $\mathcal{W}$. A $\mathcal{W}$ como superficie sobre X_5, la denotamos por $\mathcal{W}_5$.[11] Simbólicamente:

$$\begin{array}{ccc} \mathcal{W} & = & \mathcal{W}_5 \\ {\scriptstyle\iota}\uparrow\downarrow{\scriptstyle\pi} & & {\scriptstyle\pi_5}\downarrow\uparrow{\scriptstyle\iota_5} \\ \mathbb{P}^1 & \xrightarrow{f} & X_5 \end{array} \tag{6.4.12}$$

Resulta que los subgrupos de 5−torsión de casi todas las fibras de $\mathcal{W}_5$ son isomorfas entre sí como $G_{\mathbb{Q}}$−módulos. Esto también sucede para cualquier otra superficie elíptica $\mathcal{W}'$ sobre una curva X' tal que $\mathcal{W}_5 \cong \mathcal{W}'$ y $X_5 \cong X'$ sobre $\mathbb{Q}$ donde estos isomorfismos conmutan con las proyecciones y secciones cero de ambas superficies. Más precisamente tenemos que:

[11] El "5" como subíndice se refiere a la torsión y no a la fibra de $\mathcal{W}_5$ sobre 5. El contexto dicta el significado de esta notación.

Lema 6.4.9. *Sea $X'/\mathbb{Q}$ una curva y $\mathcal{W}' = (\mathcal{W}', \pi', \iota')$ una superficie elíptica sobre X', definida sobre $\mathbb{Q}$. Supongamos que hay isomorfismos $\psi_0 : X' \xrightarrow{\sim} X_5$ y $\psi : \mathcal{W}' \xrightarrow{\sim} \mathcal{W}_5$ definidos sobre $\overline{\mathbb{Q}}$ que caben en los siguientes dos diagramas conmutativos:*



Para todas $t_1, t_2 \in X'(\mathbb{C}) - T$, con T un conjunto finito, tenemos que las fibras $\mathcal{W}'_{t_1}$ y $\mathcal{W}'_{t_2}$ de t_1 y t_2 respectivamente son curvas elípticas definidas sobre $\mathbb{Q}(t_1)$ y $\mathbb{Q}(t_2)$. Además $\mathcal{W}'_{t_1}[5] \cong \mathcal{W}'_{t_2}[5]$ como $G_{\mathbb{Q}}-$módulos.

Demostración. Véase la proposición 2.1 y el corolario 2.2 de [RS97] □

En seguida describimos un algoritmo que, dada una curva elíptica E, construye una superficie elíptica $\mathcal{W}^E$ sobre $\mathbb{P}^1$ asociada a E que satisface la misma propiedad universal que cumple $\mathcal{W}$. De esta manera las fibras lisas $\mathcal{W}_t^E$ son curvas elípticas tales que $\bar{\rho}_{E,5} \cong \bar{\rho}_{\mathcal{W}_t^E,5}$ para casi toda $t \in \mathbb{P}^1$.

Para enunciar el algoritmo definimos $\mathcal{J} \in \mathbb{Q}(t)$ como $\mathcal{J}(t) := j(W)$ dado por (6.4.9).

Algoritmo 6.4.10. Sea $E/\mathbb{Q}$ una curva elíptica.

1. Calcule una raíz $t_0 \in \overline{\mathbb{Q}}$ del numerador de $\mathcal{J}(t) - j(E) \in \mathbb{Q}(t)$, i.e. $\mathcal{J}(t_0) = j(E)$.
2. Encuentre una $\mu \in \overline{\mathbb{Q}}^*$ tal que $\mu^{-2}a_4(t_0), \mu^{-3}a_6(t_0) \in \mathbb{Q}$ y tal que la curva elíptica definida por
$$y^2 = x^3 + \mu^{-2}a_4(t_0)x + \mu^{-3}a_6(t_0) \tag{6.4.13}$$
es isomorfa a E sobre $\mathbb{Q}$ (cf. la proposición 2.1.6).
3. Encuentre elementos $a, c \in \overline{\mathbb{Q}}$ tales que
$$a'_4(t) := \mu^{-2}(ct+1)^{20}a_4\left(\frac{at+t_0}{ct+1}\right) \in \mathbb{Q}[t], \quad a'_6(t) := \mu^{-3}(ct+1)^{30}a_6\left(\frac{at+t_0}{ct+1}\right) \in \mathbb{Q}[t].$$

Por lo tanto, si definimos la superficie elíptica $\mathcal{W}^E$ sobre $\mathbb{P}^1$ como:

$$\mathcal{W}^E \ : \ y^2 = x^3 + a'_4(t)x + a'_6(t),$$

entonces para toda $t \in \mathbb{Q} - S$, tenemos que la fibra $\mathcal{W}_t^E$ es una curva elíptica sobre $\mathbb{Q}$ tal que $\bar{\rho}_{E,5} \cong \bar{\rho}_{\mathcal{W}_t^E,5}$, donde S es el conjunto finito de polos de $\mathcal{J} \circ \gamma$ donde:

$$\gamma = \begin{pmatrix} a & t_0 \\ c & 1 \end{pmatrix}.$$

Nota. Observe que para $t = 0$, tenemos que $\mathcal{W}_0^E \cong E$ porque $a'_4(0) = \mu^{-2}a_4(t_0)$ y $a'_6(0) = \mu^{-3}a_6(t_0)$ implican que la fibra $\mathcal{W}_0^E$ es isomorfa a E sobre $\mathbb{Q}$ por construcción de t_0 y μ (cf. la ecuación 6.4.13).

Demostración. (del algoritmo) El algoritmo es esencialmente una aplicación de la propiedad universal que cumple la curva de Klein W, i.e. el lema 6.4.9.

Para esto primero definimos:

$$\psi_0 : \mathbb{P}^1 \longrightarrow \mathbb{P}^1 \quad \text{definido por} \quad t \mapsto \gamma t = \frac{at + t_0}{ct + 1}.$$

Observe que

$$\begin{aligned}
\mathcal{J}\left(\frac{at+t_0}{ct+1}\right) &= -1728\frac{\left(4a_4\left(\frac{at+t_0}{ct+1}\right)\right)^3}{-16\left(4a_4\left(\frac{at+t_0}{ct+1}\right)^3 + 27a_6\left(\frac{at+t_0}{ct+1}\right)^2\right)} \\
&= 6912\frac{\mu^{-6}(ct+1)^{60}}{\mu^{-6}(ct+1)^{60}} \cdot \frac{a_4\left(\frac{at+t_0}{ct+1}\right)^3}{4a_4\left(\frac{at+t_0}{ct+1}\right)^3 + 27a_6\left(\frac{at+t_0}{ct+1}\right)^2} \\
&= 6912\frac{a_4'(t)^3}{a_4'(t)^3 + a_6'(t)^2} \in \mathbb{Q}(t).
\end{aligned}$$

Por lo tanto ψ_0 es un isomorfismo definido sobre $\mathbb{Q}$.

Ahora definimos

$$\psi : \mathcal{W}^E \longrightarrow \mathcal{W} \quad \text{definido por} \quad (x, y, t) \mapsto \left(\mu(ct+1)^{-10}x, \mu^{3/2}(ct+1)^{-15}y, \frac{at+t_0}{ct+1}\right).$$

Entonces ψ está definido sobre $\mathbb{Q}$ y es un isomorfismo. De esta manera tenemos los siguientes diagramas conmutativos:

$$\begin{array}{ccc}
\mathcal{W} & \xleftarrow{\psi} & \mathcal{W}^E \\
{\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\
\mathbb{P}^1 & \xleftarrow{\psi_0} & \mathbb{P}^1 \\
& \searrow \quad \swarrow & \\
& X(1) &
\end{array}
\qquad
\begin{array}{ccc}
\mathcal{W} & \xleftarrow{\psi} & \mathcal{W}^E \\
{\scriptstyle\iota}\uparrow & & \uparrow{\scriptstyle\iota'} \\
\mathbb{P}^1 & \xleftarrow{\psi_0} & \mathbb{P}^1
\end{array}
\quad .$$

Por lo tanto la propiedad universal de $\mathcal{W}$ nos dice que para casi toda $t \in \mathbb{P}^1(\mathbb{C})$ (donde t no es polo de $\mathcal{J} \circ \psi_0$), las fibras $\mathcal{W}_t^E$ son curvas elípticas definidas sobre $\mathbb{Q}(t)$. Además, si $t_1, t_2 \in \mathbb{Q}$, entonces las fibras sobre t_1 y t_2 tienen la misma representación módulo 5. Como $\mathcal{W}_0^E \cong E$, entonces para casi toda $t \in \mathbb{Q}$, tenemos que $\bar{\rho}_{E,5} \cong \rho_{\mathcal{W}_t^E,5}$. □

Aplicamos el algoritmo de manera simbólica a una curva E dada por una ecuación de Weierstrass $y^2 = x^3 + Ax + B$; los cálculos se hacen en [RS97, §5]. Esta aplicación prueba la proposición 6.4.2:

Corolario 6.4.11. *Sea $E/\mathbb{Q}$ una curva elíptica dada por $y^2 = x^3 + Ax + B$ con j invariante $j = j(E)$. Se definen los siguientes dos polinomios*

$$A(t) := A\sum_{k=0}^{20} \alpha_k t^k, \qquad B(t) = B\sum_{k=0}^{30} \beta_k t^k,$$

donde $\alpha_k, \beta_k \in \mathbb{Q}[j]$ son los polinomios definidos en el apéndice de [RS97]. Ahora se define la curva E_t como:

$$E_t \ : \ y^2 = x^3 + A(t)x + B(t).$$

Entonces para toda $t \in \mathbb{Q}$ tal que E_t es no singular, tenemos que $\bar{\rho}_{E,5} \cong \bar{\rho}_{E_t,5}$. En el caso particular de $t = 0$, tenemos que $E = E_0$.

Para probar la proposición 6.4.4, necesitamos una construcción similar a la de la curva modular Y_5 del lema 6.4.8. Primero introducimos notación: dada una curva elíptica $\hat{E}/K$, definimos

$$\mathcal{E}_{\hat{E}}(5,3)(K) = \left\{ (E,\phi,C) \ : \ \begin{array}{c} E/K \text{ curva elíptica,} \\ \phi : \hat{E}[5] \xrightarrow{\sim} E[5] \text{ de } G_K - \text{módulos} \\ \eta_5(u,v) = e_5(\phi(u),\phi(v)) \\ C \subseteq E[3] \text{ cíclico de orden 3} \end{array} \right\}, \quad \begin{array}{c} (E,\phi,C) \cong (E',\phi',C) \text{ si:} \\ \exists f : E \xrightarrow{\sim} E' \text{ sobre } K, \quad , \\ \phi' = f \circ \phi, \ f(C) = C' \end{array}$$

Al conjunto de clases de isomorfismo de elementos de $\mathcal{E}_{\hat{E}}(5,3)(K)$, lo denotamos por $S_{\hat{E}}(5,3)(K)$. Observe que hay una función

$$S_{\hat{E}}(5,3)(K) \longrightarrow S(e_5)(K) \quad \text{definido por} \quad [E,\phi,C] \mapsto [E,\phi], \tag{6.4.14}$$

donde estamos identificando $\hat{E}[5]$ con V_5. Tenemos el siguiente resultado similar al lema 6.4.8 que enunciamos en seguida:

Lema 6.4.12. *Sea $E/\mathbb{Q}$ una curva elíptica. Existe una curva lisa y afín $Y_{5,3}^E$ y una biyección $Y_{5,3}^E(\mathbb{Q}) \to S_E(5,3)(\mathbb{Q})$. Su compactificación $X_{5,3}^E$ es isomorfa sobre $\mathbb{C}$ a $\mathbb{H}^*/(\Gamma(5) \cap \Gamma_0(3))$ y por lo tanto tiene género 9.*

Este resultado también se sigue de la teoría de Deligne y Rapaport y el género se calcula con las fórmulas de la sección 3.2.

Por el teorema de Faltings (la conjetura de Mordell), tenemos que $Y_{5,3}^E(\mathbb{Q})$, y por lo tanto $S_E(5,3)(\mathbb{Q})$, es finito. Entonces la imagen de $S_E(5,3)(\mathbb{Q}) \to S(e_5)(\mathbb{Q})$, definida en (6.4.14), es finita.

Por el lema 6.4.12, $Y_{5,3}^E(\mathbb{Q})$ está en biyección con $S_E(5,3)(\mathbb{Q})$ y por el lema 6.4.8 tenemos que $Y_5(\mathbb{Q})$ está en biyección con $S(e_5)(\mathbb{Q})$, por lo tanto la imagen de la función inducida $Y_{5,3}^E(\mathbb{Q}) \to Y_5(\mathbb{Q})$ es finita.

Esto significa que para casi todo punto $[E,\phi] \in Y_5(\mathbb{Q})$, E no tiene un subgrupo cíclico de orden 3 definido sobre $\mathbb{Q}$ y por lo tanto $E[3]$ es irreducible como $G_{\mathbb{Q}}-$módulo, i.e. $\bar{\rho}_{E,3}$ es irreducible. Esto prueba la proposición 6.4.4 y terminamos las pruebas de todos los argumentos necesarios para probar el teorema principal de esta sección.

6.5. El último teorema de Fermat

Fermat, en el margen de su copia de *Arithmetica* de Diofanto, propuso que la ecuación $x^n + y^n = z^n$ no tiene soluciones enteras no triviales para toda $n > 2$. Decimos que una solución (a,b,c) de la ecuación diofantina $x^n + y^n = z^n$, donde $a,b,c \in \mathbb{Z}$, es una solución *no trivial* si $abc \neq 0$, i.e. los tres enteros son distintos de cero. Con esto, el enunciado de Fermat se convierte en

$$(a,b,c) \text{ es una solución de la ecuación diofantina } x^n + y^n = z^n \implies abc = 0. \tag{UTF(n)}$$

Fermat dijo que esto era cierto para toda $n > 2$. Cuando $n = 1$, UTF(n) es claramente falso y también para $n = 2$. En efecto, la ecuación diofantina $x^2+y^2 = z^2$ tiene una infinidad de soluciones no triviales, las famosas *ternas pitagóricas*. De hecho las ternas pitagóricas están parametrizadas por parejas de enteros (a, b) tales que $(a, b) = 1$ y al menos uno es par; dada una pareja de éstas podemos construir la solución $(b^2 - a^2, 2ab, a^2 + b^2)$. Para ver esto simplemente hay que observar que (a, b, c) es una terna pitagórica si y solo si $|a + ib| \in \mathbb{Z}$, por lo tanto si $a + ib \in \mathbb{Z}[i]$ entonces $|(a + ib)^2| \in \mathbb{Z}$ y así $(b^2 - a^2, 2ab, a^2 + b^2)$ es una terna pitagórica.

El caso $n = 3$ es debido a Euler. La prueba es por descenso infinito como en el caso $n = 4$ (cf. proposición 6.5.1) y la prueba definitiva de Euler aparece en la segunda parte de su libro de texto de álgebra [Eul70, capítulo XV]. No probamos el caso $n = 3$, pero esbozamos una prueba debida a Lamé: factorizamos la ecuación de Fermat como

$$(x + y)(x + \zeta y)(x + \zeta^2 y) = z^3, \quad \left(\zeta = \frac{-1 + \sqrt{-3}}{2}\right).$$

Los tres factores del lado izquierdo son primos relativos, entonces, como $\mathbb{Z}[\zeta]$ es un dominio de factorización única, la ecuación anterior implica que cada factor del lado izquierdo es un cubo en $\mathbb{Z}[\zeta]$, pero esto no puede suceder.

El siguiente caso $n = 4$, lo probamos porque es muy elemental y corto; la prueba es debida a Fermat:

Proposición 6.5.1. *UTF(4) es cierto, es decir la ecuación $x^4 + y^4 = z^4$ no tiene soluciones no triviales.*

Demostración. Como Fermat, probaremos algo más fuerte: la ecuación diofantina $x^4 + y^4 = z^2$ no tiene soluciones no triviales. Observe que si (a, b, c) es una solución de $x^4+y^4 = z^4$, entonces (a, b, c^2) es una solución de $x^4 + y^4 = z^2$ y por lo tanto la falta de soluciones no triviales de $x^4 + y^4 = z^2$ implica UTF(4).

Supongamos que (a, b, c) es una solución. Probamos que a o b es par. Si ambos son impares, tenemos a^4 y b^4 son impares y por lo tanto $c^2 = a^4 + b^4$ es par. Esto implica que c es par y así $4 \mid c^2 = a^4 + b^4$. Por otro lado:

$$a^4 + b^4 = (a + b)^4 - 4a^3b - 6a^2b^2 - 4ab^3 \quad \Longrightarrow \quad (a^4 + b^4) - (a + b)^4 + 4a^3b + 4ab^3 = -6a^2b^2.$$

Como $a + b$ es par, $4 \mid (a + b)^4$, entonces 4 divide a todos los sumandos del lado izquierdo y por lo tanto 4 divide a $6a^2b^2$. Esto es una contradicción porque a^2 y b^2 son impares. Por lo tanto a o b es par.

Si (a, b, c) es una solución, entonces (b, a, c) es otra y así podemos asumir sin pérdida de generalidad que b es par. Por otro lado $(-a, -b, -c)$ también es solución, entonces podemos asumir que $b > 0$. Ahora asumimos que la solución (a, b, c) es tal que b es mínimo entre las segundas coordenadas de todas las soluciones.

Ahora, como (a, b, c) es solución, tenemos que $(a^2)^2 + (b^2)^2 = c^2$, es decir (a^2, b^2, c) es una terna pitagórica. Por lo tanto existen $d, e \in \mathbb{Z}$, primos relativos, tales que

$$a^2 = e^2 - d^2, \quad b^2 = 2de, \quad c = d^2 + e^2.$$

La primera ecuación de arriba implica que (a, d, e) es una terna pitagórica, es decir existen enteros f y g, primos relativos, tales que

$$a = g^2 - f^2, \quad d = 2fg, \quad e = f^2 + g^2.$$

Como f y g son primos relativos, la tercera ecuación de arriba implica que e, f y g son primos relativos dos a dos. Por lo tanto

$$b^2 = 2de = 4efg \quad \Longrightarrow \quad (b/2)^2 = efg \quad \Longrightarrow \quad e, f, g \text{ son cuadrados.}$$

Entonces existen $e_0, f_0, g_0 \in \mathbb{Z}$ tales que $e = e_0^2$, $f = f_0^2$ y $g = g_0^2$. Sustituimos esto en la ecuación para e y obtenemos $e_0^2 = f_0^4 + g_0^4$, es decir (f_0, g_0, e_0) es una solución de $x^4 + y^4 = z^2$. Pero esto es una contradicción porque

$$(b/2)^2 = efg \quad \Longrightarrow \quad b/2 = e_0 f_0 g_0 \quad \Longrightarrow \quad g_0 \mid b/2 \quad \Longrightarrow \quad g_0 < b$$

y por lo tanto b no es mínimo entre las segundas coordenadas de las soluciones, lo cual contradice la construcción de (a, b, c). Por lo tanto $x^4 + y^4 = z^2$ no tiene soluciones no triviales y con esto concluimos que UTF(4) es verdadero. □

Hemos visto que UTF(n) es falso para $n = 1, 2$ y verdadero para $n = 3, 4$. En lugar de seguir con $n = 5, 6, 7, \ldots$, ahora buscamos restringir los posibles valores de n donde UTF(n) es verdadero. Supongamos que hemos probado que UTF(n) es verdadero para alguna n y sea $m > 0$ un múltiplo de n, i.e. $m = nk$ para alguna $k \in \mathbb{Z}$, entonces afirmamos que UTF(m) también es verdadero. En efecto: si (a, b, c) es una solución de $x^m + y^m = z^m$ entonces (a^k, b^k, c^k) es una solución de $x^n + y^n = z^n$, por UTF(n), tenemos que $a^k b^k c^k = (abc)^k = 0$ y en particular $abc = 0$. Por lo tanto hemos probado que

$$n \mid m \quad \Longrightarrow \quad \Big(\text{UTF}(m) \implies \text{UTF}(n)\Big).$$

Esto significa que solamente hay que probar UTF(p) para todo primo impar p, para probar UTF(n) para toda $n > 2$. Con este método solamente nos faltan los casos cuando n no es divisible por un primo impar, i.e. $n = 2^k$ para alguna $k > 0$. Si $k = 1$ vimos que UTF(2) es falso, pero si $k > 1$, entonces $4 \mid n$ y por la proposición 6.5.1 tendremos que UTF(2^k) es verdadero para $k > 1$.

En resumen, solamente hay que probar UTF(n) para n primo impar o $n = 4$. Como ya vimos que UTF(3) y UTF(4) son verdaderos, el último teorema de Fermat lo hemos reducido al siguiente enunciado:

Teorema 6.5.2. *Sea $p \geq 5$ un primo impar. Entonces la ecuación diofantina $x^p + y^p + z^p = 0$ no tiene soluciones no triviales, es decir para todo $p \geq 5$ tenemos*

$$\exists\, a, b, c \in \mathbb{Z} \ \textit{tales que} \ a^p + b^p + c^p = 0 \quad \Longrightarrow \quad abc = 0. \qquad (\text{UTF}(p))$$

Nota. A la ecuación diofantina $x^p + y^p + z^p = 0$ se le llama la *ecuación de Fermat*. Por la simetría de esta ecuación, si permutamos las entradas de una solución (a, b, c) obtenemos otra solución. Por lo tanto podemos permutar libremente las entradas de cualquier solución a la ecuación de Fermat. Además, si (a, b, c) es una solución, entonces $(\lambda a, \lambda b, \lambda c)$ es otra solución para toda $\lambda \in \mathbb{Z}$, es decir podemos escalar las soluciones y en particular podemos cambiar el signo de toda la terna.

Si estamos trabajando con una supuesta solución a la ecuación de Fermat, podemos asumir algunas propiedades elementales sobre la solución. Por ejemplo, si (a, b, c) es una solución, podemos asumir que a, b y c no comparten factores primos. En efecto, si $d \mid a, b, c$, entonces $(a/d, b/d, c/d)$ es otra solución de la ecuación de Fermat. Por lo tanto podemos eliminar todos los factores comunes de las entradas de una solución (a, b, c) para obtener una terna (a', b', c') donde a', b' y c' son primos

relativos; una solución de esta forma se llama una solución *primitiva*, es decir podemos asumir que la solución (a, b, c) es primitiva.

Otra propiedad que podemos asumir de una solución (a, b, c) es que b es par. En efecto, a, b y c no pueden ser todos impares, porque en este caso la ecuación de Fermat se reduciría módulo 2 a $0 \equiv a^p + b^p \equiv c^p \equiv 1 \pmod 2$, lo cual es falso. Por lo tanto alguno de a, b o c es par. Como no importa el orden de la terna (a, b, c), podemos asumir que $2 \mid b$.

Entonces podemos escribir $b = 2b'$ para alguna $b' \in \mathbb{Z}$. Si reducimos la ecuación $a^p + b^p = c^p$ módulo 4 obtenemos

$$a \equiv a^p \equiv 2^p b'^p + c^p \equiv c^p \equiv c \pmod 4$$

y por lo tanto $a \equiv c \equiv 1$ o $a \equiv c \equiv -1 \pmod 4$ (ya que ambos no pueden ser pares). Como podemos cambiar el signo a toda la terna, podemos asumir sin pérdida de generalidad que $a \equiv -1 \pmod 4$.

En resumen, si (a, b, c) es una supuesta solución a la ecuación diofantina $x^p + y^p + z^p = 0$, entonces podemos asumir sin pérdida de generalidad que la solución satisface las siguientes tres propiedades:

$$\begin{gathered} (a, b, c) = 1, \\ 2 \mid b, \\ a \equiv -1 \pmod 4. \end{gathered} \tag{*}$$

De ahora en adelante, cuando tomamos una solución no trivial (a, b, c) de la ecuación de Fermat $x^p + y^p + z^p = 0$ vamos a asumir que a, b y c cumplen las condiciones *.

Antes de la prueba del último teorema de Fermat en 1995, una posible demostración fue propuesta por Frey en [Fre86, III. Conjectures]. Un año después, Serre adaptó el método de Frey e identificó una conjetura precisa sobre representaciones de Galois de la cual se deducía el último teorema de Fermat mediante el método de Frey.

Ahora describimos la prueba del UTF en cuatro pasos, basados en las pruebas propuestas en [Fre86] y [Ser87]. El primer paso es construir una curva elíptica semiestable E asociada a una solución no trivial de la ecuación de Fermat; esta curva se llama la *curva de Frey* y vimos algunas propiedades al final de la sección 2.5.

Recordemos que la curva de Frey se define como la curva elíptica

$$y^2 = x(x - A)(x + B)$$

donde A, B y C son enteros tales que $A + B + C = 0$; en particular tomamos $A = a^p$, $B = b^p$ y $C = c^p$ donde (a, b, c) es una solución a la ecuación de Fermat. Denotamos por E a esta curva elíptica, i.e.

$$E \ : \ y^2 = x(x - a^p)(x + b^p).$$

La curva de Frey E cumple dos propiedades importantes:

(I) E es semiestable.

(II) El conductor de E es:

$$N = \prod_{\substack{\ell \mid abc \\ \ell \text{ primo}}} \ell.$$

En particular $N_{a,b,c,p}$ es par.

El segundo paso, debido a Serre, es traducir las propiedades de E a propiedades de ramificación de la representación de Galois $\bar{\rho}_{E,p}$ asociada a los puntos de $p-$torsión. El tercer paso es aplicar el teorema de modularidad a E para obtener una forma modular f de peso 2 cuya representación de Galois asociada ρ_f satisface $\bar{\rho}_f \cong \bar{\rho}_{E,p}$ y por lo tanto cumple las mismas propiedades de ramificación. El último paso es aplicar un teorema de Ribet a la representación $\bar{\rho}_f$ para reducir el nivel de la forma modular f a 2, es decir encontramos una forma modular $g \in S_2(\Gamma_0(2)) \subset S_2(\Gamma(2))$ tal que $\bar{\rho}_{E,p} \cong \bar{\rho}_f \cong \bar{\rho}_g$. Esto produce una contradicción porque el espacio de formas modulares de peso 2 y nivel 2 es de dimensión 0.

Enunciamos estos cuatro pasos en los siguientes tres teoremas:

Teorema 6.5.3. *(Serre) Sea $E/\mathbb{Q}$ la curva de Frey asociada a una solución no trivial a la ecuación de Fermat $x^p + y^p + z^p = 0$. La representación de Galois $\bar{\rho}_{E,p}$ asociada a los puntos de $p-$torsión es irreducible, impar y además cumple las siguientes propiedades de ramificación:*

I) *$\bar{\rho}_{E,p}$ es no ramificada en todo primo q tal que $q \nmid 2p$.*

II) *$\bar{\rho}_{E,p}$ es plana en p.*

Teorema 6.5.4. *(Wiles) Toda curva elíptica $E/\mathbb{Q}$ semiestable es modular. En particular, existe $f \in S_2^{\text{new}}(\Gamma_0(N))$ tal que $\bar{\rho}_{E,p} \cong \bar{\rho}_f$ donde ρ_f es la representación de Galois asociada a f por la teoría de Eichler-Shimura (cf. teorema 5.3.1).*

Teorema 6.5.5. *(Ribet) Sea F un campo finito de característica $\ell > 2$ y sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$ una representación de Galois modular de nivel N y de peso 2, i.e. existe $f \in S_2^{\text{new}}(\Gamma_0(N))$ tal que $\rho \cong \bar{\rho}_f$. Sea q un divisor primo impar exacto de N (i.e. $q \mid N$ pero $q^2 \nmid N$). Entonces:*

$$\rho \text{ es no ramificada o plana en } q \quad \Longrightarrow \quad \rho \text{ es modular de nivel } \frac{N}{q}.$$

Con estos tres teoremas, la prueba del último teorema de Fermat es sencilla:

Demostración. (del teorema 6.5.2) Supongamos por contradicción que existe una solución no trivial (a, b, c) a la ecuación de Fermat $x^p + y^p + z^p = 0$ y además supongamos que a, b y c cumplen las condiciones *. Entonces la curva de Frey $E/\mathbb{Q}$ asociada es semiestable con conductor N par (gracias a que $2 \mid b$). Por el teorema 6.5.4 existe una forma primitiva $f \in S_2^{\text{new}}(\Gamma_0(N))$ tal que $\bar{\rho}_{E,p} \cong \bar{\rho}_f$.

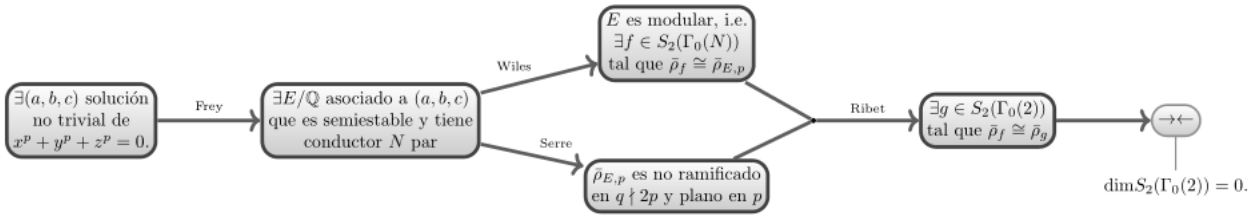
Por otro lado, como E es semiestable, su conductor N es libre de cuadrados (cf. la nota después de la definición 2.5.11) y por lo tanto todo divisor primo q de N es un divisor exacto; escribimos $N = 2q_1 \cdots q_n$ como su producto en primos donde las q_i son impares. Ahora aplicamos el teorema 6.5.3 a $\rho = \bar{\rho}_f$ y a $q = q_1$. Si $q_1 = p$, entonces el teorema 6.5.3.ii nos dice que $\bar{\rho}_f (\cong \bar{\rho}_{E,p})$ es plana en q_1; si $q_1 \neq p$, entonces el teorema 6.5.3.i dice que $\bar{\rho}_f$ es no ramificada en q. De todas maneras podemos aplicar el teorema 6.5.5 para concluir que $\bar{\rho}_f$ es modular de nivel $N/q_1 = q_2 \cdots q_n$, es decir existe $g_1 \in S_2^{\text{new}}(\Gamma_0(2q_2 \cdots q_n))$ tal que $\bar{\rho}_f \cong \bar{\rho}_{g_1}$.

Ahora repetimos este proceso para $\rho = \bar{\rho}_{g_1}$ y $q = q_2$ para obtener una forma primitiva $g_2 \in S_2^{\text{new}}(\Gamma_0(2q_3 \cdots q_n))$ tal que $\bar{\rho}_f \cong \bar{\rho}_{g_1} \cong \bar{\rho}_{g_2}$. Si en total hacemos esto n veces (i.e. la cantidad de divisores primos impares de N) obtenemos una forma primitiva $g_n \in S_2^{\text{new}}(\Gamma_0(2))$ tal que $\bar{\rho}_{E,p} \cong \bar{\rho}_f \cong \bar{\rho}_{g_n}$.

Sabemos que $S_2(\Gamma_0(2)) \subset S_2(\Gamma(2))$ que es de dimensión 0 por ser igual al género de la curva modular $X(2)$ que es de género 0 (cf. el ejemplo 3.3.7 después de la proposición 3.3.6), por lo tanto

$g_n = 0$ lo cual es una contradicción porque $\bar{\rho}_{E,p}$ es una representación no trivial. Por lo tanto una solución no trivial a la ecuación de Fermat no puede existir. □

La prueba del último teorema de Fermat se puede resumir en el siguiente diagrama:



Capítulo 7

Algoritmos y cálculos

Invariantes de curvas elípticas

Ecuaciones de Weierstrass

Primero definimos los coeficientes de una ecuación general de Weierstrass de varias curvas elípticas de interés:

```
In[1]:= X015 = {1, 1, 1, -10, -10};
        isogX015 = {1, 1, 1, 0, 0};
        E50 = {1, 0, 1, -1, -2};
        F50 = {1, 0, 1, -126, -552};
        G50 = {1, 0, 1, -76, 298};
        H50 = {1, 0, 1, 549, -2202};
        clase50 = {E50, F50, G50, H50};
```

Los coeficientes de Weiestrass de una curva de Frey asociada a la terna $A + B + C = 0$ son

```
In[8]:= frey[A_, B_, C_] := {0, B - A, 0, -A B, 0}
```

```
In[9]:= Expand[x (x - A) (x + B)]
```

$$\text{Out[9]}= -A\,B\,x - A\,x^2 + B\,x^2 + x^3$$

La curva elíptica genérica con invariante $j \neq 0, 1728$ es

```
In[10]:= Ej[j_] := {1, 0, 0, -36/(j - 1728), -1/(j - 1728)}
```

Luego definimos la ecuación de Weierstrass con coeficientes $(a_1, a_2, a_3, a_4, a_6)$ y variables (x, y):

```
In[11]:= F[a_, x_, y_] := y^2 + a[[1]] x y + a[[3]] y - (x^3 + a[[2]] x^2 + a[[4]] x + a[[5]])
```

```
In[12]:= F[E50, x, y]
```

$$\text{Out[12]}= 2 + x - x^3 + y + x\,y + y^2$$

Si en lugar de una lista de coeficientes de Weierstrass tenemos un polinomio, las siguientes funciones recuperan los coeficientes de Weierstrass:

```
In[13]:= a6[f_] := -f /. {x → 0, y → 0}
         a4[f_] := -D[f, x] /. {x → 0, y → 0}
         a3[f_] := D[f, y] /. {x → 0, y → 0}
         a2[f_] := -1/2 D[f, {x, 2}] /. {x → 0, y → 0}
         a1[f_] := D[D[f, x], y] /. {x → 0, y → 0}
```

Hacemos el cambio de variable $y \to \frac{1}{2}(y - a_1 x - a_3)$ para obtener una ecuación de Weierstrass (semi) simplificada:

In[18]:=
```
G[a_, x_, y_] := Expand[4 F[a, x, 1/2 (y - a[[1]] x - a[[3]])]]
```

Para simplificar más la ecuación, hacemos los cambios de variable $x \to (x - 3\,a_1{}^2 - 12\,a_2)$, $y \to \frac{1}{108}\,y$ para obtener la ecuación de Weierstrass simplificada:

In[19]:=
```
H[a_, x_, y_] := Expand[108^2 × G[a, (x - 3 (a[[1]]^2 + 4 a[[2]]))/36, y/108]]
```

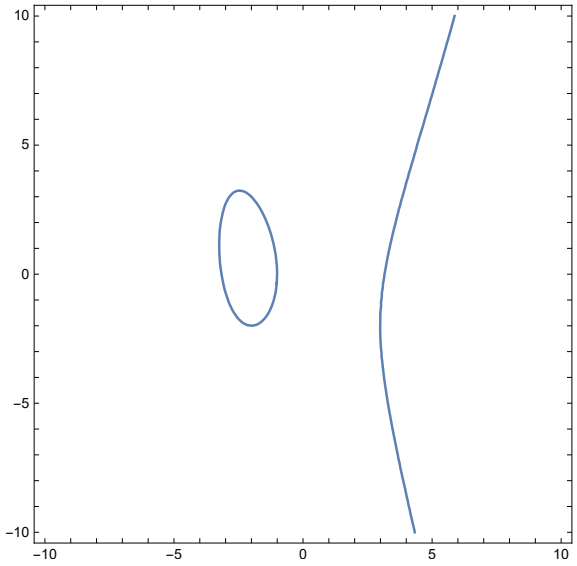
Por ejemplo para $X_0(15)$

In[20]:=
```
{F[X015, x, y], G[X015, x, y], H[X015, x, y]}
```

Out[20]=
$$\left\{10 + 10\,x - x^2 - x^3 + y + x\,y + y^2,\ 39 + 38\,x - 5\,x^2 - 4\,x^3 + y^2,\ 263\,466 + 12\,987\,x - x^3 + y^2\right\}$$

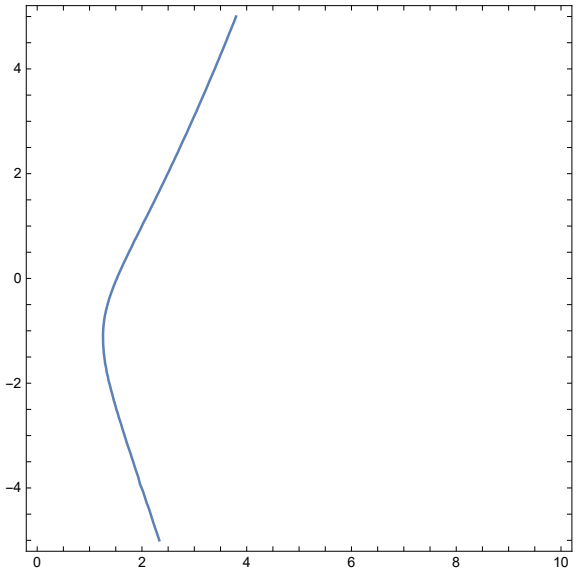
In[21]:=
```
ContourPlot[F[X015, x, y] == 0, {x, -10, 10}, {y, -10, 10}]
```

Out[21]=



In[22]:=
```
ContourPlot[F[E50, x, y] == 0, {x, 0, 10}, {y, -5, 5}]
```

Out[22]=



Los invariantes de una curva con coeficientes “a” son:

In[23]:=
```
b2[a_] := a[[1]]^2 + 4 * a[[2]]
b4[a_] := 2 a[[4]] + a[[1]] × a[[3]]
b6[a_] := a[[3]]^3 + 4 a[[5]]
b8[a_] := a[[1]]^2 × a[[5]] + 4 a[[2]] × a[[5]] -
  a[[1]] × a[[3]] × a[[4]] + a[[2]] × a[[3]]^2 - a[[4]]^2
c4[a_] := b2[a]^2 - 24 b4[a]
c6[a_] := -b2[a]^3 + 36 b2[a] × b4[a] - 216 b6[a]
Δ[a_] := -b2[a]^2 × b8[a] - 8 b4[a]^3 - 27 b6[a]^2 + 9 b2[a] × b4[a] × b6[a]
j[a_] := c4[a]^3 / Δ[a]
```

Por ejemplo:

In[31]:=
```
{j[E50], j[F50], j[G50], j[H50]}
```

Out[31]= $\left\{-\frac{25}{2}, -\frac{349\,938\,025}{8}, -\frac{121\,945}{32}, \frac{46\,969\,655}{32\,768}\right\}$

In[32]:=
```
{Δ[E50], FactorInteger[Δ[E50]]}
```

Out[32]= {−1250, {{−1, 1}, {2, 1}, {5, 4}}}

In[33]:=
```
{Δ[X015], FactorInteger[Δ[X015]]}
```

Out[33]= {50 625, {{3, 4}, {5, 4}}}

In[34]:=
```
c4[E50]
```

Out[34]= 25

In[35]:=
```
{c6[E50], FactorInteger[c6[E50]]}
```
Out[35]=
```
{1475, {{5, 2}, {59, 1}}}
```

In[36]:=
```
Table[{c6[E50] × c6[a], FactorInteger[c6[E50] × c6[a]]}, {a, clase50}]
```
Out[36]=
```
{{2 175 625, {{5, 4}, {59, 2}}}, {689 820 625, {{5, 4}, {13, 1}, {59, 1}, {1439, 1}}},
 {-388 109 375, {{-1, 1}, {5, 6}, {59, 1}, {421, 1}}},
 {2 864 265 625, {{5, 6}, {13, 1}, {59, 1}, {239, 1}}}}
```

Dada una curva con coeficientes “a”, calculamos los coeficientes de la curva que resulta del cambio de variable $x = u^2 x' + r, y = u^3 y' + s x' + t$

In[37]:=
```
cambiovar[a_, u_, r_, s_, t_] := {u^-1 (a[[1]] + 2 s), u^-2 (a[[2]] - s a[[1]] + 3 r - s^2),
  u^-3 (a[[3]] + r a[[1]] + 2 t), u^-4 (a[[4]] - s a[[3]] + 2 r a[[2]] - (t + r s) a[[1]] + 3 r^2 - 2 s t),
  u^-6 (a[[5]] + r a[[4]] + r^2 a[[2]] + r^3 - t a[[3]] - t^2 - r t a[[1]])}
```

Por ejemplo podemos calcular el cambio de variable entre la curva E50, que tiene j –invariante $-25/2$ y la curva elíptica $E_{-25/2}$ genérica del mismo j –invariante:

In[38]:=
```
Solve[E50 == cambiovar[Ej[-25/2], u, r, s, t], {u, r, s, t}]
```
Out[38]=
$$\left\{\left\{u \to -\frac{i}{\sqrt{59}}, r \to -\frac{5}{59}, s \to \frac{1}{2}\left(-1-\frac{i}{\sqrt{59}}\right), t \to \frac{1}{118}\left(5+\frac{i}{\sqrt{59}}\right)\right\},\right.$$
$$\left.\left\{u \to \frac{i}{\sqrt{59}}, r \to -\frac{5}{59}, s \to \frac{1}{2}\left(-1+\frac{i}{\sqrt{59}}\right), t \to \frac{1}{118}\left(5-\frac{i}{\sqrt{59}}\right)\right\}\right\}$$

In[39]:=
```
Solve[E50 == cambiovar[{0, 0, 0, -675, -79650}, u, r, s, t], {u, r, s, t}]
```
Out[39]=
```
{{u → -6, r → 3, s → -3, t → -108}, {u → 6, r → 3, s → 3, t → 108}}
```

Hacemos el mismo cálculo para todas las curvas en “clase50”, pero aquí solamente tomamos una solución y solamente el valor del parámetro u:

In[40]:=
```
MatrixForm[Table[
  {H[a, x, y], First[Flatten[Solve[a == cambiovar[Ej[j[a]], u, r, s, t], {u, r, s, t}]]]},
  {a, clase50}]]
```
Out[40]//MatrixForm=
$$\begin{pmatrix} 79\,650 + 675\,x - x^3 + y^2 & u \to -\frac{i}{\sqrt{59}} \\ 25\,254\,450 + 162\,675\,x - x^3 + y^2 & u \to -i\sqrt{\frac{241}{18\,707}} \\ -14\,208\,750 + 97\,875\,x - x^3 + y^2 & u \to -\sqrt{\frac{29}{2105}} \\ 104\,861\,250 - 712\,125\,x - x^3 + y^2 & u \to -\sqrt{\frac{211}{15\,535}} \end{pmatrix}$$

Reducción módulo p

Primero definimos una función que nos dice si los coeficientes de Weierstrass “a” determinan una

curva no-singular (i.e. $\Delta \neq 0$) y si es singular nos dice si tiene un nodo (i.e. $\Delta = 0$ y $c_4 \neq 0$) o una cúspide (i.e. $\Delta = 0$ y $c_4 = 0$):

In[41]:=
```
suave[a_] := If[! Δ[a] == 0, "es suave", If[c4[a] == 0, "tiene una cúspide", "tiene un nodo"]]
```

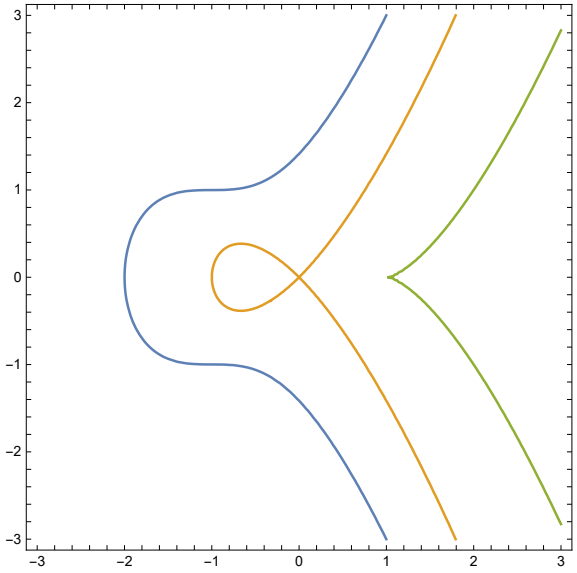
Por ejemplo para las curvas $y^2 = x^3 + x^2$, $y^2 = (x-1)^3$ y $y^2 = (x+1)^3 + 1$ tenemos respectivamente

In[42]:=
```
Map[suave, {{0, 3, 0, 3, 2}, {0, 1, 0, 0, 0}, {0, -3, 0, 3, -1}}]
```

Out[42]=
```
{es suave, tiene un nodo, tiene una cúspide}
```

In[43]:=
```
ContourPlot[{-1 - (x + 1)^3 + y^2 == 0, -x^2 - x^3 + y^2 == 0, 1 - 3 x + 3 x^2 - x^3 + y^2 == 0},
 {x, -3, 3}, {y, -3, 3}]
```

Out[43]=



Similarmente definimos una función si nos dice si cierta curva con coeficientes de Weierstrass "a" tiene reducción buena o mala módulo un primo p y si tiene mala reducción nos dice el tipo de reducción (i.e. multiplicativa o aditiva):

In[44]:=
```
redmodp[a_, p_] :=
 If[! Mod[Δ[a], p] == 0, "tiene buena reducción módulo p", If[Mod[c4[a], p] == 0,
   "tiene reducción aditiva módulo p", "tiene reducción multiplicativa módulo p"]]
```

In[45]:=
```
redmodp[X015, 2]
```

Out[45]=
```
tiene buena reducción módulo p
```

In[46]:=
```
redmodp[frey[2, 3, -5], 2]
```

Out[46]=
```
tiene reducción aditiva módulo p
```

Ahora calculamos soluciones en $\mathbb{F}_p$:

```
In[47]:= Solve[F[X015, x, y] == 0, {x, y}, Modulus → 7]
Out[47]= {{x → 1, y → 1}, {x → 1, y → 4}, {x → 2, y → 2},
  {x → 3, y → 5}, {x → 5, y → 3}, {x → 5, y → 5}, {x → 6, y → 0}}

In[48]:= Solve[F[X015, x, y] == 0, {x, y}, Modulus → 2]
Out[48]= {{x → 0, y → 0}, {x → 0, y → 1}, {x → 1, y → 0}}
```

Con esto podemos calcular el conductor de una curva elíptica dada por unos coeficientes "a". Primero definimos un exponente que codifica la información de la reducción módulo p (para característica $\neq 2, 3$):

```
In[49]:= redexp[a_, p_] := If[! Mod[Δ[a], p] == 0, 0, If[Mod[c4[a], p] == 0, 2, 1]]

In[50]:= redexp[frey[2, 3, -5], 2]
Out[50]= 2
```

Definimos el conductor de una curva dada por coeficientes "a"

```
In[51]:= cond[a_] := Product[p^(redexp[a, p]), {p, Select[Divisors[Δ[a]], PrimeQ]}]

In[52]:= cond[X015]
Out[52]= 15

In[53]:= cond[E50]
Out[53]= 50
```

Suma de E

Para calcular la suma de dos puntos $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$, primero definimos las contantes λ y μ asociadas a dos puntos:

```
In[54]:= λ[a_, u_, v_] :=
  If[u[[1]] == v[[1]], (3 u[[1]]^2 + 2 a[[2]] * u[[1]] + a[[4]] - a[[1]] * u[[2]]) /
    (2 u[[2]] + a[[1]] * u[[1]] + a[[3]]), (v[[2]] - u[[2]]) / (v[[1]] - u[[1]])]
 μ[a_, u_, v_] := If[u[[1]] == v[[1]],
    (-u[[1]]^3 + a[[4]] * u[[1]] + 2 a[[5]] - a[[3]] * u[[2]]) /
     (2 u[[2]] + a[[1]] * u[[1]] + a[[3]]), (u[[2]] * v[[1]] - u[[1]] * v[[2]]) / (v[[1]] - u[[1]])]
```

La suma $P_1 + P_2$ tiene coordenadas:

```
In[56]:= sumax[a_, u_, v_] := (λ[a, u, v])^2 + a[[1]] * λ[a, u, v] - a[[2]] - u[[1]] - v[[1]]
 sumay[a_, u_, v_] := -(λ[a, u, v] + a[[1]]) * sumax[a, u, v] - μ[a, u, v] - a[[3]]
 suma[a_, u_, v_] :=
  If[Simplify[u[[1]] - v[[1]]] == 0 && Simplify[u[[2]] + v[[2]] + a[[1]] * v[[1]] + a[[3]]] == 0,
   "O", {sumax[a, u, v], sumay[a, u, v]}]
```

Por ejemplo, sobre $X_0(15)$, tenemos $(-1, 0) + (8, 18) =$

In[59]:=
```
suma[X015, {-1, 0}, {8, 18}]
```
Out[59]=
```
{-2, 3}
```

La fórmula de duplicación es:

In[60]:=
```
dupx[a_, u_] := (u[[1]]^4 - b4[a] * u[[1]]^2 - 2 b6[a] * u[[1]] - b8[a]) /
  (4 u[[1]]^3 + b2[a] * u[[1]]^2 + 2 b4[a] * u[[1]] + b6[a])
dupy[a_, u_] :=
 1/2 ((2 * u[[1]]^6 + b2[a] * u[[1]]^5 + 5 b4[a] * u[[1]]^4 + 10 b6[a] * u[[1]]^3 + 10 b8[a] * u[[1]]^2 +
       (b2[a] * b8[a] - b4[a] * b6[a]) * u[[1]] + b4[a] * b8[a] - b6[a]^2) /
     (2 * u[[2]] + a[[1]] * u[[1]] + a[[3]])^3 - a[[3]] - a[[1]] * dupx[a, u])
dupli[a_, u_] := {dupx[a, u], dupy[a, u]}
```

In[63]:=
```
dupli[X015, {8, 18}]
```
Out[63]=
```
{3, -2}
```

La inversión de un punto es fácil de definir:

In[64]:=
```
inv[a_, u_] := {u[[1]], -u[[2]] - a[[1]] * u[[1]] - a[[3]]}
```

In[65]:=
```
inv[X015, {-2, 3}]
```
Out[65]=
```
{-2, -2}
```

Puntos de Torsión

Aquí usamos el teorema de Lutz-Nagell para encontrar los puntos de torsión de curvas elípticas cuyas ecuaciones simplificadas de Weierstrass tienen coeficientes enteros. Primero vemos qué puntos son de orden 2, i.e. los puntos (x, y) donde $y = 0$. Los enlistamos con la función "tor2" que toma como argumento una lista de coeficientes de Weierstrass "a":

In[66]:=
```
tor2[a_] :=
 Table[{x, 0}, {x, Map[Last, Flatten[Solve[H[a, x, 0] == 0, x, Integers] /. Rule → List, 1]]}]
```

In[67]:=
```
tor2[X015]
```
Out[67]=
```
{{-102, 0}, {-21, 0}, {123, 0}}
```

Después buscamos soluciones a la ecuación de Weierstrass con $y^2 \mid D$ donde D es la constante

In[68]:=
```
d[a_] := 4 * (-D[H[a, x, 0], x] /. x → 0)^3 + 27 (H[a, 0, 0])^2
```

In[69]:=
```
{d[X015], FactorInteger[d[X015]]}
```
Out[69]=
```
{-6 887 475 360 000, {{-1, 1}, {2, 8}, {3, 16}, {5, 4}}}
```

Tomamos todos los divisores, positivos y negativos, cuyos cuadrados dividen a la constante D asociada a la ecuación con coeficientes "a":

In[70]:=
```
divcuad[a_] := Select[Union[Divisors[d[a]], -Divisors[d[a]]], Divisible[d[a], #^2] &]
```

Para cada tal divisor y_0, resolvemos la ecuación de Weierstrass para encontrar coordenadas x asociadas a y_0. Juntamos estas soluciones al conjunto de torsion 2 y obtenemos todos los elementos no triviales del grupo de torsión de la curva con coeficientes "a"

```
In[71]:= torsim[a_] := Table[
           {Last[Flatten[Solve[H[a, x, k] == 0, x, Integers] /. Rule → List]], k},
           {k, Select[divcuad[a], Length[Solve[H[a, x, #] == 0, x, Integers]] > 0 &]}
         ] ⋃ tor2[a]
```

Cambiamos de variable a la ecuación general de Weierstrass:

```
In[72]:= tor[a_] :=
          Table[{(p[[1]] - 3 b2[a])/36, 1/2 (p[[2]]/108 - a[[1]] (p[[1]] - 3 b2[a])/36 - a[[3]])}, {p, torsim[a]}]
```

```
In[73]:= torsim[X015]
Out[73]= {{-102, 0}, {-57, -540}, {-57, 540}, {-21, 0}, {123, 0}, {303, -4860}, {303, 4860}}
```

```
In[74]:= tor[X015]
Out[74]= {{-13/4, 9/8}, {-2, -2}, {-2, 3}, {-1, 0}, {3, -2}, {8, -27}, {8, 18}}
```

Rango

Definimos ecuaciones de la forma $y^2 = x^3 + a\,x^2 + b\,x$:

```
In[75]:= R[{a_, b_}, x_, y_] := y^2 - (x^3 + a x^2 + b x)
```

```
In[76]:= R[{-63, 1296}, x, y]
Out[76]= -1296 x + 63 x^2 - x^3 + y^2
```

Definimos div(b) como el conjunto de divisores positivos y negativos de b.

```
In[77]:= div[b_] := Union[Divisors[b], -Divisors[b]]
```

Como solamente necesitamos el conjunto de divisores módulo $\mathbb{Q}^{*2}$, eliminamos la parte cuadrática de la factorización de los divisores con la función "librecuad" :

```
In[78]:= librecuad[δ_] := δ * Max[Select[div[δ], Divisible[δ, #^2] &]]^-2
```

Aplicamos esta función al conjunto de divisores de b para obtener las clases módulo $\mathbb{Q}^{*2}$ de los divisores de b:

```
In[79]:= divmod[b_] := Union[Map[librecuad, div[b]]]
```

```
In[80]:= {div[16], divmod[16]}
Out[80]= {{-16, -8, -4, -2, -1, 1, 2, 4, 8, 16}, {-2, -1, 1, 2}}
```

Para cada divisor δ de b definimos el polinomio homogéneo F_δ que define a la ecuación diofantina $x^2 = F_\delta(Y, Z)$:

In[81]:=
```
Fδ[δ_, {a_, b_}, y_, z_] := δ y^4 + a y^2 z^2 + b/δ z^4
```

Dado un divisor δ definimos la siguiente función para verificar si $x^2 = F_\delta(Y, Z)$ tiene una solución en una lista "li(m)" de ternas (X_0, Y_0, Z_0) donde $0 \leq X_0, Y_0, Z_0 \leq m$ y $Y_0 \neq 0$:

In[82]:=
```
posiblesol[δ_, {a_, b_}, t_] :=
 Select[Table[{v, v[[1]]^2 - Fδ[δ, {a, b}, v[[2]], v[[3]]]}, {v, t}], Last[#] == 0 &]
li[m_] := Select[Tuples[Range[0, m, 1], 3], ! #[[2]] == 0 &]
```

Posibles soluciones para a las ecuaciones diofantinas asociadas a cada divisor δ de la curva $y^2 = x^3 - 7x^2 + 16x$ y la curva $y^2 = x^3 + 14x^2 - 15x$

In[84]:=
```
MatrixForm[Table[{δ, posiblesol[δ, {-7, 16}, li[3]]}, {δ, divmod[16]}]]
```

Out[84]//MatrixForm=

$$\begin{pmatrix} -2 & \{\} \\ -1 & \{\} \\ 1 & \{\{\{1, 1, 0\}, 0\}, \{\{2, 2, 1\}, 0\}\} \\ 2 & \{\} \end{pmatrix}$$

In[85]:=
```
MatrixForm[Table[{δ, posiblesol[δ, {14, -15}, li[5]]}, {δ, divmod[15]}]]
```

Out[85]//MatrixForm=

$$\begin{pmatrix} -15 & \{\{\{0, 1, 1\}, 0\}, \{\{0, 2, 2\}, 0\}, \{\{0, 3, 3\}, 0\}, \{\{0, 4, 4\}, 0\}, \{\{0, 5, 5\}, \\ -5 & \{\} \\ -3 & \{\{\{4, 1, 1\}, 0\}\} \\ -1 & \{\} \\ 1 & \{\{\{0, 1, 1\}, 0\}, \{\{0, 2, 2\}, 0\}, \{\{0, 3, 3\}, 0\}, \{\{0, 4, 4\}, 0\}, \{\{0, 5, 5\}, 0\}, \{\{1, 1, 0\}, \\ 3 & \{\} \\ 5 & \{\{\{4, 1, 1\}, 0\}\} \\ 15 & \{\} \end{pmatrix}$$

$X_0(15)$

La curva modular $X_0(15)$ es elíptica, de rango 0 con 8 puntos racionales.

In[86]:=
```
F[X015, x, y]
```

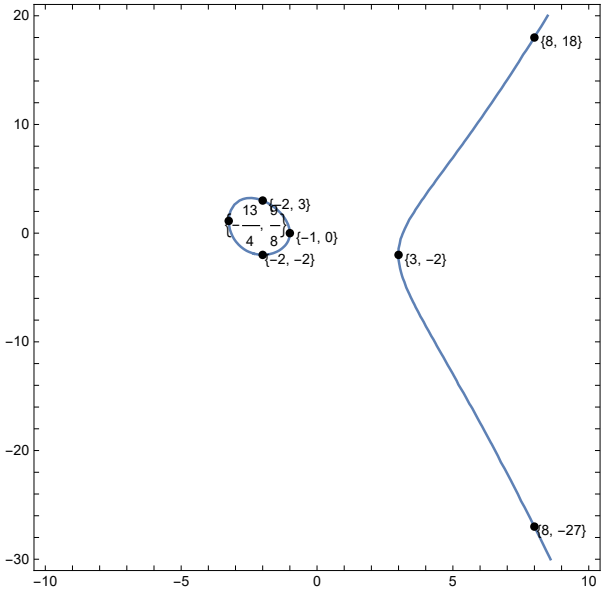
Out[86]=
$$10 + 10\,x - x^2 - x^3 + y + x\,y + y^2$$

In[87]:=
```
tor[X015]
```

Out[87]=
$$\left\{\left\{-\frac{13}{4}, \frac{9}{8}\right\}, \{-2, -2\}, \{-2, 3\}, \{-1, 0\}, \{3, -2\}, \{8, -27\}, \{8, 18\}\right\}$$

In[88]:=
```
Show[
 ContourPlot[F[X015, x, y] == 0, {x, -10, 10}, {y, -30, 20}],
 Table[Graphics[{PointSize[0.015], Inset[p, p + {+1, -.5}], Point[p]}], {p, tor[X015]}]
]
```

Out[88]=



Si $x, y \in \mathbb{Q}(X_0(15))$ son funciones meromorfas que satisfacen la ecuación de Weierstrass, tenemos que $\mathbb{Q}(x, y) = \mathbb{Q}(X_0(15)) = \mathbb{Q}(j, j_N)$. Por lo tanto existen dos polinomios $P, Q \in \mathbb{Q}[s, t]$ tales que $j = P(x, y)/Q(x, y)$. Esta relación la calculamos con el método de Fricke:

Aplica la siguiente transformación racional para cambiar (x, y) a (τ, σ) con

In[89]:=
```
τσ[{x_, y_}] := {(2 y + x + 46)/(2 (x - 8)) + 5/2, ((2 y + x + 46)/(2 (x - 8)))^2 - 2 (x - 8) - 101/4}
```

In[•]:=
```
Map[τσ, tor[X015]]
```

Out[•]=
```
{{1/2, 5/4}, {1/2, -5/4}, {0, 1}, {0, -1}, {-2, 5},
 {Indeterminate, Indeterminate}, {ComplexInfinity, ComplexInfinity}}
```

Para calcular la relación $j = P(\tau, \sigma)/Q(\tau, \sigma)$ usamos la fórmula (9) p.440 de [Fri22] y la fórmula (13) pg.393 (nota: la fórmula 13 depende de otra τ, que llamamos "$\tau 5$" aquí).

In[90]:=
```
τ5[{τ_, σ_}] := (τ^4 - 9 τ^3 - 9 τ - 1 - σ (τ^2 - 4 τ - 1))/(2 τ)
```

In[91]:=
```
jfricke[{τ_, σ_}] := ((τ5[{τ, σ}])^2 + 10 τ5[{τ, σ}] + 5)^3/(τ5[{τ, σ}])
```

Por lo tanto si componemos "jfricke" con "$\tau\sigma$" obtenemos la relación general de j como función

racional de x y y:

In[92]:=
```
Simplify[jfricke[τσ[{x, y}]]]
```

Out[92]=
$$-\left(\left(-179+16\,x^4-16\,x^3\,(-6+y)-124\,y-14\,y^2-4\,y^3+y^4-4\,x^2\left(11+8\,y+y^2\right)+4\,x\left(-96-17\,y-8\,y^2+y^3\right)\right)^3\Big/\left(\left(3+3\,x+y\right)^5\left(14+4\,x^2+x\left(27-2\,y\right)+7\,y-y^2\right)\right)\right)$$

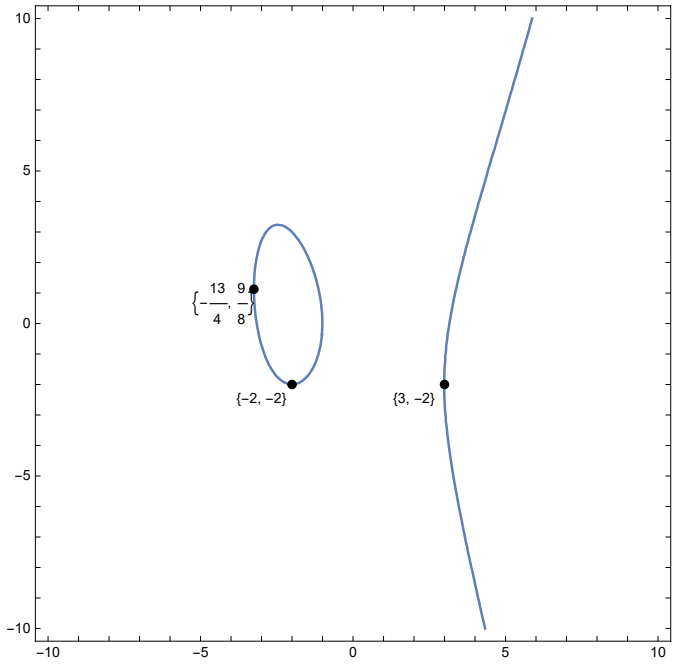
La transformación que toma un punto racional en $X_0(15)$ con coordenadas en la ecuación $10+10\,x-x^2-x^3+y+x\,y+y^2=0$ y calcula la primera coordenada del punto racional correspondiente en el modelo racional $X_0{}^{\mathbb{Q}}(15)$, i.e. j del punto $(j,\ j_{15})$ sobre la curva definida por el polinomio modular Φ_{15}.

In[93]:=
```
jpunto[{x_, y_}] := jfricke[τσ[{x, y}]]
```

Los cuatro “Indeterminate” corresponden a las cuatro cúspides de $X_0(15)$.

In[94]:=
```
Show[
 ContourPlot[F[X015, x, y] == 0, {x, -10, 10}, {y, -10, 10}],
 Table[Graphics[{PointSize[0.015], Inset[p, p + {-1, -.5}], Point[p]}],
  {p, Select[tor[X015], Element[jpunto[#], Rationals] &]}]
]
```

Out[94]=



Para calcular “jpunto” en el neutro O de la curva elíptica $10+10\,x-x^2-x^3+y+x\,y+y^2$

In[95]:=
```
valoresj = {-25/2, -349938025/8, -121945/32, 46969655/32768}
```
Out[95]=
$$\left\{-\frac{25}{2}, -\frac{349\,938\,025}{8}, -\frac{121\,945}{32}, \frac{46\,969\,655}{32\,768}\right\}$$

Una vez que tenemos los j –invariantes formamos las curvas genéricas de invariante j:

In[96]:=
```
Table[F[Ej[J], x, y], {J, valoresj}]
```
Out[96]=
$$\left\{-\frac{2}{3481}-\frac{72\,x}{3481}-x^3+x\,y+y^2, -\frac{8}{349\,951\,849}-\frac{288\,x}{349\,951\,849}-x^3+x\,y+y^2,\right.$$
$$\left.-\frac{32}{177\,241}-\frac{1152\,x}{177\,241}-x^3+x\,y+y^2, -\frac{32\,768}{9\,653\,449}-\frac{1\,179\,648\,x}{9\,653\,449}-x^3+x\,y+y^2\right\}$$

Obtenemos la ecuación de Weirestrass simplificada de cada uno:

In[97]:=
```
listaeqsim = Table[H[Ej[J], x, y], {J, valoresj}]
```
Out[97]=
$$\left\{-\frac{1350}{3481}+\frac{675\,x}{3481}-x^3+y^2, -\frac{18\,896\,653\,350}{349\,951\,849}+\frac{9\,448\,326\,675\,x}{349\,951\,849}-x^3+y^2,\right.$$
$$\left.-\frac{6\,585\,030}{177\,241}+\frac{3\,292\,515\,x}{177\,241}-x^3+y^2, \frac{2\,536\,361\,370}{9\,653\,449}-\frac{1\,268\,180\,685\,x}{9\,653\,449}-x^3+y^2\right\}$$

Para cada j escribimos la $u \in \overline{\mathbb{Q}}$ tal que el cambio de variable $x = u^2\,x'$, $y = u^3\,y'$ transforma la ecuación simplificada de E_j a una ecuación de Weierstrass simplificada con los coeficientes enteros más pequeños posibles.

In[98]:=
```
Table[
 {valoresj[[f]], Solve[
   {0, 0, 0, a4[H[clase50[[f]], x, y]], a6[H[clase50[[f]], x, y]]} ==
    cambiovar[{0, 0, 0, a4[listaeqsim[[f]]], a6[listaeqsim[[f]]]}, u, r, s, t],
   {u, r, s, t}]},
 {f, 1, Length[listaeqsim]}]
```
Out[98]=
$$\left\{\left\{-\frac{25}{2}, \left\{\left\{u \to -\frac{i}{\sqrt{59}}, r \to 0, s \to 0, t \to 0\right\}, \left\{u \to \frac{i}{\sqrt{59}}, r \to 0, s \to 0, t \to 0\right\}\right\}\right\}, \left\{-\frac{349\,938\,025}{8},\right.\right.$$
$$\left.\left\{\left\{u \to -i\sqrt{\frac{241}{18\,707}}, r \to 0, s \to 0, t \to 0\right\}, \left\{u \to i\sqrt{\frac{241}{18\,707}}, r \to 0, s \to 0, t \to 0\right\}\right\}\right\},$$
$$\left\{-\frac{121\,945}{32}, \left\{\left\{u \to -\sqrt{\frac{29}{2105}}, r \to 0, s \to 0, t \to 0\right\}, \left\{u \to \sqrt{\frac{29}{2105}}, r \to 0, s \to 0, t \to 0\right\}\right\}\right\},$$
$$\left.\left\{\frac{46\,969\,655}{32\,768}, \left\{\left\{u \to -\sqrt{\frac{211}{15\,535}}, r \to 0, s \to 0, t \to 0\right\}, \left\{u \to \sqrt{\frac{211}{15\,535}}, r \to 0, s \to 0, t \to 0\right\}\right\}\right\}\right\}$$

Hacemos los cambios de variable

In[99]:=
```
MatrixForm[{listaeqsim[[1]] → F[
    cambiovar[{0, 0, 0, a4[listaeqsim[[1]]], a6[listaeqsim[[1]]]}, i/Sqrt[59], 0, 0, 0], x, y],
 listaeqsim[[2]] → F[cambiovar[{0, 0, 0, a4[listaeqsim[[2]]], a6[listaeqsim[[2]]]},
   i Sqrt[241/18707], 0, 0, 0], x, y],
 listaeqsim[[3]] → F[cambiovar[{0, 0, 0, a4[listaeqsim[[3]]], a6[listaeqsim[[3]]]},
   Sqrt[29/2105], 0, 0, 0], x, y], listaeqsim[[4]] → F[cambiovar[
   {0, 0, 0, a4[listaeqsim[[4]]], a6[listaeqsim[[4]]]}, Sqrt[211/15535], 0, 0, 0], x, y]}]
```

Out[99]//MatrixForm=

$$\begin{pmatrix} -\frac{1350}{3481}+\frac{675\,x}{3481}-x^3+y^2 \to 79\,650+675\,x-x^3+y^2 \\ -\frac{18\,896\,653\,350}{349\,951\,849}+\frac{9\,448\,326\,675\,x}{349\,951\,849}-x^3+y^2 \to 25\,254\,450+162\,675\,x-x^3+y^2 \\ -\frac{6\,585\,030}{177\,241}+\frac{3\,292\,515\,x}{177\,241}-x^3+y^2 \to -14\,208\,750+97\,875\,x-x^3+y^2 \\ \frac{2\,536\,361\,370}{9\,653\,449}-\frac{1\,268\,180\,685\,x}{9\,653\,449}-x^3+y^2 \to 104\,861\,250-712\,125\,x-x^3+y^2 \end{pmatrix}$$

Son iguales a las ecuaciones simplificadas de las cuatro curvas E50, F50, G50 y H50:

In[100]:=
```
MatrixForm[Table[H[a, x, y], {a, clase50}]]
```

Out[100]//MatrixForm=

$$\begin{pmatrix} 79\,650+675\,x-x^3+y^2 \\ 25\,254\,450+162\,675\,x-x^3+y^2 \\ -14\,208\,750+97\,875\,x-x^3+y^2 \\ 104\,861\,250-712\,125\,x-x^3+y^2 \end{pmatrix}$$

Ninguna de estas curvas es semiestable en 5 porque todas se reducen a $y^2 \equiv x^3 \pmod 5$ que tiene reducción aditiva.

In[101]:=
```
Table[redmodp[a, 5], {a, clase50}]
```

Out[101]=
```
{tiene reducción aditiva módulo p, tiene reducción aditiva módulo p,
 tiene reducción aditiva módulo p, tiene reducción aditiva módulo p}
```

La curva de Klein

Definimos la la curva $W/\mathbb{Q}(u)$ con coeficientes

In[102]:=
```
a4u[u_] := -(u^20 - 228 u^15 + 494 u^10 + 228 u^5 + 1)/48
a6u[u_] := (u^30 + 522 u^25 - 10005 u^20 - 10005 u^10 - 522 u^5 + 1)/864
W[u_] := {0, 0, 0, a4u[u], a6u[u]}
ζ = e^(2 π i/5);
```

La curva W tiene j –invariante:

In[106]:=
```
Simplify[j[W[u]]]
```

Out[106]=
$$-\frac{\left(1+228\,u^5+494\,u^{10}-228\,u^{15}+u^{20}\right)^3}{u^5\left(-1+11\,u^5+u^{10}\right)^5}$$

In[107]:=
```
J[u_] := j[W[u]]
```

In[108]:=
```
Simplify[J[(a t + to)/(c t + 1)]]
```

Out[108]=
$$\left(1728\,(1+c\,t)^{60}\left(1+\frac{228\,(a\,t+to)^5}{(1+c\,t)^5}+\frac{494\,(a\,t+to)^{10}}{(1+c\,t)^{10}}-\frac{228\,(a\,t+to)^{15}}{(1+c\,t)^{15}}+\frac{(a\,t+to)^{20}}{(1+c\,t)^{20}}\right)^3\right)\Big/$$
$$\Big(\big((1+c\,t)^{20}+228\,(1+c\,t)^{15}\,(a\,t+to)^5+494\,(1+c\,t)^{10}\,(a\,t+to)^{10}-228\,(1+c\,t)^5\,(a\,t+to)^{15}+(a\,t+to)^{20}\big)^3-\big((1+c\,t)^{30}-522\,(1+c\,t)^{25}\,(a\,t+to)^5-10\,005\,(1+c\,t)^{20}\,(a\,t+to)^{10}-10\,005\,(1+c\,t)^{10}\,(a\,t+to)^{20}+522\,(1+c\,t)^5\,(a\,t+to)^{25}+(a\,t+to)^{30}\big)^2\Big)$$

Definimos una versión simplificada de la suma de dos puntos u y v de una curva dada por los coeficientes “a”:

In[109]:=
```
sumasimx[a_, u_, v_] :=
 Simplify[((v[[2]] - u[[2]])/(v[[1]] - u[[1]]))^2 + a[[1]] * ((v[[2]] - u[[2]])/(v[[1]] - u[[1]])) - a[[2]] - u[[1]] - v[[1]]]
sumasimy[a_, u_, v_] := Simplify[-((v[[2]] - u[[2]])/(v[[1]] - u[[1]]) + a[[1]])) * sumasimx[a, u, v] -
   (u[[2]] * v[[1]] - v[[2]] * u[[1]])/(v[[1]] - u[[1]]) - a[[3]]]
sumasim[a_, u_, v_] := {sumasimx[a, u, v], sumasimy[a, u, v]}
```

El punto $P_z = (x_0(z\,u),\, y_0(z\,u)) \in W(\mathbb{Q}(u, z))$ con $z \in \mathbb{C}$ lod definimos:

In[112]:=
```
P[z_, u_] :=
 {1/12 ((z u)^10 + 12 (z u)^8 - 12 (z u)^7 + 24 (z u)^6 + 30 (z u)^5 + 60 (z u)^4 + 36 (z u)^3 + 24 (z u)^2 +
     12 (z u) + 1), 1/2 ((z u)^13 + (z u)^12 + 4 (z u)^11 + 5 (z u)^9 + 6 (z u)^8 +
     21 (z u)^7 + 29 (z u)^6 + 25 (z u)^5 + 15 (z u)^4 + 9 (z u)^3 + 4 (z u)^2 + (z u))}
```

Estaremos interesados en los puntos P_1 y P_ζ. Observe que $5\,P_1 = O$ porque $(2\,(2\,P_1)) + P_1$ es

In[113]:=
```
sumasim[W[u], Simplify[dupli[W[u], Simplify[dupli[W[u], P[1, u]]]]], P[1, u]]
```

Out[113]=
```
{ComplexInfinity, ComplexInfinity}
```

Observe que también $5\,P_\zeta = (2\,(2\,P_\zeta)) + P_\zeta = O$:

In[114]:=
```
sumasim[W[u], Simplify[dupli[W[u], Simplify[dupli[W[u], P[ζ, u]]]]], P[ζ, u]]
```

Out[114]=
```
{ComplexInfinity, ComplexInfinity}
```

Ahora verificamos las siguientes relaciones entre los puntos P_1 y P_ζ. Para esto generamos la lista de

puntos $2\,P_\zeta$, $3\,P_\zeta$, $4\,P_\zeta$, $-2\,P_1$, $-3\,P_1$ respectivamente:

In[115]:=
```
dosPζ = dupli[W[u], P[ζ, u]];
tresPζ = inv[W[u], dosPζ];
cuatroPζ = inv[W[u], P[ζ, u]];
menos2P1 = inv[W[u], dupli[W[u], P[1, u]]];
menos3P1 = dupli[W[u], P[1, u]];
```

Ahora generamos los puntos $2\,P_\zeta - P_1$, $3\,P_\zeta - 2\,P_1$ y $4\,P_\zeta - 3\,P_1$ respectivamente (approx 5min):

In[120]:=
```
σ2P = sumasim[W[u], dosPζ, inv[W[u], P[1, u]]];
σ3P = sumasim[W[u], tresPζ, menos2P1];
σ4P = sumasim[W[u], cuatroPζ, menos3P1];
```

Para el automorfismo $\sigma : \zeta \mapsto \zeta^2$ tenemos que $\sigma \mathrm{P}_\zeta = P(\zeta^2, u) = 2\,P_\zeta - P_1$ (approx. 6 min):

In[123]:=
```
sumasim[W[u], σ2P, inv[W[u], P[ζ^2, u]]]
```

Out[123]=
```
{ComplexInfinity, ComplexInfinity}
```

Para el automorfismo $\sigma : \zeta \mapsto \zeta^4$ tenemos que $\sigma \mathrm{P}_\zeta = P(\zeta^4, u) = 4\,P_\zeta - 3\,P_1$:

In[124]:=
```
sumasim[W[u], σ4P, inv[W[u], P[ζ^4, u]]]
```

Out[124]=
```
{ComplexInfinity, ComplexInfinity}
```

Para el automorfismo $\sigma : \zeta \mapsto \zeta^3$ tenemos que $\sigma \mathrm{P}_\zeta = P(\zeta^3, u) = 3\,P_\zeta - 2\,P_1$:

In[127]:=
```
sumasim[W[u], σ3P, inv[W[u], P[ζ^3, u]]]
```

Out[128]=
```
{ComplexInfinity, ComplexInfinity}
```

Bibliografía

[Ahl79] L. V. Ahlfors. *Complex Analysis*. McGraw-Hill, 1979.

[AL70] A. O. L. Atkin and J. Lehner. Hecke Operators on $\Gamma_0(N)$. *Mathematische Annalen*, pages 185:134–160, 1970.

[AM94] M. F. Atiyah and I.G. Macdonald. *Introduction to Commutative Algebra*. Avalon Publishing, 1994.

[Apo90] T. Apostol. *Modular Functions and Dirichlet Series in Number Theory*. Springer, 1990.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the Modularity of Elliptic Curves Over $\mathbb{Q}$: Wild 3-adic Exercises. *Journal of the American Mathematical Society*, 14, 2001.

[Bum98] D. Bump. *Automorphic Forms and Representations*. Cambridge University Press, 1998.

[Cas49] J. W. S. Cassels. A Note on the Division Values of $s(u)$. *Mathematical Proceedings of the Cambridge Philosophical Society*, 45(2):167–172, 1949.

[Cas67] J. W. S. Cassels. Global Fields. In J. W. S. Cassells and A. Fröhlich, editors, *Algebraic Number Theory*, pages 42–84. London Mathematical Society, 1967.

[Cre97] J. Cremona. *Algorithms for Modular Elliptic Curves*. Springer New York, 1997.

[CWJ06] J. Carlson, A. Wiles, and A. Jaffe. *The Millennium Prize Problems*. Amsns AMS non-series Title Series. American Mathematical Society, 2006.

[Del71] P. Deligne. *Formes modulaires et représentations $\ell-$adiques*. Springer, 1971. en "Lecture Notes in Math", volumen 179, páginas 139-172.

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In Pierre Deligne and Willem Kuijk, editors, *Modular Functions of One Variable II*, pages 143–316. Springer Berlin Heidelberg, 1973.

[DS74] P. Deligne and J.P. Serre. Formes modulaires de poids 1. *Annales scientifiques de L'É.N.S.*, pages 507–530, 1974.

[DS05] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Springer, 2005.

[Eis04] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, 2004.

[Eul70] L. Euler. *Vollständige Anleitung zur Algebra II.* 1770. Aparece como E388 en http://eulerarchive.maa.org/.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inventiones mathematicae*, 73:349–366, 1983.

[FK12] H. M. Farkas and I. Kra. *Riemann Surfaces.* Graduate Texts in Mathematics. Springer New York, 2012.

[Fre86] G. Frey. *Links Between Stable Elliptic Curves and Certain Diophantine Equations.* Saarbrücken : Universität des Saarlandes. Fachbereich Mathematik, 1986.

[Fri22] R. Fricke. *Die elliptischen Funktionen und ihere Anwendungen.* Leipzig, Berlin, B.G. Teubner, 1922.

[Ful08] W. Fulton. *Algebraic Curves: an Introduction to Algebraic Geometry.* Addison-Wesley Pub. Co., 2008.

[Gel97] S. Gelbart. Three lectures on the Modularity of $\bar{\rho}_{E,3}$ and the Langlands Reciprocity Conjecture. In G. Cornell, J.H. Silverman, and G. Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 155–207. Springer New York, 1997.

[Gro72] A. Grothendieck. Modeles de neron et monodromie. In *Groupes de Monodromie en Géométrie Algébrique*, pages 313–523. Springer Berlin Heidelberg, 1972.

[Har77] R. Hartshorne. *Algebraic Geometry.* Springer, 1977.

[Hel75] Y. Hellegouarch. Points d'ordre $2p^h$ sur les courbes elliptiques. *Polska Akademia Nauk. Instytut Matematyczny. Acta Arithmetica*, 26:253–263, 1975.

[Hus04] D. Husemöller. *Elliptic Curves.* Springer, 2004.

[Igu55] J. I. Igusa. Arithmetic Genera of Normal Varieties in an Algebraic Family. *Proceedings of the National Academy of Sciences of the United States of America*, 41(1):34–37, 1955.

[IR90] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer, 1990.

[KKS11] K. Kato, N. Kurokawa, and T. Saito. *Number Theory 2: An introduction to Class Field Theory.* American Mathematical Society, 2011.

[Kle45] F. Klein. *Elementary Mathematics from an Advanced Standpoint. Vol. 1.* Dover Publications, 1945.

[KM85] N. M. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves. (AM-108).* Princeton University Press, 1985.

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

[Lan80] R. P. Langlands. *Base Change for GL(2).* Annals of Mathematics Studies. Princeton University Press, 1980.

[Lan87] S. Lang. *Elliptic Functions*. Graduate texts in mathematics. Springer, 1987.

[LdS97] H. W. Lenstra and B. de Smit. Explicit Construction of Universal Deformation Rings. In G. Cornell, J.H. Silverman, and G. Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 313–326. Springer New York, 1997.

[Lig75] G. Ligozat. *Courbes modulaires de genre 1.* Number 43 in Mémoires de la Société Mathématique de France. Société mathématique de France, 1975.

[Lut37] E. Lutz. Sur l'équation $y^2 = x^3 - ax - b$ dans les corps $p-$adiques. *Journal für die reine und angewandte Mathematik*, 177:238–247, 1937.

[Maz77] B. Mazur. Modular Curves and the Eisenstein Ideal. *Publications Mathématiques de l'IHÉS*, 47:33–186, 1977.

[Mil06] J. S. Milne. *Elliptic Curves*. 2006. Disponible en www.jmilne.org/math/.

[Mil17a] J. S. Milne. *Algebraic Geometry*. 2017. Disponible en www.jmilne.org/math/.

[Mil17b] J. S. Milne. *Modular Functions and Modular Forms*. 2017. Disponible en www.jmilne.org/math/.

[Nag35] T. Nagell. Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre. *Wid. Akad. Skrifter Oslo I*, 1935.

[Neu99] J. Neukirch. *Algebraic Number Theory*. Springer, 1999.

[New56] M. Newman. Construction and Application of a Class of Modular Functions i. *Proc. London Math. Soc.*, pages 334–350, 1956.

[New58] M. Newman. Construction and Application of a Class of Modular Functions ii. *Proc. London Math. Soc.*, pages 373–387, 1958.

[Ram16] S. Ramanujan. On Certain Arithmetical Functions. *Trans. Cambridge Philos. Soc*, 22(9):159–184, 1916.

[Rot95] J.J. Rotman. *An Introduction to the Theory of Groups*. Springer, 1995.

[RS97] K. Rubin and A. Silverberg. Families of Elliptic Curves with Constant Mod p Representations. In J. Coates and S.T. Yau, editors, *Elliptic Curves, Modular Forms & Fermat's Last Theorem*, pages 296–309. International Press, 1997.

[Rub97] K. Rubin. Modularity of Mod 5 Representations. In G. Cornell, J. H. Silverman, and G. Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 463–474. Springer New York, 1997.

[Sai13a] T. Saito. *Fermat's Last Theorem: Basic Tools*. American Mathematical Society, 2013.

[Sai13b] T. Saito. *Fermat's Last Theorem: The Proof*. American Mathematical Society, 2013.

[Sch68] M. Schlessinger. Functors of Artin Rings. *Transactions of the American Mathematical Society*, 130:208–222, 1968.

[SDB65] H.P.F. Swinnerton-Dyer and B.J. Birch. Notes on elliptic curves. ii. *Journal für die reine und angewandte Mathematik*, 218:79–108, 1965.

[Ser73] J.-P. Serre. *A Course in Arithmetic*. Springer, 1973.

[Ser77a] J.-P. Serre. *Linear Representations of Finite Groups*. Springer, 1977.

[Ser77b] J.-P. Serre. *Modular Forms of Weight 1 and Galois Representations*. Academic Press, 1977. en "Algebraic Number Fields", editado por A. Frölich.

[Ser79] J.-P. Serre. *Local Fields*. Springer, 1979.

[Ser87] J.-P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Mathematical Journal*, 54(1):179–230, 1987.

[Ser96] J.-P. Serre. Travaux de Wiles (et Taylor, ...), partie i. In *Séminaire Bourbaki : volume 1994/95, exposés 790-804*, number 237 in Astérisque, pages 319–332. Société mathématique de France, 1996. talk:803.

[Ser72] J-P Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15:259–331, 1971/72.

[Sha86] S. S. Shatz. Group Schemes, Formal Groups, and p-Divisible Groups. In G. Cornell and J. H. Silverman, editors, *Arithmetic Geometry*, pages 29–78. Springer New York, 1986.

[Shi94] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Springer, 1994.

[Sil97] A. Silverberg. Explicit Families of Elliptic Curves with Prescribed Mod n Representations. In G. Cornell, J. H. Silverman, and G. Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 447–461. Springer New York, 1997.

[Sil99] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, 1999.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

[ST09] J.H. Silverman and J.T. Tate. *Rational Points on Elliptic Curves*. Springer, 2009.

[Tat66] J. T. Tate. On the Conjectures of Birch and Swinnerton-Dyer and a Geometric Analog. In *Séminaire Bourbaki : années 1964/65 1965/66, exposés 277-312*, number 9 in Séminaire Bourbaki, pages 415–440. Société mathématique de France, 1966.

[Tat67] J. T. Tate. Global Class Field Theory. In J. W. S. Cassells and A. Fröhlich, editors, *Algebraic Number Theory*, pages 163–203. London Mathematical Society, 1967.

[Tat75] J. T. Tate. Algorithm for determining the Type of a Singular Fiber in an Elliptic Pencil. In Bryan J. Birch and Willem Kuyk, editors, *Modular Functions of One Variable IV*, pages 33–52. Springer Berlin Heidelberg, 1975.

[Tat97] J. T. Tate. Finite Flat Groups Schemes. In G. Cornell, J. H. Silverman, and G. Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 121–154. Springer New York, 1997.

[Tun81] J. Tunnell. Artin's Conjecture for Representations of Octahedral Type. *Bulletin of the American Mathematical Society*, 5:173–175, 1981.

[Vé71] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris*, 273:A238–A241, 1971.

[Wei56] A. Weil. The Field of Definition of a Variety. *American Journal of Mathematics*, 78(3):509–524, 1956.

[Wei74] A. Weil. *Basic Number Theory*. Springer New York, 1974.

[Wei12] A. Weil. *Adeles and Algebraic Groups*. Progress in Mathematics. Birkhäuser Boston, 2012.

[Wil95] A. Wiles. Modular Elliptic Curves and Fermat's Last Theorem. *Annals of Mathematics*, 141:443–551, 1995.