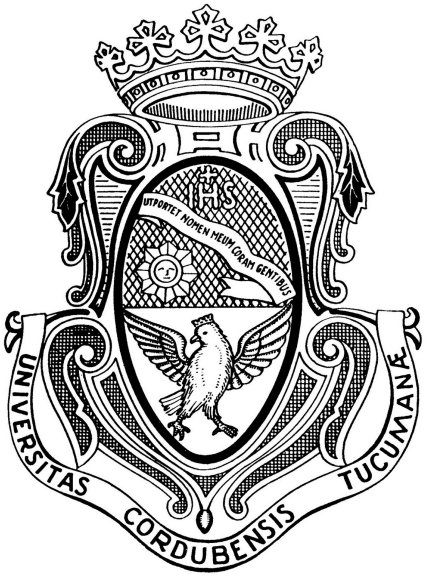
FACULTAD DE MATEMÁTICA, ASTRONOMÍA, FÍSICA y COMPUTACIÓN

- UNIVERSIDAD NACIONAL de CÓRDOBA -



EL ÚLTIMO TEOREMA DE FERMAT

TRABAJO ESPECIAL DE LICENCIATURA EN MATEMÁTICA:

Franco Aníbal Golfieri Madriaga

Dirigido por:

Dr. Ariel Pacetti

CÓRDOBA - ARGENTINA

Clasificación

[11D41] Higher degree equations; Fermat's equation.
[11F11] Holomorphic modular forms of integral weight.
[11F80] Galois representations.
[11G05] Elliptic curves over global fields.
[11G18] Arithmetic aspects of modular and Shimura varieties.

Palabras Claves

- Curvas Elípticas
- Formas Modulares
- L-series
- Representación de Galois
- Modularidad

Resumen

El objetivo del presente trabajo es estudiar la demostración del Último Teorema de Fermat. En la primera parte se hablará acerca de las curvas elípticas y sus propiedades. Se mostrará cómo estas se relacionan a hipotéticas soluciones a la ecuación del Teorema en estudio. Seguido de esto estudiaremos las formas modulares, funciones holomorfas del plano complejo superior que guardan cierta relación con las curvas elípticas.

En la segunda parte se expondrá la relación que existe entre curvas elípticas y formas modulares, relación dada por el Teorema de Eichler-Shimura y la conjetura de Shimura-Taniyama.

Finalizamos juntando todos los resultados previos, junto con el Teorema de Ribet-Mazur y el Teorema de Wiles, para demostrar el Último Teorema de Fermat.

Abstract

The main goal of this work is to study the proof of Fermat's Last Theorem.

In the first part we will study the properties of elliptic curves. It will be shown how these curves are related to hypothetical solutions to Fermat's Last Theorem equation. Following this, we will review modular forms, which are holomorphic functions of the superior complex plane that bear a certain relationship with elliptic curves.

In the following chapters, we shall examine the connection between elliptic curves and modular forms. This relationship will be given by the Eichler-Shimura Theorem and the Shimura-Taniyama Conjecture.

We will finish by putting together all the previous results, conjointly with the Ribet-Mazur Theorem and the Wiles Theorem, to prove Fermat's Last Theorem.

Agradecimientos

Agradecer, principalmente, a mi madre Adriana y a mi padre Claudio por brindarme su total apoyo en estos cinco años y por confiar en mi decisión de viajar a Córdoba para estudiar lo que más me apasionaba. Agradecer, también, a mi padrino Carlos, por sus infinitos consejos y a mi hermana Antonella por estos últimos años de convivencia y por estar presente en los buenos y malos momentos.

Agradecer a la Olimpiada Matemática Argentina por permitirme descubrir y apreciar la matemática desde otro punto de vista, y por haberme incentivado a forjar tan preciadas y especiales amistades. En particular, agradecer a Rosa Mugas, quien me inició en las mismas y quien estimuló mi entusiasmo por la matemática.

Doy gracias a Gustavo y a Luciana por haberme guiado en mi decisión de estudiar la Licenciatura en Matemática, y por haberme mostrado, desde un inicio, lo lindo de la carrera.

Por otro lado, me gustaría agradecer a todos los compañeros que tuve en estos cinco años; sin duda he aprendido algo de cada uno de ellos y han sido un gran apoyo, no solo en lo académico. Desde luego que sin ellos el cursado hubiera sido mucho más difícil y aburrido.

Agradecer a mis amigos, aquellos de toda la vida de San Juan, y a los que fui conociendo en Córdoba. Todos me han acompañado, ya sea a la distancia o desde cerca. Entre estos últimos me gustaría agradecer especialmente a Emiliano y a Héctor por su apoyo incondicional.

Agradezco, también, a todos los profesores que tuve a lo largo de carrera, profesionales que admiro enormemente; me siento privilegiado y ha sido un verdadero placer aprender de ellos. Me gustaría destacar al Dr. Juan Pablo Rossetti, quien me acompañó y ayudó desde el primer año de la carrera, tanto en actividades curriculares como extracurriculares.

Debo agradecer de manera especial y sincera al Dr. Ariel Pacetti, por aceptarme para realizar esta trabajo bajo su dirección. Su apoyo y confianza en mi trabajo y su capacidad para guiar mis ideas ha sido un aporte invaluable. Agradecerle, además, por todas las correcciones que me fue haciendo durante el trabajo, las dudas que me fue resolviendo y los consejos que me fue brindando.

Agradecer, finalmente, a la FAMAF y a la Universidad Nacional de Córdoba por permitir mi desarrollo, como persona y como profesional.

Índice general

Lista de Notación

Capítulo 1

Introducción

1.1. Breve reseña histórica

El último Teorema de Fermat fue originalmente conjeturado por Pierre de Fermat en 1637 en el margen de una copia del libro *Arithmetica*. El teorema decía lo siguiente:

Último Teorema de Fermat. La ecuación $x^n + y^n = z^n$, con $xyz \neq 0$ no tiene soluciones enteras, para $n \geq 3$.

Fermat aseguró tener una demostración del mismo Teorema pero, debido a su extensión, no cabía en el margen del mismo libro donde lo enunció. Citando textualmente:

> *Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet.*
>
> Tengo una demostración verdaderamente maravillosa de esta proposición pero este margen es muy angosto para contenerla.

Con el paso de los años, una gran cantidad de matemáticos intentaron abordar este problema. Dentro de tales matemáticos se encuentran Euler, Sophie Germain, Kummer, Legendre, Abel, Dirichlet y Cauchy. En el presente Capítulo discutiremos los primeros intentos en resolver el presente Teorema, comenzando por los casos $n = 4$ y $n = 3$ resueltos por Fermat y Euler respectivamente. En el capítulo siguiente se discutirá acerca de la solución de Kummer para el caso donde n es un primo regular, es decir primos que no dividen al número de clases del cuerpo ciclotómico respectivo.

Antes de tratar los primeros casos, cabe mencionar la siguiente observación: El Último Teorema de Fermat basta ser probado para los casos $n = 4$ y n primo. En efecto si $n \geq 3$ entonces o bien el único primo que aparece en su factorización es el 2, en cuyo caso será una potencia de 2; o bien n contiene en su factorización un primo $p \neq 2$. En el primer caso n será un múltiplo de 4, es decir $n = 4k$ y por lo tanto el problema $x^n + y^n = z^n$ se reduce al problema $(x^k)^4 + (y^k)^4 = (z^k)^4$; y en el segundo caso, si $p \neq 2$ es un primo que divide a n entonces $n = pk$ y luego el problema $x^n + y^n = z^n$ se reduce al problema $(x^k)^p + (y^k)^p = (z^k)^p$.

Además a la hora de ver si existen soluciones, basta ver el caso en el cual x, y, z sean coprimos dos a dos. En efecto, si existen dos de estos valores que tienen un divisor d en

común, entonces, por la expresión de la ecuación, d también dividirá a la variable restante. Por lo tanto, tomando $d = \text{mcd}(x, y, z) > 1$, reducimos nuestra ecuación $x^n + y^n = z^n$ a la ecuación $(x/d)^n + (y/d)^n = (z/d)^n$ en donde $x/d, y/d$ y z/d son coprimos dos a dos. Una tal solución se dirá que es *primitiva*.

1.2. Caso n=4

Este fue el primer caso que se trató y fue probado por el mismo Fermat. La demostración propuesta por Fermat se basa en el truco del *descenso infinito*. Para la misma se precisará el siguiente lema, el cual caracteriza a las ternas pitagóricas.

Lema 1.2.1. Toda solución entera a la ecuación $x^2 + y^2 = z^2$ donde x, y, z son coprimos dos a dos puede ser escrita en la siguiente forma (con x e y intercambiados de ser necesario)

$$\begin{aligned} \pm x &= r^2 - s^2, \\ \pm y &= 2rs, \\ \pm z &= r^2 + s^2, \end{aligned}$$

donde r y s son coprimos y exactamente uno de ellos es impar.

El resultado que probó Fermat fue el siguiente, el cual implica como corolario el resultado que queremos.

Teorema 1.2.2. No existen soluciones en enteros distintos de cero a la ecuación $x^4 + y^4 = z^2$

Demostración. Supongamos que existen soluciones. Sea (x, y, z) solución en los enteros positivos tal que z es mínimo entre dichas soluciones. Podemos además asumir que x, y, z son coprimos dos a dos. Luego aplicamos el Lema 1.2.1 y escribimos, intercambiando en caso de ser necesario a x e y, $x^2 = r^2 - s^2$, $y^2 = 2rs$, y $z = r^2 + s^2$. La primera ecuación nos da otra terna pitagórica $x^2 + s^2 = r^2$, y no es dificil de ver que x, s, y r tienen que ser coprimos dos a dos. Por nuestra primera elección de x, sabemos que x tiene que ser impar, por lo que, aplicando nuevamente el Lema 1.2.1 tenemos que $x = a^2 - b^2$, $s = 2ab$, y $r = a^2 + b^2$. Por lo tanto obtenemos que

$$y^2 = 2rs = 4ab(a^2 + b^2). \tag{1.1}$$

Por el Lema, a y b tienen que ser coprimos, luego deben ser coprimos con $a^2 + b^2$ también. Por lo tanto, la factorización en primos de (1.1) nos dice que $a = c^2$, $b = d^2$, y $a^2 + b^2 = e^2$ tienen que ser todos cuadrados perfectos (al serlo 4 y al ser a, b y $a^2 + b^2$ coprimos dos a dos). Finalmente sustituyendo obtenemos que $c^4 + d^4 = e^2$, y como $e \leq a^2 + b^2 = r < z$, lo que contradice la minimalidad de z. Por lo tanto, no existen soluciones no nulas a la ecuación. □

Corolario 1.2.3. No existen soluciones en enteros positivos a la ecuación $x^4 + y^4 = z^4$.

Demostración. Supongamos que existiese una solución (x_0, y_0, z_0) a esta ecuación en los enteros positivos . Luego tendríamos que (x_0, y_0, z_0^2) es una solución no trivial de la ecuación $x^4 + y^4 = z^2$ lo que contradice el Teorema anterior. Por lo tanto no existen soluciones en enteros positivos a la ecuación deseada. □

1.3. Caso n=3

Leonard Euler, inspirado en el método del descenso infinito que utilizó Fermat para probar el caso $n = 4$, probó en el año 1770 el caso $n = 3$ (ver [Rib79, §III.3]). La prueba que realizó Euler se basó en el siguiente resultado, también probado por él mismo.

Lema 1.3.1. Si s es impar y $s^3 = a^2 + 3b^2$, con $\text{mcd}(a, b) = 1$, entonces $s = u^2 + 3v^2$, para algunos u, v enteros.

Basándose en dicho Lema, Euler prueba, de forma incompleta pero elegante, el Último Teorema de Fermat para el caso $n = 3$. Gauss también dió una prueba para el caso $n = 3$ usando la extensión cuadrática $\mathbb{Q}(\sqrt{-3})$. Dicha demostración no fue publicada hasta después de su muerte.

Euler quiso repetir el mismo método del descenso infinito para los casos restantes pero falló en el intento.

1.4. Teoremas de Sophie Germain

Un siglo después de la muerte de Fermat solo se habían logrado probar los casos $n = 3$ y $n = 4$ del Últimto Teorema de Fermat. La primera en dar una aproximación general del problema fue Sophie Germain. En una de sus cartas dirigidas a Gauss ella menciona que su propósito inmediato no era demostrar un caso particular, sino decir algo acerca de muchos casos simultáneamente. Germain dividió el Último Teorema de Fermat $x^p + y^p = z^p$, con p primo, en dos casos:

Caso 1 $x^p + y^p = z^p$ no tiene soluciones enteras en donde x, y y z son coprimos con p,

Caso 2 $x^p + y^p = z^p$ no tiene soluciones enteras en donde uno y solamente uno de los valores x, y, z es divisible por p.

Notar que estos dos casos abarcan todos los posibles, ya que estamos analizando el caso en el cual x, y, z son coprimos dos a dos.

Luego, prueba los siguientes dos Teoremas, cuyas demostraciones están incluidas en [Rib79, §IV].

Teorema 1.4.1. (Sophie Germain) Sean p y q primos impares que satisfacen

1. $p \not\equiv a^p \pmod{q}$ para todo $a \in \mathbb{Z}$,
2. Si x, y, z satisfacen $x^p + y^p + z^p \equiv 0 \pmod{q}$, entonces q tiene que dividir uno de los valores x, y o z,

entonces el **Caso 1** del Último Teorema de Fermat es cierto para p.

Teorema 1.4.2. (Sophie German) Si p es primo y $2p + 1$ también lo es, entonces el **Caso 1** del Último Teorema de Fermat es cierto para p.

Los primos que cumplen la hipótesis del Teorema 1.4.2 fueron llamados Primos de Sophie Germain, y es aún un problema abierto si existen infinitos de los mismos.

Como consecuencia del aporte realizado por Germain, Legendre y Dirichlet, de manera independiente, probaron en 1825 el caso $n = 5$. Más adelante 1839 Lamé y Lebesgue el caso $n = 7$. Sophie Germain y Legendre, de forma conjunta, usando los resultados probados por Germain, probaron todos los casos del Último Teorema de Fermat para $p < 197$.

Sin embargo los teoremas propuestos por Sophie Germain tenían sus limitaciones. Era difícil extender sus resultados para los casos en los cuales $2kp + 1$ era primo con k grande. Además, sus resultados no abarcan el **Caso 2** del Último Teorema de Fermat. Caso que sí iba a ser abarcado en la solución de Kummer para primos regulares, solución que discutiremos en el próximo capítulo.

Capítulo 2

Teoría Algebraica de Números y la Demostración de Kummer

2.1. Introducción

Después de los avances realizados por Sophie Germain, la Academia Francesa ofreció una serie de premios al matemático que lograse resolver el Último Teorema de Fermat. En 1847 se celebraría una reunión en la Academia, en la cual asistirían tres matemáticos que deseaban resolver el problema de Fermat: Mané, Cauchy y Kummer. Mané, que hacía unos años había probado el caso $n = 7$, afirmaba que había probado el Último Teorema de Fermat. La prueba que presentó Mané se basó en la siguiente descomposición de $x^p + y^p$ en el cuerpo ciclotómico $\mathbb{Q}(\zeta_p)$:

$$x^p + y^p = (x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \dots (x + \zeta_p^{p-1} y),$$

donde ζ_p es una raíz p-ésima primitiva de la unidad. Mané además afirmó que ésta era a su vez una descomposición única en primos. Cauchy por su parte, también había presentado una prueba en la cual usaba la factorización única en primos. Por el contrario, Kummer había probado, tiempo antes de que Mané y Cauchy presentaran sus pruebas, que tal propiedad de factorización única no necesariamente se cumplía en los cuerpos $\mathbb{Q}(\zeta_p)$. Kummer observó que dicha factorización iba a ser única para el caso en el cual los ideales en el anillo de enteros de $\mathbb{Q}(\zeta_p)$ sean principales, por lo que se interesó en ver qué tan lejos estaban dichos ideales de serlo. De esta forma Kummer introduciría lo que sería el concepto de primos regulares. Kummer, unas semanas después de que Mané y Cauchy entregaran sus pruebas, terminó entregando una prueba completa del Teorema de Fermat para el caso de estos últimos primos mencionados.

En la presente Capítulo nos dedicaremos a estudiar en profundidad la prueba de Kummer para el caso de los primos regulares. Para eso necesitaremos desarrolar y probar algunos resultados de Teoría Algebraica de Números en los cuales se basa el mismo Teorema. En este Capítulo se usarán como referencia los siguientes libros: [Sha86], [Mil08], [Lan13], [Hun80], [Rib79] y [Was97].

2.2. Preliminares

Definición 2.2.1. Sea K un cuerpo de característica 0. Dado $n \in \mathbb{N}$, se dice que $x \in K$ es una *raíz n-ésima de la unidad* si $x^n = 1$. Una raíz n-ésima de la unidad x se dice *primitiva* si $\text{ord}(x) = n$. Llamaremos $G_n(K)$ y $H_n(K)$ a los conjuntos de raíces n-ésimas de la unidad y raíces primitivas respectivamente.

Observación 2.2.2. $G_n(K)$ es un subgrupo de $K^\times$. En efecto, $G_n(K)$ es el núcleo del endomorfismo de $K^\times$, $x \mapsto x^n$.

Teorema 2.2.3. (Kronecker) Sea $K/\mathbb{Q}$ una extensión finita de $\mathbb{Q}$. Luego si $\alpha \in K$ es un entero algebraico (ver Definición 2.2.12) tal que todos sus conjugados por $\text{Gal}(K/\mathbb{Q})$ tienen valor absoluto 1, α es una raíz de la unidad.

Demostración. Ver [HK81, §34 Lema (a).], □

Definición 2.2.4. Sea K un cuerpo de característica 0. Se llama *cuerpo ciclotómico*, de índice n sobre K, a todo cuerpo de descomposición, sobre K, del polinomio $x^n - 1$.

Definición 2.2.5. Sea K un cuerpo de característica 0 y $\overline{K}$ una clausura algebraica. Se llama *polinomio cilcotómico* de índice n, sobre K al polinomio

$$\Phi_n(x) = \prod_{w \in H_n(\overline{K})} (x - w).$$

Proposición 2.2.6. Φ_n es un polinomio de grado $\varphi(n)$ (donde φ es la función indicadora de Euler), cuya definición es independiente de $\overline{K}$.

Demostración. $G_n(\overline{K})$ tiene orden n, con lo cual $H_n(\overline{K})$ tiene $\varphi(n)$ elementos. Es claro, entonces, que Φ_n es un polinomio de grado $\varphi(n)$. Lo restante sale como consecuencia de [Hun80, Proposición 8.2]. □

Proposición 2.2.7. Sea K un cuerpo de característica 0. Para todo natural n, $x^n - 1 = \prod_{0<d|n} \Phi_d(x)$.

Demostración. Por razones de orden, $(H_d)_{0<d|n}$ es una partición de G_n , donde $G_n = G_n(\overline{K})$ y $H_d = H_d(\overline{K})$. Asociando según esta partición, se tiene que

$$x^n - 1 = \prod_{w \in G_n} (x - w) = \prod_{0<d|n} \left(\prod_{w \in H_d} (x - w) \right).$$

□

Corolario 2.2.8. Sea K un cuerpo de característica 0. Si q es primo, entonces $\Phi_q(x) = \sum_{0 \le i < q} x^i$.

Demostración. En este caso la igualdad del final de la Proposición anterior se lee $x^q - 1 = (x - 1)\Phi_q(x)$. □

Solamente nos interesará trabajar en el caso particular $K = \mathbb{Q}$ y $n = p$ primo impar. Denotaremos a la raíz primitiva $e^{2\pi i/p}$ como ζ_p. Además, por el Corolario 2.2.8 tenemos que

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = \sum_{i=0}^{p-1} x^i. \tag{2.1}$$

Observar además que el cuerpo ciclotómico de índice p sobre $\mathbb{Q}$ corresponde a $\mathbb{Q}(\zeta_p)$. En efecto, $\mathbb{Q}(\zeta_p)$ es el cuerpo de descomposición del polinomio $\Phi_p(x)$. Esto se debe a que todas las raíces de Φ_p son potencias de ζ_p y luego al ser $x^p - 1 = (x-1)\Phi_p(x)$ (usamos la igualdad mencionada en la demostración del Corolario 2.2.8), y al estar $1 \in \mathbb{Q}$, tenemos que $\mathbb{Q}(\zeta_p)$ será el cuerpo de descomposición de $x^p - 1$ y, por lo tanto, el cuerpo ciclotómico de orden p sobre $\mathbb{Q}$.

Proposición 2.2.9. Φ_p es el polinomio minimal de ζ_p sobre $\mathbb{Q}$.

Demostración. Como Φ_p es mónico y tiene a ζ_p como raíz, basta ver que es irreducible. Notar que $\Phi_p(x)$ es irreducible si y solo si $\Phi_p(x+1)$ lo es. Y este último lo es por el Criterio de Einsenstein. En efecto,

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \ldots + \binom{p}{p-2}x + \binom{p}{p-1},$$

y $p \nmid 1$, $p \mid \binom{p}{j}$ para $j = 0, 1, \ldots, p-1$ y $p^2 \nmid \binom{p}{p-1}$. □

Corolario 2.2.10. $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

Demostración. $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = gr(m_{\zeta_p}(x))$ donde $m_{\zeta_p}(x)$ es el polinomio minimal de ζ_p sobre $\mathbb{Q}$, pero por la Proposición 2.2.9, $gr(m_{\zeta_p}(x)) = p - 1$, y estamos. □

Proposición 2.2.11. $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es una extensión Galoisiana de grado finito y $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

Demostración. La primera afirmación es inmediata, porque $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es, por definición, un cuerpo de descomposición de un polinomio separable. Es de grado finito al ser de tipo finito y algebraica. Notar que todo elemento de $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ es un automorfismo de $\mathbb{Q}(\zeta_p)^\times$, por lo que preserva el orden de los elementos de $\mathbb{Q}(\zeta_p)$. Luego toda función $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ cumple que $\sigma(\zeta_p) = \zeta_p^k$ para algún $k = 1, \ldots, p-1$. Como todo automorfismos de $\mathbb{Q}(\zeta_p)$ queda determinado por donde envía a ζ_p, llamaremos σ_k a la función $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ tal que $\sigma(\zeta_p) = \zeta_p^k$. Queda entonces probado el isomorfismo entre $(\mathbb{Z}/p\mathbb{Z})^\times$ y $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ dado por $k \mapsto \sigma_k$. □

Llamaremos a cualquier extensión finita de $\mathbb{Q}$ como *cuerpo de números*. Definamos a continuación algunos conceptos importantes.

Definición 2.2.12. Sea K un cuerpo de números. Decimos que $\alpha \in K$ es un *entero algebraico* si existe $f \in \mathbb{Z}[X]$ mónico tal que tiene a α como raíz. Denotaremos por $\mathcal{O}_K$ al conjunto de enteros algebraicos en K.

Proposición 2.2.13. Se cumplen los siguientes resultados

(a) $\mathcal{O}_K$ es un anillo y es finitamente generado como $\mathbb{Z}$-módulo con dimensión igual al grado de la extensión.
(b) $\mathcal{O}_K$ es un dominio de Dedekind y por lo tanto todo ideal en $\mathcal{O}_K$ se descompone, de forma única, como producto de ideales primos.
(c) Si $[K : \mathbb{Q}] = n$, entonces la cantidad de factores primos que puede tener un ideal de $\mathcal{O}_K$ en su descomposición en ideales primos es siempre menor o igual a n.

Demostración. (a) Ver [Mil08, Corolario 2.30].
(b) Ver [Mil08, Teorema 3.29, Lema 3.30 y Teorema 3.7].
(c) Ver [Lan13, §I. VII. Corolario 2]. □

Definamos ahora la norma y la traza en una extensión de cuerpos en general, no necesariamente en cuerpo de números.

Definición 2.2.14. Sea F/K una extensión finita de cuerpos. Fijando $\alpha \in F$ definimos $m_\alpha : F \to F$ como $m_\alpha(a) = \alpha \cdot a$. Fijando β una base de F como K-espacio vectorial definimos a la norma como $\mathrm{Nm} : (F^\times, \cdot) \to (K^\times, \cdot)$, dada por $\mathrm{Nm}(\alpha) = \det([m_\alpha]_\beta)$; y a la traza como $\mathrm{Tr} : (F, +) \to (K, +)$, dada por $\mathrm{Tr}(\alpha) = \mathrm{Tr}([m_\alpha]_\beta)$.

Mencionemos algunas propiedades importantes.

Proposición 2.2.15. Se cumplen los siguientes resultados
(a) Las funciones traza y norma están bien definidas.
(b) $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$.
(c) $\mathrm{Nm}(\alpha \cdot \beta) = \mathrm{Nm}(\alpha) \cdot \mathrm{Nm}(\beta)$.
(d) Si $\alpha \in K$ y $[F : K] = n$, entonces $\mathrm{Tr}(\alpha) = n\alpha$ y $\mathrm{Nm}(\alpha) = \alpha^n$.

Demostración. Ver [Hun80, Teorema 7.3]. □

Si $K/\mathbb{Q}$ es una extensión finita e $I \subset \mathcal{O}_K$ es un ideal no nulo, definimos la norma de I como $\mathrm{Nm}(I) = |\mathcal{O}_K/I|$.

Proposición 2.2.16. Se cumplen los siguientes resultados
(a) Si $I, J \subset \mathcal{O}_K$ son ideales no nulos, entonces se cumple que $\mathrm{Nm}(I \cdot J) = \mathrm{Nm}(I) \cdot \mathrm{Nm}(J)$.
(b) $\mathrm{Nm}(\langle\alpha\rangle) = |\mathrm{Nm}(\alpha)|$.

Demostración. Ver [Mil08, Proposición 4.2]. □

2.3. Solución de Kummer

Mencionamos antes que si estamos en un dominio de Dedekind, la factorización en ideales es única, pero eso no implica que todo elemento en un Dedekind se factorice de forma única como producto de elementos primos. Sin embargo, si todos los ideales de $\mathcal{O}_K$ son principales, dicha factorización en primos sí va a ser única. Nos gustaría medir entonces, qué tan lejos están los ideales de ser principales, una medida que representará el número de clase. Antes de definir el número de clase, deberemos definir otro concepto.

Definición 2.3.1. Sea A un dominio conmutativo y $F(A)$ su cuerpo de fracciones. Un ideal *fraccionario* de A es un sub A-módulo $I \subset F(A)$ no nulo para el cual existe $a \in A$ tal que $aI \subset A$. Decimos que un ideal fracionario I es *principal* si existe $x \in F(A)$ tal que $I = xA$.

Observación 2.3.2. Es claro que todo ideal de A es un ideal fraccionario. Además un ideal I de A es principal en A si y solo si es principal como ideal fraccionario. Por lo que el conjunto de ideales principales de A coincide con el conjunto de ideales fraccionarios principales incluidos en A.

Además, si A es un dominio de Dedekind, resulta que con el producto usual de ideales, el conjunto de ideales fraccionarios es un grupo. Luego al ser $\mathcal{O}_K$ un dominio de Dedekind, tiene sentido definir su grupo de ideales fraccionarios. Ahora estamos en condiciones de definir el grupo de clases.

Definición 2.3.3. Definimos el grupo de clases de K, el cual denotaremos por $Cl(K)$, como el cociente de grupos $Cl(K) = G_K/H_K$ donde G_K es el grupo de ideales fraccionarios de $\mathcal{O}_K$ y H_K el grupo de ideales fraccionarios principales de $\mathcal{O}_K$.

Se puede probar que, si K es un cuerpo de números, el grupo de clases es siempre finito (ver [Mil08]), y llamamos a su orden el número de clase de K, al cual denotaremos por h_K. Enunciemos una observación que será de vital importancia cuando queramos probar el Teorema probado por Kummer.

Observación 2.3.4. Sea p primo tal que $p \nmid h_K$. Supongamos que I es un ideal fraccionario de $\mathcal{O}_K$ tal que I^p es principal , luego I es principal. En efecto, si no lo fuese, I no sería trivial en el grupo de clases, y tendría orden p. Por lo que el grupo de clases tendría un subgrupo de orden p, el subgrupo generado por I. Pero esto implica que el orden de dicho subgrupo, que es p, tendría que dividir al orden de grupo de clases, lo cual supusimos que no valía. Entonces I tiene que ser principal.

Una vez definido el número de clase, podemos definir a los primos regulares.

Definición 2.3.5. Decimos que un primo impar p es *regular* si $p \nmid h_K$ donde h_K es el número de clase de $K = \mathbb{Q}(\zeta_p)$.

Antes de mostrar la solución de Kummer para el Teorema de Fermat en el caso de primos regulares, demostraremos un par de resultados previos. De acá en adelante, denotaremos $K = \mathbb{Q}(\zeta_p)$ para algún primo p.

Teorema 2.3.6. $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

Demostración. Ver [Mil08, Proposición 6.2]. □

Nos interesará saber cómo se factorizan ideales tales como $\langle p \rangle$ como producto de ideales primos en $\mathcal{O}_K$. En general, si tenemos una extensión de cuerpos $\widetilde{F}/F$, con $\widetilde{F}$ y F cuerpo de números, decimos que un ideal primo $I \in \mathcal{O}_F$ es *inerte* en $\mathcal{O}_{\widetilde{F}}$ si se mantiene primo en $\mathcal{O}_{\widetilde{F}}$. Se dice que *ramifica* si hay factores repetidos en su descomposición en $\mathcal{O}_{\widetilde{F}}$, y decimos que *ramifica totalmente* si se factoriza como potencia de un único primo con exponente igual al grado de la extensión. Veamos que p ramifica totalmente en $\mathcal{O}_K$.

Lema 2.3.7. El ideal $p \cdot \mathcal{O}_K$ se descompone como $\langle 1-\zeta_p\rangle^{p-1}$. Por lo tanto el ideal principal $\langle 1-\zeta_p\rangle$ es primo en $\mathcal{O}_K$ y $\mathrm{Nm}(\langle 1-\zeta_p\rangle) = p$.

Demostración. Como el polinomio minimal de ζ_p es $\Phi_p(x) = \frac{x^p-1}{x-1}$, podemos descomponerlo como,

$$\Phi_p(x) = \prod_{i=1}^{p-1}(x-\zeta_p^i).$$

Evaluando en 1 en ambos lados de dicha igualdad, y usando la expresión (2.1) obtenemos que

$$p = \prod_{i=1}^{p-1}(1-\zeta_p^i). \tag{2.2}$$

De la igualdad anterior obtenemos una descomposición de $\langle p\rangle$ en $\mathcal{O}_K$, que será justamente $\langle p\rangle = \prod_{i=1}^{p-1}\langle 1-\zeta_p^i\rangle$. Notar que $1-\zeta_p = \frac{\zeta_p^i-1}{\zeta_p-1}(1-\zeta_p^i)$, y $\frac{\zeta_p^i-1}{\zeta_p-1}$ es una unidad en $\mathcal{O}_K$ (pues tiene inversa que es $\frac{\zeta_p-1}{\zeta_p^i-1}$). Luego $\langle 1-\zeta_p\rangle = \langle 1-\zeta_p^i\rangle$ para todo $i = 1,\dots,p-1$. Por lo tanto, de esto último, sumado a la factorización de $\langle p\rangle$, tenemos que $\langle p\rangle = \langle 1-\zeta_p\rangle^{p-1}$. Más aún, por la Observación 2.2.13 y usando que $[K:\mathbb{Q}] = p-1$, tenemos que $\langle 1-\zeta_p\rangle^{p-1}$ es, en efecto, la factorización en ideales primos de $\langle p\rangle$. Por lo tanto $\langle 1-\zeta_p\rangle$ es un ideal primo. Para la última afirmación notemos lo siguiente, como $p \in \mathbb{Q}$ tenemos, por la Proposición 2.2.15, que $\mathrm{Nm}(p) = p^{p-1}$. Luego, usando que $\langle p\rangle = \langle 1-\zeta_p\rangle^{p-1}$ y la Proposición 2.2.16, tenemos que $(\mathrm{Nm}(\langle 1-\zeta_p\rangle))^{p-1} = \mathrm{Nm}(\langle 1-\zeta_p\rangle^{p-1}) = \mathrm{Nm}(\langle p\rangle) = |\,\mathrm{Nm}\langle p\rangle| = p^{p-1}$. Como además $\mathrm{Nm}(\langle 1-\zeta_p\rangle) \in \mathbb{N}$, tenemos que $\mathrm{Nm}(\langle 1-\zeta_p\rangle) = p$. □

Lema 2.3.8. Supongamos que x, y, z son soluciones no triviales a la ecuación $x^p + y^p = z^p$ con p primo impar tal que $p \nmid xyz$. Luego, los ideales $\langle x+\zeta_p^i y\rangle$, con $i = 0,\dots,p-1$, son coprimos dos a dos.

Demostración. Como $z^p = x^p + y^p = (x+y)(x+\zeta_p y)(x+\zeta_p^2 y)\cdots(x+\zeta_p^{p-1}y)$, tenemos la siguiente igualdad de ideales

$$\prod_{i=0}^{p-1}\langle x+\zeta_p^i y\rangle = \langle z\rangle^p. \tag{2.3}$$

Supongamos que existe un ideal primo $\mathfrak{p}$ tal que divide a $\langle x+\zeta_p^j\rangle$ y a $\langle x+\zeta_p^k\rangle$, para algunos $0 \le j < k \le p-1$, por lo que el elemento $(x+\zeta_p^j y) - (x+\zeta_p^k y) = y\zeta_p^j(1-\zeta_p^{k-j})$ está en $\mathfrak{p}$. Notar que $1-\zeta_p^{k-j}$ es un asociado de $1-\zeta_p$, y ζ_p^j es una unidad, luego $\mathfrak{p}$ contiene a $y(1-\zeta_p)$. Como $\mathfrak{p}$ es un ideal primo, tenemos que $y \in \mathfrak{p}$ o $1-\zeta_p \in \mathfrak{p}$. En el primer caso, como además asumimos que $x+\zeta_p^j y \in \mathfrak{p}$, tenemos que $x \in \mathfrak{p}$. Como x e y son coprimos [1], existen enteros a y b tales que $ax+by = 1$. Pero esto último implica que $1 \in \mathfrak{p}$, lo que contradice el hecho de

[1] En el capítulo anterior mencionamos que podemos reducir el Teorema de Fermat al caso en el que x, y, z sean coprimos dos a dos, así que podemos analizar simplemente este caso.

que $\mathfrak{p}$ sea un ideal primo. Por lo tanto, tiene que pasar que $1-\zeta_p \in \mathfrak{p}$. Luego en particular $\mathfrak{p}|\langle 1-\zeta_p\rangle$, pero como probamos en el Lema 2.3.7 que $\langle 1-\zeta_p\rangle$ era un ideal primo, y sumado a la factorización única de ideales en ideales primos en $\mathcal{O}_K$, tenemos que $\mathfrak{p} = \langle 1-\zeta_p\rangle$. Como $\mathfrak{p}$ divide el lado izquierdo de (2.3), tenemos que $\langle 1-\zeta_p\rangle$ divide a $\langle z\rangle$. Lo que implica que $\mathrm{Nm}(\langle 1-\zeta_p\rangle)|\,\mathrm{Nm}(\langle z\rangle)$. Pero por lo probado en el Lema 2.3.7, $\mathrm{Nm}(\langle 1-\zeta_p\rangle) = p$ y como $z \in \mathbb{Q}$, tenemos que $\mathrm{Nm}(\langle z\rangle) = |\,\mathrm{Nm}(z)| = |z|^{p-1}$. Luego $p|z$, contradiciendo nuestra hipótesis. Por lo tanto, los ideales $\langle x+\zeta_p^i y\rangle$ son coprimos dos a dos. □

Lema 2.3.9. Para $v \in \mathbb{Z}[\zeta_p]^\times$, $v/\bar{v}$ es una raíz de la unidad.

Demostración. Si $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ entonces $\sigma(\bar{v}) = \overline{\sigma(v)}$ por lo que $v/\bar{v}$ y todas sus conjucaciones sobre $\mathbb{Q}$ tienen valor absoluto 1. Luego por Teorema 2.2.3 $v/\bar{v}$ es una raíz de la unidad. □

Más aún, se puede ver que todas las raíces de la unidad en $\mathbb{Q}[\zeta_p]$ (ver [Was97] pág.4) son de la forma $\pm\zeta_p^j$ para algún j entre 0 y $p-1$.

Con todos los resultados previos, podemos probar ahora el Teorema de Fermat para primos regulares. Dividiremos la prueba en dos partes. Primero lo haremos para el caso en el cual $p \nmid xyz$ y luego para el caso en el cual p divide a algúno de los elementos x, y, z. Notar que esto cubre todos los casos posibles a analizar, pues si p divide a dos de los elementos x, y, z, como $x^p + y^p = z^p$, entonces va a dividir al tercero, pero solo queremos analizar el caso en el cual x, y, z son coprimos dos a dos, pues mencionamos antes que solo bastaba analizar este caso.

Teorema 2.3.10. (Kummer) Si p es primo impar regular, entonces la ecuación $x^p + y^p = z^p$ no tiene soluciones enteras no triviales tales que $p \nmid xyz$.

Demostración. Como p es primo impar, podemos analizar si tiene solución no trivial la ecuación $x^p + y^p + z^p = 0$, pues hay una biyección entre el espacio de soluciones de ambas ecuaciones dada por $(x, y, z) \mapsto (x, y, -z)$. Asumimos que existen enteros x, y, z que solucionan mi ecuación y que además $p \nmid xyz$. Como probamos en el Lema 2.3.8, los ideales $\langle x+\zeta_p^i y\rangle$ con $i = 0, \ldots, p-1$ son coprimos dos a dos. El hecho de que sean coprimos, sumado a que la descomposición en ideales primos es única y al hecho de que los ideales en el lado derecho de la expresión (2.3) están elevados a la potencia p-ésima, nos dice que cada ideal $\langle x+\zeta_p^i\rangle$ es la potencia p-ésima de un ideal primo, digamos $\langle x+\zeta_p^i\rangle = \mathfrak{J}_i^p$ con $\mathfrak{J}_i$ ideales primos, coprimos entre sí (al ser coprimos los ideales $\langle x+\zeta_p^i y\rangle$) y tal que $\mathfrak{J}_1\mathfrak{J}_2\ldots\mathfrak{J}_{p-1} = \langle z\rangle$. Además, como $\mathfrak{J}_i^p$ es un ideal principal y $p \nmid h_K$ al ser p primo regular, tenemos, por la Observación 2.3.4, que cada $\mathfrak{J}_i$ es un ideal principal. Sea $\alpha_i \in \mathcal{O}_K = \mathbb{Z}[\zeta_p]$ un generador de $\mathfrak{J}_i$. De esto sigue que existe un $u \in \mathcal{O}_K = \mathbb{Z}[\zeta_p]$ unidad tal que $x+\zeta_p y = u\alpha_1^p$. Escribiendo $\alpha_1 = b_0 + b_1\zeta_p + \ldots + b_{p-2}\zeta_p^{p-2}$, con $b_j \in \mathbb{Z}$, tenemos que

$$\alpha_1^p \equiv b_0^p + (b_1\zeta_p)^p + \ldots + (b_{p-2}\zeta_p^{p-2})^p \equiv b_0 + b_1 + \ldots + b_{p-2} \pmod{p\mathbb{Z}[\zeta_p]}, \tag{2.4}$$

al ser los coeficientes binomiales no triviales congruentes a 0 (mod $p\mathbb{Z}[\zeta_p]$). Por lo que $\alpha_1^p \equiv \bar{\alpha_1}^p \pmod{p\mathbb{Z}[\zeta_p]}$. Luego por el Lema 2.3.9, y la observación siguiente a dicho Lema,

tenemos que $u/\bar{u} = \pm\zeta_p^j$ para algún j entre 0 y $p-1$. Si $u/\bar{u} = \zeta_p^j$ entonces

$$\begin{aligned} x + \zeta_p y &= u\alpha_1^p \\ &= \zeta_p^j \bar{u}\alpha_1^p \\ &\equiv \zeta_p^j \bar{u}(\bar{\alpha_1})^p \pmod{p\mathbb{Z}[\zeta_p]} \\ &\equiv \zeta_p^j (x + \bar{\zeta_p}) \pmod{p\mathbb{Z}[\zeta_p]}. \end{aligned}$$

Por lo tanto

$$u/\bar{u} = \zeta_p^j \Longrightarrow x + y\zeta_p - y\zeta_p^{j-1} - x\zeta_p^j \equiv 0 \pmod{p\mathbb{Z}[\zeta_p]}. \tag{2.5}$$

De forma similar,

$$u/\bar{u} = -\zeta_p^j \Longrightarrow x + y\zeta_p + y\zeta_p^{j-1} + x\zeta_p^j \equiv 0 \pmod{p\mathbb{Z}[\zeta_p]}. \tag{2.6}$$

Nos gustaría ver que ninguna de estas ecuaciones vale para $0 \leq j \leq p-1$ y x e y coprimos con p. Como x e y son no congruentes a 0 módulo p, estas congruencias parecen mostrar una dependencia lineal sobre $\mathbb{Z}/p\mathbb{Z}$ entre algunas potencias de ζ_p en $\mathbb{Z}[\zeta_p]/p\mathbb{Z}[\zeta_p]$. Sin embargo, en $\mathbb{Z}[\zeta_p]/p\mathbb{Z}[\zeta_p]$ las potencias $1, \zeta_p, \ldots, \zeta_p^{p-2}$ son linealmente independientes sobre $\mathbb{Z}/p\mathbb{Z}$ pues

$$\mathbb{Z}[\zeta_p]/p\mathbb{Z}[\zeta_p] \cong \mathbb{Z}[X]/\langle p, \Phi_p(X)\rangle \cong (\mathbb{Z}/p\mathbb{Z})[X]/\langle \Phi_p(X)\rangle \cong (\mathbb{Z}/p\mathbb{Z})[X]/\langle (X-1)^{p-1}\rangle,$$

y $\{1, X, \ldots, X^{p-2}\}$ es una base del último anillo, sobre $\mathbb{Z}/p\mathbb{Z}$. Luego para tales $j \leq p-1$ tal que $1, \zeta_p, \zeta_p^{j-1}, \zeta_p^j$ son potencias distintas en el conjunto $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$, es decir, siempre que $0, 1, j-1, j$ sean enteros distintos con $j \leq p-2$, las Ecuaciones (2.5) y (2.6) llevan a una contradicción. Por lo que tenemos una contradicción cuando $3 \leq j \leq p-2$. Por lo tanto, solo quedan descartar los casos $j = 0, 1, 2, p-1$. Primero que nada, podemos suponer $p \geq 5$ pues la ecuación $x^3 + y^3 = z^3$ no tiene soluciones en enteros coprimos con 3. En efecto, no existen soluciones a la ecuación $x^3 + y^3 \equiv z^3 \pmod 9$ ya que el cubo de unidades módulo 9 son ± 1.

1. Caso $j = p-1$. En este caso, el lado izquierdo de (2.5) nos queda

   $$x(1 - \zeta_p^{p-1}) + y(\zeta_p - \zeta_p^{p-2}) = 2x + (x+y)\zeta_p + x(\zeta_p^2 + \ldots + \zeta_p^{p-3}) + (x-y)\zeta_p^{p-2},$$

   lo que contradice la independencia lineal de los elementos $1, \zeta_p, \ldots, \zeta_p^{p-2} \pmod p$ sobre $\mathbb{Z}/p\mathbb{Z}$ mirando los coeficientes de ζ_p^2. Hay una contradicción similar en el caso de (2.6).

2. Caso $j = 0$. En este caso, (2.5) se transforma en $y(\zeta_p - \zeta_p^{-1}) \equiv 0 \pmod{p\mathbb{Z}[\zeta_p]}$. Como y no es divisible por p, podemos dividir por él y tenemos que $\zeta_p^2 - 1 \equiv 0 \pmod p$, lo que contradice la independencia lineal de 1 y $\zeta_p^2 \mod p$ al ser $p \geq 5$. De forma similar, (2.6) implica $2x\zeta_p + y\zeta_p^2 + y \equiv 0 \pmod p$, por lo que nuevamente llegamos a una contradicción.

3. Caso $j = 2$. Se llega también a una contradicción en (2.5) y (2.6) en la independencia lineal.

4. Caso $j = 1$. En este caso (2.6) implica que $(x+y)(1+\zeta_p) \equiv 0 \pmod p$, por lo que $x + y \equiv 0 \pmod{p\mathbb{Z}}$ (acá usamos el Lema 2.3.7). Por lo tanto $z^p = x^p + y^p \equiv (x+y)^p \equiv 0 \pmod p$,

por lo que p divide a z, lo cual sería una contradicción. Nos queda por analizar el subcaso (2.5). En este caso, (2.5) nos queda

$$x(1-\zeta_p)+y(\zeta_p-1)\equiv 0 \pmod{p}. \tag{2.7}$$

Escribiendo $p=u(1-\zeta_p)^{p-1}$, (2.7) implica que

$$x\equiv y \pmod{(1-\zeta_p)^{p-2}}.$$

Como $p-2\geq 1$ y x e y están en $\mathbb{Z}$, nos queda $x\equiv y \pmod{p\mathbb{Z}}$. Realizando la prueba con y y $-z$ intercambiados, tenemos $x\equiv -z \pmod{p\mathbb{Z}}$, luego

$$0=x^p+y^p-z^p\equiv 3x^p \pmod{p}.$$

Como $p\neq 3$ y x es coprimo con p, tenemos una contradicción. Habiendo descartado todos los posibles casos de j, llegamos a una contradicción al asumir que existía solución a dicha ecuación con x,y,z coprimos con p. Por lo tanto probamos el Teorema para este caso.

□

Para probar el caso restante, es decir cuando $p|z$, enunciemos primero algunos resultados.

Lema 2.3.11. Para cada $\alpha\in\mathbb{Z}[\zeta_p]$ existe un entero $a\in\mathbb{Z}$ tal que $\alpha^p\equiv a \pmod{p\cdot\mathcal{O}_K}$.

Demostración. Tomemos $\{1,\ldots,\zeta_p^{p-2}\}$ como base de $\mathbb{Z}[\zeta_p]$. Podemos escribir $\alpha=a_0+a_1\zeta_p+\ldots+a_{p-2}\zeta_p^{p-2}$. Esto nos da

$$\alpha^p\equiv a_0^p+(a_1\zeta_p)^p+\ldots+(a_{p-2}\zeta_p^{p-2})^p\equiv a_0^p+a_1^p+\ldots+a_{p-2}^p \pmod{p}$$

al ser todos los coeficientes binomiales (no triviales) congruentes a 0 módulo p. □

Lema 2.3.12. Si $\langle 1-\zeta_p\rangle|\langle x+\zeta_p^k y\rangle$ para algún k entonces $\langle 1-\zeta_p\rangle|\langle x+\zeta_p^j y\rangle$ para todo j

Demostración. Sale del hecho que si $\langle 1-\zeta_p\rangle|\langle x+\zeta_p^k y\rangle$ entonces $\langle 1-\zeta_p\rangle|\langle x+\zeta_p^{k+1} y\rangle$. Esto es pues $\langle x+\zeta_p^{k+1}y\rangle\subset\langle x+\zeta_p^k y\rangle+\langle\zeta_p^k\rangle\langle\zeta_p-1\rangle\langle y\rangle$. □

Lema 2.3.13. (Kummer) Si p es un primo regular y $u\in K=\mathbb{Q}(\zeta_p)$ es una unidad congruente a un elemento de $\mathbb{Z}$ módulo $p\cdot\mathcal{O}_K$, entonces $u=v^p$ para alguna unidad v en K.

Demostración. Ver [Sha86, §V.6., Teorema 3]. □

Veamos ahora la demostración del último Teorema caso $p|z$.

Teorema 2.3.14. (Kummer) Si p es primo impar regular con $p|z$, entonces la ecuación $x^p+y^p=z^p$ no tiene soluciones enteras no triviales.

Demostración. Queremos ver si existen soluciones a la ecuación

$$x^p+y^p=z^p. \tag{2.8}$$

Sea $z = p^k z_0$ donde z_0 es coprimo con p y $k \geq 1$. Por el Lema 2.3.7, $p = u(1-\zeta_p)^{p-1}$ para alguna unidad u en $\mathbb{Q}(\zeta_p)$. Por lo tanto una solución a (2.8) nos daría la siguiente igualdad

$$x^p + y^p = u(1-\zeta_p)^{pm} z_0^p, \tag{2.9}$$

donde $m = k(p-1) > 0$. Probaremos entonces que no existen soluciones a una ecuación como en (2.9), donde x, y, z_0 son elementos en $\mathbb{Z}[\zeta_p]$ y coprimos con $(1-\zeta_p)$, lo que claramente implica que lo mismo es cierto para x, y, z_0 enteros coprimos con p. Asumiendo que una solución a (2.9) existe, sean $x, y, z_0 \in \mathbb{Z}[\zeta_p]$ coprimos a $(1-\zeta_p)$ que satisface (2.9) para alguna unidad u y tal que m es minimal con tal condición. Factorizando el lado izquierdo de (2.9) y pasando a ideales tenemos

$$\prod_{j=0}^{p-1} \langle x + \zeta_p^j y \rangle = \langle 1-\zeta_p \rangle^{pm} \langle z_0 \rangle^p. \tag{2.10}$$

Luego existe un i tal que $\langle 1-\zeta_p \rangle | \langle x+\zeta_p^i y \rangle$. Sigue entonces, del Lema 2.3.12 que $\langle 1-\zeta_p \rangle$ divide a todos los miembros de la izquierda de (2.10). Supongamos que $x+\zeta_p^i \equiv x+\zeta_p^j \pmod{\langle 1-\zeta_p \rangle^2}$ con $0 \leq i < j \leq p-1$, entonces $\zeta_p^i y(1-\zeta_p^{j-i}) \equiv 0 \pmod{\langle 1-\zeta_p \rangle^2}$, lo cual es imposible pues $\zeta_p^i y$ es coprimo con $1-\zeta_p$ y $1-\zeta_p^{j-i}$ es asociado con $1-\zeta_p$. Por lo tanto, los elementos $x + \zeta_p^j y$ son distintos módulo $(1-\zeta_p)^2$, por lo que los elementos

$$\frac{x+\zeta_p^j y}{1-\zeta_p} \ (j = 0, 1, \ldots, p-1) \tag{2.11}$$

son no congruentes dos a dos módulo $(1-\zeta_p)$. Como $\mathrm{Nm}(\langle 1-\zeta_p \rangle) = p$ entonces tenemos que $|\mathbb{Z}[\zeta_p]/\langle 1-\zeta_p \rangle| = p$ y los elementos de (2.11) son un conjunto completo de representantes de los residuos módulo $\langle 1-\zeta_p \rangle$. En particular, alguno de dichos elementos tiene que ser un elemento de $\langle 1-\zeta_p \rangle$. Como podemos reemplazar y por cualquier elemento $\zeta_p^j y$ en (2.9), podemos asumir que $x + y \in \langle 1-\zeta_p \rangle^2$. Luego cada $x + \zeta_p^j y$ con $j \neq 0$ es un elemento de $\langle 1-\zeta_p \rangle \setminus \langle 1-\zeta_p \rangle^2$. Por lo tanto, el lado izquierdo de (2.10) es divisible por $\langle 1-\zeta_p \rangle^{p+1}$ y $m > 1$. Denotemos por $\mathfrak{m}$ al máximo común divisor de $\langle x \rangle$ e $\langle y \rangle$. Como asumimos que x e y eran coprimos con $1-\zeta_p$ tendremos que $\langle x \rangle$ e $\langle y \rangle$ no serán divisibles por $\langle 1-\zeta_p \rangle$, por lo que $\mathfrak{m}$ tampoco. Luego $\langle x + \zeta_p^j y \rangle$ es divisible por $\langle 1-\zeta_p \rangle \mathfrak{m}$ cuando $j \neq 0$ y $\langle x+y \rangle$ es divisible por $\langle 1-\zeta_p \rangle^{p(m-1)+1} \mathfrak{m}$, y denotamos $\langle x + \zeta_p^j y \rangle = (1-\zeta_p)\mathfrak{m}\mathfrak{c}_j$ para cada $j \neq 0$ y $\langle x+y \rangle = \langle 1-\zeta_p \rangle^{p(m-1)+1} \mathfrak{m}\mathfrak{c}_0$. Afirmamos que $\mathfrak{c}_0, \ldots, \mathfrak{c}_{p-1}$ son coprimos dos a dos. En efecto, si $\mathfrak{c}_i$ y $\mathfrak{c}_k$ $(0 \leq i < k \leq p-1)$ tienen un divisor $\mathfrak{p}$, entonces $\langle x + \zeta_p^i y \rangle$ y $\langle x + \zeta_p^k y \rangle$ deberían ser divisibles por $\langle 1-\zeta_p \rangle \mathfrak{m}\mathfrak{p}$. Pero luego $\zeta_p^i y(1-\zeta_p^{k-i})$ y $x(1-\zeta_p^{k-i})$ deberían estar en $\langle 1-\zeta_p \rangle \mathfrak{m}\mathfrak{p}$, lo cual significa que $x, y \in \mathfrak{m}\mathfrak{p}$, contradiciendo la elección de $\mathfrak{m}$. Luego los ideales $\mathfrak{c}_0, \ldots, \mathfrak{c}_{p-1}$ son coprimos dos a dos. Sustituyendo estas nuevas ecuaciones en (2.10) obtenemos $\mathfrak{m}^p \langle 1-\zeta_p \rangle^{pm} \mathfrak{c}_0 \cdots \mathfrak{c}_{p-1} = \langle 1-\zeta_p \rangle^{pm} \langle z_0 \rangle^p$. Como los ideales $\mathfrak{c}_0, \ldots, \mathfrak{c}_{p-1}$ son coprimos dos a dos, tenemos, por la expresión previamente mencionada y por la factorización única en ideales, que cada $\mathfrak{c}_j$ tiene que ser la potencia p-ésima de algún ideal que divida a $\langle z_0 \rangle$. Digamos $\mathfrak{c}_j = \mathfrak{a}_j^p$ para $j = 0, 1, \ldots, p-1$. Luego $\langle x+y \rangle = \langle 1-\zeta_p \rangle^{p(m-1)+1} \mathfrak{m}\mathfrak{a}_0^p$ y $\langle x + \zeta_p^j y \rangle = \langle 1-\zeta_p \rangle \mathfrak{m}\mathfrak{a}_k^p$. Despejando $\mathfrak{m}$ de la primera ecuación [2] y reemplazando en la

[2] Notar que al estar viendo a los ideales en el grupo de ideales fraccionarios tiene sentido hablar de sus inversos.

segunda ecuación obtenemos que

$$\langle x+\zeta_p^j y\rangle\langle 1-\zeta_p\rangle^{p(m-1)} = \langle x+y\rangle(\mathfrak{a}_j\mathfrak{a}_0^{-1})^p. \tag{2.12}$$

Sigue de esto que los ideales $(\mathfrak{a}_j\mathfrak{a}_0^{-1})^p$ son principales, pues el lado izquierdo de (2.12) lo es. Luego por la Observación 2.3.4 tenemos que entonces los ideales $\mathfrak{a}_j\mathfrak{a}_0^{-1}$ serán ideales principales. Por lo tanto, existen $\alpha_j, \beta_j \in \mathbb{Z}[\zeta_p]$ tal que $\mathfrak{a}_j\mathfrak{a}_0^{-1} = \langle\frac{\alpha_j}{\beta_j}\rangle$ para $j = 1, \ldots, p-1$. Como $\mathfrak{a}_j$ y $\mathfrak{a}_0$ son coprimos con $\langle 1-\zeta_p\rangle$, podemos asumir que ni α_j o β_j están en $\langle 1-\zeta_p\rangle$. De (2.12) podemos ver que

$$\langle x+\zeta_p^j y\rangle\langle 1-\zeta_p\rangle^{p(m-1)} = \langle x+y\rangle\langle\frac{\alpha_j}{\beta_j}\rangle^p u_j \ (j = 1, 2, \ldots, p-1) \tag{2.13}$$

donde cada $u_j \in \mathbb{Z}[\zeta_p]$ es una unidad. Consideremos ahora la igualdad $(x+\zeta_p y)(1+\zeta_p)-(x+\zeta_p^2 y) = \zeta_p(x+y)$. Si multiplicamos esta igualdad por $(1-\zeta_p)^{p(m-1)}$ y evaluamos (2.13) en $j = 1$ y $j = 2$, vemos que $(x+y)\left(\frac{\alpha_1}{\beta_1}\right)^p u_1(1+\zeta_p)-(x+y)\left(\frac{\alpha_2}{\beta_2}\right)^p u_2 = (x+y)\zeta_p(1-\zeta_p)^{p(m-1)}$. Por lo tanto,

$$(\alpha_1\beta_1)^p - \frac{u_2}{u_1(1+\zeta_p)}(\alpha_2\beta_1)^p = \frac{\zeta_p}{u_1(1+\zeta_p)}(1-\zeta_p)^{p(m-1)}(\beta_1\beta_2)^p.$$

Luego denotando $\alpha = \alpha_1\beta_2$, $\beta = \alpha_2\beta_1$,$\gamma = \beta_1\beta_2$, $e = \frac{u_2}{u_1(1+\zeta_p)}$ y $e' = \frac{\zeta_p}{u_1(1+\zeta_p)}$ tenemos

$$\alpha^p + e\beta^p = e'(1-\zeta_p)^{p(m-1)}\gamma^p \tag{2.14}$$

donde $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta_p]\setminus(1-\zeta_p)$. Notar además que $1+\zeta_p$ es una unidad, pues $(1-\zeta_p)(1+\zeta_p) = 1-\zeta_p^2$, que es asociado con $1-\zeta_p$. Por lo que e, e' son unidades en $\mathbb{Q}(\zeta_p)$.

Vimos que $m > 1$, por lo que $p(m-1) \geq p$, por lo que $\alpha^p + e\beta^p \equiv 0 \pmod{\langle 1-\zeta_p\rangle^p}$. Como β es coprimo con $\langle 1-\zeta_p\rangle$, existe β' tal que $\beta\beta' \equiv 1 \pmod{\langle 1-\zeta_p\rangle^p}$. Multiplicando la primer congruencia por β'^p tenemos que $e \equiv \omega^p \pmod{\langle 1-\zeta_p\rangle}$ con $\omega = (-\alpha\beta')$. Como $\mathrm{Nm}(\langle 1-\zeta_p\rangle) = p$, y $\omega \in \mathbb{Z}[\zeta_p]$, tenemos por el Lema 2.3.11 que existe $a \in \mathbb{Z}$ tal que $\omega^p \equiv a \ (\mathrm{mod} p\cot\mathcal{O}_K)$, por lo que lo mismo vale para e. Como $\langle p\rangle|\langle 1-\zeta_p\rangle^p$ podemos usar el Lema 2.3.13 y entonces $e = \eta^p$, para algún $\eta \in \mathbb{Z}[\zeta_p]$ unidad. Luego

$$\alpha^p + (\eta\beta)^p = e'(1-\zeta_p)^{p(m-1)}\zeta_p^p$$

que es una igualdad del mismo tipo que en (2.9). Pero en este caso se reemplazó el exponente m por $m-1$ lo cual contradice la minimalidad de m. Por lo tanto, (2.8) no tiene solución en $\mathbb{Z}$ con $p|z$. □

Capítulo 3

Geometría Proyectiva

En este Capítulo se hablará de ciertas definiciones y propiedades acerca de curvas proyectivas. Estos conceptos serán necesarias para el Capítulo 4 , en el cual hablaremos de Curvas elípticas, las cuales son en particular curvas proyectivas.

3.1. Espacio proyectivo y curvas algebraicas

Definición 3.1.1. Sea K un cuerpo. Definimos en $K^{n+1} \setminus \{0\}$ la siguiente relación de equivalencia: Dadas dos $(n+1)$-tuplas en K^{n+1}, $[a_0, a_1, \ldots, a_n]$,$[a'_0, a'_1, \ldots, a'_n]$ decimos que $[a_0, a_1, \ldots, a_n] \sim [a'_0, a'_1, \ldots, a'_n]$ si existe $t \neq 0$ tal que $a_i = ta'_i$ para todo $i = 0, 1, \ldots, n$. Definimos al n-espacio proyectivo sobre K como $(K^{n+1} \setminus \{0\})/\sim$ y lo denotaremos por $\mathbb{P}^n(K)$.

Observación 3.1.2. (i) $\mathbb{P}^2(\mathbb{R})$ y $\mathbb{P}^2(\mathbb{C})$ son variedades diferenciables.

De ahora en más solamente trabajaremos con los espacios $\mathbb{P}^2(K)$.

Definición 3.1.3. Un polinomio $F \in K[X, Y, Z]$ se dice *homogéneo de grado d* si se cumple que cada monomio de F tiene grado d. En particular se cumple que $F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z)$ para todo $x, y, z, \lambda \in K$.

Denotamos al espacio de polinomios homogéneos de grado d sobre K como $K[X, Y, Z]_d$.

Definición 3.1.4. Sean K y k cuerpos de tal forma que k es subcuerpo de K. Una curva proyectiva definida sobre k es un polinomio homogéneo de grado d para algún $d \in \mathbb{N}$, es decir $F \in k[X, Y, Z]_d$. Definimos a los puntos de la curva en K como los puntos $[x, y, z] \in \mathbb{P}^2(K)$ tal que $F(x, y, z) = 0$ y los denotamos por $C(K)$. El grado de dicha curva será el grado del polinomio. Diremos que la curva es racional si $k = \mathbb{Q}$.

Observación 3.1.5. Si K es un subcuerpo de $\widetilde{K}$ y C es una curva algebraica proyectiva dada por un polinomio $F \in K[X, Y, Z]_d$, entonces $C(K) \subset C(\widetilde{K})$.

El plano afín K^2 se incrusta en $\mathbb{P}^2(K)$ mediante la aplicación $(x, y) \longmapsto (x, y, 1)$. El espacio que queda por cubrir de $\mathbb{P}^2(K)$ es lo que se conoce como la recta en el infinito. Dicha recta será la que tiene polinomio $F(X, Y, Z) = Z$.

Sea C la recta mencionada anteriormente. Notar que $C(K) \cong \mathbb{P}^1(K)$. En efecto $C(K) = \{[X, Y, Z] \in \mathbb{P}^2(K) |\ Z = 0\}$ y la aplicación $[X, Y, 0] \mapsto [X, Y]$ está bien definida. Luego $\mathbb{P}^2(K) \cong K^2 \cup C(K) \cong K^2 \cup \mathbb{P}^1(K)$

Definición 3.1.6. Sea C curva proyectiva dada por el polinomio $F \in K[X,Y,Z]_d$. Definimos la curva afín de C a la curva $\widetilde{C}$ en K^2 asociada al polinomio $f(x,y) = F(x,y,1)$. Es decir, los puntos $(x,y) \in K^2$ que satisfacen $f(x,y) = 0$.

Observación 3.1.7. (i) De la misma definición de curva afín podemos observar que $[x_0,y_0,z_0] \in C(K)$ con $z_0 \neq 0$ se corresponde de manera biunívoca con los elementos de la curva afín mediante la aplicación $[x_0,y_0,z_0] \longmapsto \left(\frac{x_0}{z_0}, \frac{y_0}{z_0}\right)$.

(ii) Dado un polinomio $f \in K[X,Y]$ de grado d puedo homogeneizarlo en un polinomio $F \in K[X,Y,Z]_d$ (es decir que $F(x,y,1) = f(x,y)$). En efecto, si $f(x,y) = \sum_{i,j} a_{ij}x^iy^j$ tenemos que $F(X,Y,Z) = \sum_{i,j} a_{ij}X^iY^jZ^{d-i-j}$ satisiface lo pedido. Definimos a dicha F como la *homogeneización* de f.

A la hora de trabajar con curvas elípticas más adelante, la primera observación va a ser de suma importancia. Esto se debe a que el punto de una curva elíptica que se encuentra en la recta del infinito es conocido. Y por lo tanto para ver los demás puntos de la misma, (es decir los puntos de C cuya tercer coordenada no sea 0) basta con ver su curva afín, que es mucho más facil de analizar.

Definición 3.1.8. Sea C una curva afín con polinomio $f(x,y)$. Decimos que un punto $(x_0,y_0) \in C(K)$ es singular si $\frac{\partial f}{\partial x}(x_0,y_0) = 0 = \frac{\partial f}{\partial y}(x_0,y_0)$. En caso contrario decimos que (x_0,y_0) es no singular. C es una curva no singular si es no singular en todos los puntos de $C(\overline{K})$, donde $\bar{K}$ es una clausura algebraica de K . En caso contrario se dirá que es singular. Si (x_0,y_0) es un punto no singular, definimos la recta tangente a C en (x_0,y_0) de la siguiente forma:

$$L = \left\{(x,y) \in K^2 : \frac{\partial f}{\partial x}(x_0,y_0)(x-x_0) + \frac{\partial f}{\partial y}(x_0,y_0)(y-y_0) = 0\right\}.$$

De la misma manera se define para curvas proyectivas. Sea ahora C una curva proyectiva con polinomio $F \in K[X,Y,Z]_d$. Decimos que un punto $[X_0,Y_0,Z_0] \in C$ es singular si

$$\frac{\partial F}{\partial X}([X_0,Y_0,Z_0]) = \frac{\partial F}{\partial Y}([X_0,Y_0,Z_0]) = \frac{\partial F}{\partial X}([X_0,Y_0,Z_0]) = 0.$$

En caso contrario decimos que (x_0,y_0) es no singular. C es una curva no singular si es no singular en todos los puntos de $C(\overline{K})$. En caso contrario se dirá que es singular. Si $[X_0,Y_0,Z_0]$ es un punto no singular, definimos la recta tangente a C en $P = [X_0,Y_0,Z_0]$ de la siguiente forma:

$$L = \left\{[X,Y,Z] \in \mathbb{P}^2(K) : \frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z = 0\right\}.$$

3.2. Intersección de curvas proyectivas

En esta sección definiremos la *multiplicidad de la intersección* entre una curva proyectiva y una recta proyectiva en un punto. Sean $C \in K[X,Y,Z]_d$, $L \in K[X,Y,Z]_1$ y un punto

$P = [x_0, y_0, z_0] \in C(K) \cap L(K)$. Sea Φ un cambio de coordenadas afín respecto a P, es decir, $\Phi \in \mathrm{GL}_3(K)$ tal que $\Phi(x_0, y_0, z_0) = (0, 0, 1)$. Denotamos entonces

$$f(x, y) = C(\Phi^{-1}(x, y, 1)) = f_1(x, y) + \ldots + f_d(x, y)$$
$$l(x, y) = L(\Phi^{-1}(x, y, 1))$$

donde $f_i(x, y)$ representa la suma de los términos de grado i en $f(x, y)$. Como $l(0, 0) = 0$, $l(x, y) = bx - ay$ para algunas constantes a y b con al menos una distinta de 0. Luego $\phi(t) = \begin{bmatrix} at \\ bt \end{bmatrix}$ parametriza a la recta $l(x, y) = 0$. La expresión $f(\phi(t))$ es un polinomio en t con $f(\phi(0)) = 0$. En efecto,

$$\begin{aligned} f(\phi(t)) &= f_1(at, bt) + f_2(at, bt) + \ldots + f_d(at, bt) \\ &= tf_1(a, b) + t^2 f_2(a, b) + \ldots + t^d f_d(a, b). \end{aligned}$$

Definición 3.2.1. Definimos la multiplicidad de la intersección de $C \in K[X, Y, Z]_d$ y $L \in K[X, Y, Z]_1$ en $P = [x_0, y_0, z_0]$, la cual denotaremos por $I(C \cap L, P)$, como

$$I(C \cap L, P) = \begin{cases} \text{orden de anulación de } t = 0 \text{ en } f(\phi(t)) & \text{si } f \circ \Phi \neq 0, \\ +\infty & \text{si } f \circ \Phi = 0. \end{cases}$$

Observación 3.2.2. Esta definición no depende del cambio de coordenadas afín Φ (ver [Kna92, §II.3.]).

Definición 3.2.3. Sea $C \in K[X, Y, Z]_d$ una curva proyectiva. Decimos que un punto no singular $P = [x_0, y_0, z_0] \in C$ es un *punto de inflexión* si $I(C \cap L, P) \geq 3$ donde L es la recta tangente de C en P.

El concepto de multiplicidad de intersección se puede generalizar para intersección de curvas algebraicas en general (ver [Tat92, §A.4.]). En este contexto vale el siguiente resultado:

Teorema 3.2.4. (Bezout) Sean C_1 y C_2 dos curvas proyectivas de grados d_1 y d_2 respectivamente con ninguna componente en común, sobre un cuerpo K. Luego

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) \leq d_1 d_2.$$

Además, si K es algebraicamente cerrado entonces vale la igualdad.

Demostración. Ver [Tat92, §A.4.]. □

Proposición 3.2.5. Sea E una curva proyectiva cúbica sobre K no singular, y L una recta proyectiva sobre K. Luego $\sum_{P \in E \cap L} I(E \cap L, P)$ es 0, 1 ó 3.

Demostración. Ver [Kna92, Proposición 2.15]. □

Capítulo 4

Curvas Elípticas

La idea de usar curvas elípticas para afrontar el Último Teorema de Fermat se debe a Hellegourach [Hel01] y Frey [Fre86]. La idea de Hellegourach fue, suponiendo que existe una solución al Último Teorema de Fermat $a^p + b^p = c^p$ con $p \geq 5$, asociarle una curva elíptica a la cual se llamó curva de Hellegourach-Frey. Esta curva presentaba propiedades muy poco probables de ocurrir en dichas curvas elípticas, razón que apoyaba la idea de que no existía tal solución. En particular, Frey afirmaba que estas curvas no iban a ser modulares, por lo que si se llegaba a probar la Conjetura de Taniyama-Shimura para curvas elípticas semiestables (la cual se mencionará al final del Capítulo 6), entonces se llegaría a un absurdo, absurdo que provenía de suponer que existía una solución a la ecuación planteada en el Último Teorema de Fermat. En el presente Capítulo se hablará entonces acerca de Curvas Elípticas y sus propiedades, finalizando con la teoría acerca de las Curvas de Hellegourach-Frey y sobre las representaciones de las mismas. Las principales referencias usadas a lo largo de esta Capítulo son las siguientes: [Kna92], [Tat92], [Sil09], [Pac18] y [Hel01].

4.1. Forma de Weierstrass y discriminante

Sea k un cuerpo. Decimos que una curva algebraica proyectiva C de grado 3 sobre k está en la forma de Weierstrass si está dada por

$$C : Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0. \tag{4.1}$$

Es decir que

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{4.2}$$

Definición 4.1.1. Una curva elíptica sobre k es una curva proyectiva de grado 3 no singular y tal que se encuentra en su forma de Weierstrass.

Observación 4.1.2. (i) El único punto en una curva en su forma de Weierstrass que pertenece a la recta en el infinito es $[0, 1, 0]$.
(ii) $[0, 1, 0]$ es un punto no singular y además es punto de inflexión. La recta tangente a dicho punto es la recta en el infinito.

Luego por la observación que hicimos en el capítulo pasado, bastará con estudiar su curva afín, que resulta ser la dada por la ecuación

$$C : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Es decir,

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

Principalmente vamos a trabajar con curvas elípticas sobre $\mathbb{Q}$ y $\mathbb{F}_p$.

Definición 4.1.3. Sea una curva sobre un cuerpo k dada en su forma de Weierstrass como en la Ecuación (4.1). Definimos su discriminante como

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

donde $b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6,\ b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

Teorema 4.1.4. Una curva dada por la Ecuación (4.1) es singular si y solo si $\Delta = 0$.

Demostración. Ver [Kna92, Teorema 3.2]. □

El punto $[0, 1, 0]$ siempre es no singular, por lo que las singularidades las tendremos en el plano afín. Además, una curva en la forma de Weierstrass tendrá a lo sumo una singularidad. Si hubiesen 2 puntos de singularidad, la recta que pasa por ellos tendría multiplicidad mayor o igual a 2 en cada uno. Luego la suma de las multiplicidades en los puntos de intersección de la curva con dicha recta sería mayor ó igual a 4, lo cual contradice el Teorema de Bezout 3.2.4.

Definición 4.1.5. Sea C una curva dada en su forma de Weierstrass vista en el plano afín. Supongamos que C es singular en P. Decimos que dicha singularidad es un *nodo* si existen dos rectas tangentes distintas en P, y decimos que es una *cúpside* si tiene una única tangente (doble) en P.

Más aún, podemos determinar el tipo de singularidad mediante la siguiente Proposición.

Proposición 4.1.6. Sea C una curva dada en su forma de Weierstrass. Luego

- C es una curva elíptica $\iff \Delta \neq 0$,
- C tiene un nodo $\iff \Delta = 0$ y $c_4 \neq 0$,
- C tiene una cúspide $\iff \Delta = 0$ y $c_4 = 0$,

donde $c_4 = b_2^2 - 24b_4$.

Demostración. Ver [Kna92, Proposición 3.10]. □

Definición 4.1.7. Un **cambio de variables admisible** en una curva en su forma de Weierstras sobre el cuerpo k, es un cambio de variable de la forma:

$$\begin{pmatrix} x \\ y \\ w \end{pmatrix} = \Phi^{-1} \begin{pmatrix} x' \\ y' \\ w' \end{pmatrix} \quad \text{con} \quad \Phi^{-1} = \begin{pmatrix} u^2 & 0 & r \\ su^2 & u^3 & t \\ 0 & 0 & 1 \end{pmatrix} \tag{4.3}$$

con u, r, s, t en k y $u \neq 0$.

Dos curvas elípticas que estén relacionadas mediante un cambio de variables admisible diremos que son *isomorfas*.

Observación 4.1.8. i) Todo cambio de variables aceptable fija a $[0, 1, 0]$ y lleva la recta en el infinito a ella misma.

ii) Si E' es una curva elíptica obtenida de otra curva elíptica E mediante un cambio de variables admisible como en (4.3) entonces su discriminante Δ' será $\Delta' = u^{-12}\Delta$ donde Δ es el discriminante de E.

Si K es un cuerpo de característica distinta de 2 o 3 podemos probar que, mediante un cambio de variable admisible, toda curva cúbica dada por la Ecuación (4.1) puede ser expresada de la forma $y^2 = x^3 - 27c_4x - 54c_6$ donde $c_4 = b_2^2 - 24b_4$ y $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. En este caso, donde la curva elíptica está dada por la ecuación $y^2 = x^3 + ax + b$, tenemos que su discriminante será $\Delta = -2^4(4a^3 + 27b^2)$. Se puede ver además lo siguiente:

Proposición 4.1.9. Sea $E : y^2 = x^3 + ax + b$ una curva elíptica. Entonces $\Delta = 2^4 d_f$ donde d_f es el discriminante de $f(x) = x^3 + ax + b$. Es decir, si $f(x) = (x - r_1)(x - r_2)(x - r_3)$ entonces $d_f = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2$.

Demostración. Ver [Kna92, Proposición 3.6]. □

Corolario 4.1.10. Sea $E : y^2 = x^3 + ax + b$ una curva elíptica. Entonces E es no singular si y solo si $f(x) = x^3 + ax + b$ tiene sus 3 raíces distintas.

Demostración. Inmediato de la Proposición 4.1.9 y del Teorema 4.1.4. □

Definición 4.1.11. El j invariante de una curva elíptica está definido por $j = \frac{c_4^3}{\Delta}$. En el caso en el que nuestra curva elíptica se encuentre dada por la expresión $y^2 = x^3 + ax + b$, tendremos que su invariante j será $j = 1728\frac{4a^3}{4a^3+27b^2}$.

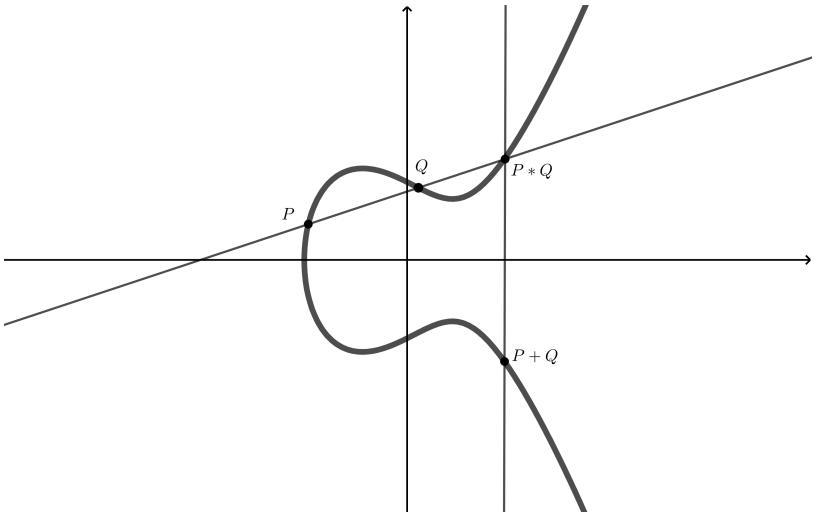
Proposición 4.1.12. Sea k un cuerpo de característica distinta de 2 y 3. Luego

(a) Si dos curvas elípticas están relacionadas por el mismo cambio de variable, entonces tienen el mismo invariante j,
(b) Si j_0 es dado, entonces existe una curva elíptica sobre k con invariante j dado por j_0,
(c) Si k es algebraicamente cerrado y dos curvas elípticas tienen el mismo invariante j, entonces están relacionadas por un cambio de variable admisible.

Demostración. Ver [Kna92, Proposición 3.7]. □

4.2. Estructura de una curva elíptica

Sea E una curva elíptica sobre un cuerpo K. Nos gustaría ahora describir los puntos de esta curva elíptica en dicho cuerpo, para eso vamos a tratar de darle alguna estructura. Observamos que la intersección de esta curva con la recta en el infinito era el punto $\mathcal{O} = [0, 1, 0]$. Vamos a definir la suma de tal forma que este elmento sea el neutro de la misma. Observar que para la suma de puntos, basta verlos en el plano afín, ya que el único punto de $E(K)$ que pertence a la recta en el infinito es el $[0, 1, 0]$. Vamos a definir la suma en $E(K)$ de la siguiente forma: sean P y Q dos puntos en $E(K)$, trazamos la recta que une dichos puntos y obtenemos el tercer punto de intersección con $E(K)$, llamemoslo $P * Q$. Luego trazamos la recta que une $P * Q$ con $\mathcal{O}$, es decir trazamos la recta vertical que pasa por $P * Q$ (Si $P * Q = \mathcal{O}$ dicha recta es la recta del infinito) y obtenemos el tercer punto de intersección de dicha recta con E, a dicho punto lo llamamos $P + Q$.



Por como definimos la suma $\mathcal{O} + P = P + \mathcal{O} = P$, y todo elemento tiene su opuesto. Si K es un cuerpo de característica distinta de 2 y de 3 podemos pensar a E, en su forma afín, como una curva elíptica de la forma $E : y^2 = x^3 + ax + b$, ya que probamos que existe un cambio de variable admisible que me lo lleva a esa expresión. Mirando a nuestra curva E bajo esta expresión, el opuesto de $\mathcal{O}$ será él mismo y el opuesto de $P = (x, y)$ será $P' = (x, -y)$. Sean entonces $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E(K)$ tal que $P \neq \pm Q$. Entonces

$$x(P + Q) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2. \tag{4.4}$$

Y en el caso que $P = Q$ se ve que

$$x([2]P) = \frac{x_1^4 - 2ax^2 - 8bx_1 + a^2}{4x_1^3 + 4ax_1 + 4b}, \tag{4.5}$$

donde $x(P + Q)$ y $x([2]P)$ indican la coordenada x de $P + Q$ y $[2]P$ respectivamente. Para una demostración de dichas fórmulas ver [Tat92, §I.4].

Notación 4.2.1. Para $m \in \mathbb{Z}$ y $P \in E$, denotaremos

$$[m]P = \overbrace{P + \ldots + P}^{m \text{ veces si } m>0}, \quad [m]P = \overbrace{(-P) + \ldots + (-P)}^{|m| \text{ veces si } m<0}, \quad [0]P = \mathcal{O}. \tag{4.6}$$

Teorema 4.2.2. Con la suma definida previamente y el neutro elegido $(E(\mathbb{Q}), +)$ es un grupo abeliano.

Demostración. Ver [Tat92, §I.2-4]. □

Teorema 4.2.3. (Mordell) Sea $E/\mathbb{Q}$ una curva elíptica. Luego $E(\mathbb{Q})$ es un grupo abeliano finitamente generado.

Demostración. Ver [Tat92, §III.1-5]. □

Por el Teorema de estructuras de grupos abelianos finitamente generados tenemos que $E(\mathbb{Q}) = E_{\text{tors}}(\mathbb{Q}) \oplus \mathbb{Z}^r$ donde $E_{\text{tors}}(\mathbb{Q})$ es la parte de torsión de $E(\mathbb{Q})$ y $\mathbb{Z}^r$ su parte libre. El siguiente Teorema caracteriza al subgrupo de torsión $E_{\text{tors}}(\mathbb{Q})$. Este resultado va a ser importante para más adelante.

Teorema 4.2.4. (Mazur) Sea $E/\mathbb{Q}$ una curva elíptica. Luego el subgrupo de torsión $E_{\text{tors}}(\mathbb{Q})$ de $E(\mathbb{Q})$ es isomorfo a uno de los siguientes quince grupos:

$$\mathbb{Z}/n\mathbb{Z} \text{ con } 1 \leq n \leq 10 \text{ ó } n = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ con } 1 \leq n \leq 4.$$

Demostración. Ver [Maz77, §III.5]. □

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

Si el cuerpo en el cual miro mi curva elíptica es $\mathbb{C}$, E será isomorfa, como variedad compleja, a un toro complejo $\mathbb{C}/\Lambda$, donde Λ es un retículo en $\mathbb{C}$. Las operaciones de grupo de $E(\mathbb{C})$ se corresponderán con la suma usual en $\mathbb{C}/\Lambda$. Sea $\mathbb{C}/\Lambda$ un toro complejo, con $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$. Definimos la función $\wp$ de Weierstrass asociada al retículo Λ como la función elíptica $\wp : \mathbb{C} \to \mathbb{C}$ dada por

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

que resulta ser meromorfa, doble periódica y con polo doble en Λ.

Sean

$$g_2 = 60 \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^4}, \quad g_3 = 140 \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^6}.$$

Luego se puede ver que $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ (ver [Kna92, Teorema 6.12]). Por lo tanto, los puntos de la imagen de $(\wp, \wp')$ se encuentran en los puntos, sobre $\mathbb{C}$ de la curva afín $E : y^2 = 4x^3 - g_2x - g_3$. Se puede probar (ver [Kna92, Teorema 6.5]), que

$$E : y^2 = 4x^3 - g_2x - g_3 = 4(x - u_1)(x - u_2)(x - u_3)$$

donde $u_1 = \wp\left(\frac{1}{2}\omega_1\right)$, $u_2 = \wp\left(\frac{1}{2}\omega_2\right)$ y $u_3 = \wp\left(\frac{1}{2}(\omega_1+\omega_2)\right)$. Además se puede ver que u_1, u_2, u_3 son distintos dos a dos (ver [Kna92, Lema 6.11]), por lo que la curva será no singular, y por lo tanto una curva elítpica.

Luego podemos definir la siguiente función $\mathbb{C}/\Lambda \to E(\mathbb{C})$ dada por $z \mapsto [\wp(z), \wp'(z), 1]$. Esta función se puede probar (ver [Sil09, §VI.3.] §, Proposición 3.6.) que es un isomorfismo como grupos de Lie complejos, es decir, un isomorfismo como superficies de Riemann (ver Definición 6.1.1) y un homomorfismo de grupos.

Por lo tanto todo toro complejo unidemensional es, en esencia, una curva elíptica vista sobre $\mathbb{C}$. La recíproca también es cierta, es decir, para toda curva elíptica sobre $\mathbb{C}$ existe un retículo Λ tal que $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ mediante la asociación previamente mencionada (ver [Sil09, VI.1]).

Observación 4.3.1. Ver a una curva elíptica sobre $\mathbb{C}$ como un toro complejo $\mathbb{C}/\Lambda$, es otra forma de darle una estructura de grupo a la misma. La estructura va a ser la heredada de $\mathbb{C}$ por lo que será un grupo abeliano. Dicha estructura va a coincidir con la previamente dada.

Una curva elíptica E/K, además de ser una curva proyectiva sobre K, es una *variedad proyectiva* sobre K, concepto que extiende al anterior. Más aún, al ser un grupo, pasa a ser lo que se denomina una *variedad abeliana* definida sobre K. En esta sección vimos que $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. En este caso se dirá que será una variedad abeliana de dimensión 1. Toda variedad abeliana sobre $\mathbb{C}$ cumplirá, al igual que las curvas elítpicas, que es isomorfa a un g-toro complejo. En dicho caso se dirá que la variedad abeliana tiene dimensión g. En el Capítulo 6 construiremos una variedad abeliana, dada por el Teorema de Eichler-Shimura, que será importante ya que se la vinculará a ciertas formas modulares. Para más información acerca de variedades proyectivas y abelianas ver [Kna92, §XI.7].

4.4. Isogenías y multiplicación compleja

Para definir la isogenía entre curvas elípticas precisaremos definir qué es un morfismo entre curvas elípticas. Si E/k y E'/k son curvas elípticas, entonces decimos que $\phi : E \to E'$ es un *mapa racional* definido (a priori) sobre k, si $\phi = [\phi_1, \phi_2, \phi_3]$ cumple que cada $\phi_i \in \overline{k}(E(k))$, donde $\overline{k}(E(k))$ es el cuerpo de funciones de $E(k)$ (ver [Kna92, §XI.7.]); y tal que para todo $x \in E(k)$ en donde ϕ_1, ϕ_2, ϕ_3 estén definidas, $\phi(x) = [\phi_1(x), \phi_2(x), \phi_3(x)]$ esté en $E'(k)$. Si las curvas elípticas E y E' pueden ser definidas sobre un subcuerpo k_0 de k y las funciones ϕ_i pueden ser multiplicadas por un elemento de $\overline{k}^*$ tal que estén en $k_0(E(K))$ entonces decimos que el mapa racional ϕ está definido sobre k_0.

Definición 4.4.1. Un mapa racional $\phi : E \to E'$ se dice regular o definido en $x \in E(k)$ si existe $g \in \bar{k}(E(k))$ tal que $g\phi_i$ está definido en x y $[(g\phi_1)(x), (g\phi_2)(x), (g\phi_3)(x)]$ no es nula. Un mapa racional que es regular en cada punto de $E(k)$ se dice un *morfismo*.

Definición 4.4.2. Sean E_1 y E_2 curvas elípticas sobre $\bar{k}$. Una *isogenía* entre E_1 y E_2 es un morfismo

$$\phi : E_1 \to E_2$$

no trivial. Cuando $E_1 = E_2$ decimos que es un *endomorfismo*. Diremos que E_1 es *isógena* a E_2 si existe una isogenía $\phi : E_1 \to E_2$.

Proposición 4.4.3. La isogenía entre curvas elípticas es una relación de equivalencia.

Demostración. Ver [Sil09, §III.6., Proposición 6.1]. □

Ejemplo 4.4.4. Sea E una curva elíptica sobre k. Entonces el morfismo $[n] : E \to E$ dado en (4.6) es un endormofismo de curvas elípticas.

Ejemplo 4.4.5. Si E es una curva elíptica sobre $\mathbb{F}_q$ entonces el morfismo de Frobenius

$$\sigma_q[(x_0, x_1, x_2)] \to [(x_0^q, x_1^q, x_2^q)]$$

es un endomorfismo sobre $\mathbb{F}_q$.

Notación 4.4.6. Supongamos que E_1 y E_2 son dos curvas elípticas definidas sobre k. Denotaremos por $\mathrm{Hom}(E_1, E_2)$ al conjunto de isogenías entre E_1 y E_2. Dicho conjunto con la suma punto a punto, y neutro la isogenía nula, termina siendo un grupo abeliano, al cual llamaremos *grupo de isogenías* entre E_1 y E_2. Si k_0 es un subcuerpo de k, entonces el grupo de isogenías sobre k_0 termina siendo un subgrupo de $\mathrm{Hom}(E_1, E_2)$. Denotaremos al *anillo de endomorfismos* de E como $\mathrm{End}(E)$, donde la suma es la suma punto a punto y el producto es la composición de funciones. Los elementos invertibles de $\mathrm{End}(E)$ forman el *grupo de automorfismos* de E, denotado por $\mathrm{Aut}(E)$.

Proposición 4.4.7. Sea E una curva elíptica. Luego el anillo de endomorfismos $\mathrm{End}(E)$ es un anillo (no necesariamente conmutativo) de característica 0 con ningún divisor de 0.

Demostración. Ver [Sil09, §III.4., Proposición 4.2]. □

Definición 4.4.8. Sea E una curva elíptica sobre k y $m \in \mathbb{Z}$. El m-subgrupo de torsión de E, denotado por $E[m]$, es el conjunto de puntos de m-torsión de $E(\bar{k})$. Vale decir,

$$E[m] = \{P \in E(\bar{k}) : [m]P = \mathcal{O}\}.$$

Si k_0 es una extensión de cuerpos de k, entonces denotaremos por $E(k_0)[m]$ al conjunto de puntos de torsión m en $E(k_0)$.

Teorema 4.4.9. Sea $m \in \mathbb{Z}$ con $m \neq 0$ y sea E una curva elíptica sobre k con $char\ k = 0$ o $char\ k = p$ con $p \nmid m$. Entonces

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Si E es una curva elíptica sobre un cuerpo de característica 0, los endomorfismos $[m]$ son generalmente todos los endomorfismos que tiene una curva elíptica. En dicho caso tenemos que $\mathrm{End}(E) \cong \mathbb{Z}$. Sin embargo, no siempre es el caso.

Definición 4.4.10. Decimos que una curva elíptica sobre $\mathbb{C}$ tiene multiplicación compleja si $\mathrm{End}(E) \ncong \mathbb{Z}$.

Es decir, hay más morfismos aparte de los $[m]$.

Ejemplo 4.4.11. La curva elíptica

$$E : y^2 = x^3 + x$$

tiene multiplicación compleja. En efecto $\phi(x, y) = (-x, iy)$ es un endomorfismo de E ya que $(iy)^2 = -y^2 = -x^3 - x = (-x)^3 + (-x)$.

Enunciemos y probemos ahora algunos resultados acerca de los subgrupos de torsión $E[m]$, para curvas elípticas sobre $\mathbb{Q}$, que serán importantes para más adelante.

Teorema 4.4.12. Sea $E/\mathbb{Q}$ una curva elíptica, K un cuerpo de Galois sobre $\mathbb{Q}$ y $G = \mathrm{Gal}(K/\mathbb{Q})$ su grupo de Galois. Entonces

(a) $E(K)$ es un subgrupo de $E(\mathbb{C})$.
(b) $P \in E(K) \Longrightarrow \forall\ \sigma \in G, \sigma(P) \in E(K)$.
(c) $\forall P, Q \in E(K)$,
  i) $\sigma(P + Q) = \sigma(P) + \sigma(Q)$,
  ii) $\sigma(-P) = -\sigma(P)$,
  iii) $\sigma(nP) = n\sigma(P)$.
(d) $P \in E(K)[m] \Longrightarrow \sigma(P) \in E(K)[m]$. Más aún, P y $\sigma(P)$ tienen el mismo orden.

Demostración. El item a) sale directo de las fórmulas de suma en $E(K)$ (ver las Ecuaciones (4.4) y (4.5)) y usando que K es un cuerpo. El ítem b) sale usando la linealidad de σ y el hecho que fija a los elementos de $\mathbb{Q}$. El ítem c) sale usando nuevamente las fórmulas de la suma en $E(K)$ y el hecho que σ es un morfismo de cuerpos. Para el item d) observamos que $[m]P = \mathcal{O}$. Entonces por el apartado c) tenemos que

$$[m]\sigma(P) = \sigma([m]P) = \sigma(\mathcal{O}) = \mathcal{O},$$

por lo que $\sigma(P) \in E(K)[m]$. Denotemos por $k = ord(P)$ y $d = \mathrm{ord}(\sigma(P))$ a los órdenes de P y $\sigma(P)$ respectivamente. Notar que,

$$[k]\sigma(P) = \sigma([k]P) = \sigma(\mathcal{O}) = \mathcal{O},$$

por lo que $d|k$. Por otro lado tenemos que,

$$[d]P = [d](\sigma^{-1}(\sigma(P))) = \sigma^{-1}([d]\sigma(P)) = \sigma^{-1}(\mathcal{O}) = \mathcal{O},$$

por lo que $k|d$. Entonces $k = d$ y por lo tanto P y $\sigma(P)$ tienen el mismo orden. □

Teorema 4.4.13. Sea $E/\mathbb{Q}$ una curva elíptica y $m \in \mathbb{N}$. Luego $\mathbb{Q}(E[m])/\mathbb{Q}$ es un cuerpo de números Galois.

Demostración. Que es un cuerpo de números sale pues al ser $E[m]$ un grupo finito, entonces $\mathbb{Q}(E[m])/\mathbb{Q}$ es una extensión finita de $\mathbb{Q}$. Observar que todo automorfismo $\sigma : \mathbb{Q}(E[m]) \to \mathbb{C}$ queda determinado por cuánto vale en los elementos (x_i, y_i) de $E[m]$. Por la parte d) del Teorema 4.4.12, tomando $K = \overline{\mathbb{Q}}$, tenemos que si $P_i \in E[m]$ entonces $\sigma(P_i) \in E[m]$, y tiene el mismo orden que P_i. Luego $\sigma(E[m]) \subset E[m]$ lo cual implica que $\mathbb{Q}(E[m])/\mathbb{Q}$ es una extensión normal y, sumado a que es una extensión separable, tenemos que es una extensión Galoisiana. □

Otro resultado acerca del cuerpo $\mathbb{Q}(E[p])$ que usaremos más adelante es el siguiente:

Proposición 4.4.14. $\mathbb{Q}(E[p])$ contiene una raíz primitiva ζ_p de orden p.

Demostración. Ver Observación 4.6.2 en [Hel01]. □

4.5. Reducción módulo p

Comencemos introduciendo el concepto de norma p-ádica. Sea p primo. Definimos entonces la siguiente valuación

$$\begin{aligned} v_p : \mathbb{Z} \setminus \{0\} &\longrightarrow \mathbb{Z} \\ a &\mapsto \text{máx}\{i \in \mathbb{N} \cup \{0\} : p^i | a\}. \end{aligned}$$

Llamaremos a esta valuación como *valuación p-ádica*. De la misma definición de v_p se desprende el siguiente resultado:

Proposición 4.5.1. Se cumplen las siguientes afirmaciones
(a) $v_p(ab) = v_p(a) + v_p(b)$
(b) $v_p(a+b) \geq \text{mín}\{v_p(a), v_p(b)\}$

Esta valuación puede extenderse a $\mathbb{Q} \setminus \{0\}$ de la siguiente forma natural: $v_p(r/s) = v_p(r) - v_s(s)$. Al extender la valuación p-ádica a $\mathbb{Q}$ sigue cumpliendo la Proposición 4.5.1.

Definición 4.5.2. Definimos el valor absoluto p-ádico $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ por

$$|a|_p = \begin{cases} p^{-v_p(a)} & \text{si } a \neq 0, \\ 0 & \text{si } a = 0. \end{cases}$$

Esta función es, en efecto, un valor absoluto. Es decir cumple la siguiente Proposición:

Proposición 4.5.3. Se cumplen los siguientes resultados
(a) $|r|_p \geq 0$.
(b) $|r|_p = 0 \iff r = 0$.
(c) $|r+s|_p \leq \text{máx}\{|r|_p, |s|_p\}$.
(d) $|rs|_p = |r|_p |s|_p$.

Demostración. (a) y (b) son claras. Para probar (c) basta usar la Proposición 4.5.1 (b) y que p^{-x} es decreciente. Finalmente (d) sale inmediato de la Proposición 4.5.1 (a). Observar que el apartado (c), también conocido como propiedad *ultramétrica*, prueba la desigualdad triangular, propiedad que caracteriza al valor absoluto. □

Decimos que un elemento $q \in \mathbb{Q}$ es *p-íntegro* si $|q|_p \leq 1$.

Al ser $|\cdot|_p$ un valor absoluto podemos ver que los elementos p-íntegros forman un subanillo de $\mathbb{Q}$ que contiene a $\mathbb{Z}$.

Sea q un elemento p-íntegro escrito de la forma $q = p^{v_p(q)} u/v$. Al ser p-íntegro tenemos que $v_p(q) \geq 0$. Luego podemos construir un homomorfismo de anillos entre los elementos p-íntegros de $\mathbb{Q}$ y $\mathbb{F}_p$ de la siguiente forma:

$$r_p(q) = \begin{cases} u/v \text{ mod p} & \text{si } v_p(q) = 0, \\ 0 & \text{si } v_p(q) > 0. \end{cases}$$

Llamamos a dicha función r_p la *reducción módulo p* de un elemento p-íntegro. Se ve inmediato, de la definición de r_p, que $r_p : \{\text{elementos } p\text{-íntegros}\} \to \mathbb{F}_p$ es un homomorfismo de anillos.

Observación 4.5.4. Sea $[x, y, z] \in \mathbb{P}^2(\mathbb{Q})$ y $d = \text{mcd}(v_p(x), v_p(y), v_p(z))$. Entonces $p^{-d}(x, y, z)$ tiene sus coordenadas p-íntegras y alguna de ellas es una unidad.

Luego de esta última observación podemos definir la operación $r_p : \mathbb{P}^2(\mathbb{Q}) \to \mathbb{P}^2(\mathbb{F}_p)$ dada por

$$r_p([x, y, z]) = [r_p(x), r_p(y), r_p(z)] \tag{4.7}$$

con x, y, z representantes tal que todos sean elementos p-íntegros, y tal que al menos uno tenga valor absoluto p-ádico 1. Dicho elemento representativo $[x, y, z] \in \mathbb{P}^2(\mathbb{Q})$ se dice *p-reducido*. Además, este elemento es único salvo un factor de valor absoluto p-ádico 1. Por lo que la función r_p está bien definida.

Usando dicha función r_p podemos reducir módulo p curvas proyectivas sobre $\mathbb{Q}$. Sea C una curva proyectiva sobre $\mathbb{Q}$ de grado m dada por el polinomio $F \in \mathbb{Q}[X, Y, Z]_m$. Multiplicando los coeficientes por una constante, podemos asumir que todos los coeficientes son p-íntegros y que al menos uno tiene valor absoluto p-ádico 1. Luego podemos reducir los coeficientes de F módulo p mediante r_p. De esta forma obtenemos el polinomio reducido $F_p \in \mathbb{F}_p[X, Y, Z]_m$. Al ser F_p bien definido salvo un escalar va a estar bien definida $C_p(\mathbb{F}_p)$, donde C_p la reducción de la curva C módulo p, es decir la curva proyectiva sobre $\mathbb{F}_p$, de grado m y cuyo polinomio asociado es F_p (para alguno de los F_p posibles, pues como mencionamos antes, no importa la elección del mismo ya que $C_p(\mathbb{F}_p)$ será el mismo).

Ejemplo 4.5.5. Sea la curva elíptica $E : y^2z = x^3 + \frac{2}{3}xz^2 - \frac{4}{9}z^3$. En este caso $E : F(x, y, z) = 0$ donde $F(x, y, z) = y^2z - x^3 - \frac{2}{3}xz^2 - \frac{4}{9}z^3$. Multiplicando por 9 podemos pensar a F como el polinomio $F(x, y, z) = 9y^2z - 9x^3 - 6xz^2 - 4z^3$. Notar que de esta forma los coeficientes nos quedan con valor absoluto 3-ádico menor igual a 1 y $|4|_3 = 1$. Luego reduciendo los coeficientes a $\mathbb{F}_3$ mediante r_3 nos queda el polinomio $F_p(x, y, z) \in \mathbb{F}_3[X, Y, Z]_3$ dado por $F_3(x, y, z) = 2z^3$. Por lo que la curva reducida módulo 3 nos queda $E' : 2z^3 = 0$.

Enunciemos ahora dos resultados que nos ayudarán a probar que la estructura de grupo se mantiene al reducir mi curva módulo p.

Proposición 4.5.6. Sea C una curva proyectiva dada por el polinomio $F \in \mathbb{Q}[X, Y, Z]_m$ y C_p la reducción módulo p de la curva. Luego mediante la reducción $r_p : \mathbb{P}^2(\mathbb{Q}) \to \mathbb{P}^2(\mathbb{F}_p)$ dado en la Ecuación (4.7), la imagen de $C(\mathbb{Q})$ está contenida en la imagen de $C_p(\mathbb{F}_p)$.

Demostración. Sea $[x, y, z] \in \mathbb{P}^2(\mathbb{Q})$ un elemento p-reducido. Luego

$$\begin{aligned}
[x, y, z] \in C(\mathbb{Q}) &\iff F([x, y, z]) = 0 \\
&\implies r_p([x, y, z]) = 0 \\
&\iff F_p(r_p(x), r_p(y), r_p(z)) = 0 \\
&\iff F_p(r_p([x, y, z])) = 0 \\
&\iff r_p(x, y, z) \in C_p(\mathbb{F}_p).
\end{aligned}$$

□

Proposición 4.5.7. Sea C una curva proyectiva de grado m sobre $\mathbb{Q}$, L una recta proyectiva sobre $\mathbb{Q}$ y $P = [x_0, y_0, z_0] \in L$. Si C_p y L_p son reducciones módulo p de C y L respectivamente. Entonces $I(C \cap L, P) \leq I(C_p \cap L_p, r_p(P))$

Demostración. Ver [Kna92, Proposición 5.5]. □

Observación 4.5.8. Sea ahora E una curva elíptica sobre $\mathbb{Q}$. Aplicamos en E un cambio de variable admisible como en la Ecuación (4.3) con $r = s = t = 0$ y $u \in \mathbb{N}$ elegido de tal forma que llevamos nuestra curva E a una curva elíptica isomorfa $\widetilde{E}$ donde todos sus coeficientes son enteros. Además los coeficientes de X^3 y ZY^2 van a ser 1. Por lo que E_p es justamente reducir los coeficientes de $\widetilde{E}$ módulo p. Denotemos por Δ_p, Δ_E y $\Delta_{\widetilde{E}}$ a los discriminantes de E_p, E y $\widetilde{E}$ respectivamente. Luego tenemos que $\Delta_p = \Delta_{\widetilde{E}}$ *mod* p. Por lo que E_p es no singular si y solo si $p \nmid \Delta_{\widetilde{E}}$.

Probamos en la Proposición 4.5.6 que la reducción de $E(\mathbb{Q})$ módulo p induce una función

$$r_p : E(\mathbb{Q}) \to E_p(\mathbb{F}_p) \tag{4.8}$$

Luego, usando las dos proposiciones previas y lo anteriormente mencionado, podemos probar el siguiente resultado que nos permite afirmar que al reducir módulo p una curva elíptica, se preserva la estructura de grupo entre $E(\mathbb{Q})$ y $E_p(\mathbb{F}_p)$.

Proposición 4.5.9. Sea $E/\mathbb{Q}$ una curva elíptica no singular y supongamos que su reducción E_p, también es no singular, entonces r_p dada en la Ecuación (4.8) es un morfimo de grupos

Demostración. Sean $P, Q \in E(\mathbb{Q})$. Como $r_p([0,1,0]) = [0,1,0]$ tenemos que r_p envía $\mathcal{O}$ a $\mathcal{O}_p$. Usando que E y E_p son no singulares tenemos por la Proposición 3.2.5 que $\sum_{P \in E \cap L} I(E \cap L, P)$ y $\sum_{P \in E_p \cap L_p} I(E_p \cap L_p, P)$ son menor iguales que 3, para cualquier recta L. Entonces por la Proposición 4.5.7 tenemos que $r_p(P * Q) = r_p(P) * r_p(Q)$. Por lo tanto

$$\begin{aligned} r_p(P+Q) &= r_p(\mathcal{O} * (P * Q)) = r_p(\mathcal{O}) * r_p(P * Q) = r_p(\mathcal{O}) * (r_p(P) * r_p(Q)) \\ &= \mathcal{O}_p * (r_p(P) * r_p(Q)) = r_p(P) + r_p(Q) \end{aligned}$$

y luego r_p es un morfismo de grupos. □

Observación 4.5.10. Otra forma de demostrar la proposición anterior es la siguiente. Sean $P = [x_0, y_0, z_0]$ y $Q = [x_0', y_0', z_0']$ elementos en $E(\mathbb{Q})$ con $x_0, y_0, z_0, x_0', y_0', z_0'$ representantes tal que todos sean elementos p-íntegros. Suponiendo que no son $\mathcal{O}$, podemos tomar su representación en $\mathbb{Q}^2$, es decir $P = \left(\frac{x_0}{z_0}, \frac{y_0}{z_0}\right)$ y $Q = \left(\frac{x_0'}{z_0'}, \frac{y_0'}{z_0'}\right)$. Luego solo basta dividir en todos los casos posibles de suma entre P y Q, usar las fórmulas expresadas en las Ecuaciones (4.4) y (4.5) para dichas sumas, y usar que r_p es un morfismo.

4.6. L-serie de una curva elíptica

4.6.1. Forma de Weierstrass globalmente minimal

Definición 4.6.1. Una curva proyectiva que se encuentre en su forma de Weierstrass, con coeficientes en $\mathbb{Z}$, se dice *minimal* para el primo p si $|\Delta|_p$ (donde $|\Delta|_p$ es el valor absoluto p-ádico de Δ) no puede aumentar mediante un cambio de variable admisible. Una curva que se encuentre en su forma de Weierstrass se dirá *globalmente minimal* si es minimal para todo primo p y si sus coeficientes son enteros.

Teorema 4.6.2. (Néron). Si E es una curva elíptica sobre $\mathbb{Q}$, existe un cambio de variables admisible sobre $\mathbb{Q}$ tal que la ecuación resultante sea una ecuación de Weierstrass globalmente minimal. Dos ecuaciones de Weierstrass globalmente minimales resultantes están relacionadas por un cambio de variables admisible donde $u = \pm 1$ y r, s, t en $\mathbb{Z}$.

Definición 4.6.3. Sea p un primo, E una curva elíptica dada un su forma de Weierstrass globalmente minimal y E_p su reducción módulo p. Decimos que dicha reducción es

- *buena* [*no singular, estable*] si E_p es nuevamente una curva elíptica, es decir, es no singular. Esta reducción puede ser a su vez
  (a) *ordinaria* si $E_p[p] \cong \mathbb{Z}/p\mathbb{Z}$,
  (b) *supersingular* si $E_p[p] = \{0\}$.
- *mala* [singular] si E_p no es una curva elíptica, es decir, es singular. En este caso tiene solamente un solo punto singular. Esta reducción puede ser a su vez
  (a) *multiplicativa* si E_p tiene un nodo,
  (b) *aditiva* si E_p tiene una cúspide.

Proposición 4.6.4. Sea E/K una curva elíptica y p primo. Entonces:
(a) E tiene reducción buena en p si $p \nmid \Delta$.
(b) E tiene reducción multiplicativa en p si $p|\Delta$ y $p \nmid c_4$.
(c) E tiene reducción aditiva en p si $p|\Delta$ y $p|c_4$.

Demostración. Inmediato de la Proposición 4.1.6. □

Definición 4.6.5. Decimos que una curva elíptica sobre $\mathbb{Q}$ es *semiestable* si la reducción módulo p de alguna de sus formas globalmente minimal, es a lo sumo multiplicativa. Es decir, para todo p primo, E_p es o bien una reducción buena o bien multiplicativa.

Si E tiene reducción multplicativa en p entonces se dice que *se parte* (*no se parte*) si las pendientes de las rectas tangentes en el nodo están en $\mathbb{F}_p$ (no están en $\mathbb{F}_p$).

Observación 4.6.6. Este tipo de reducciones es independiente de como E es puesta en su forma de Weierstrass globalmente minimal. En efecto, supongamos que E es una curva elíptica sobre $\mathbb{Q}$ y sean E_1 y E_2 dos formas de Weierstrass globalmente minimales de E. Por el Teorema 4.6.2 tendremos que estarán relacionadas por un cambio de variables admisible con $r, s, t, u \in \mathbb{Z}$ y $u = \pm 1$. Luego, por la Observación 4.1.8, $\Delta_{E_1} = (\pm 1)^{-12}\Delta_{E_2} = \Delta_{E_2}$. Por lo que tendrán el mismo discriminante. Además como están relacionadas por un cambio de variable admisible tendrán el mismo j-invariante, por lo que, al tener el mismo determinante, tendrán el mismo c_4. Por lo mencionado en la Observación 4.5.8, tener una buena reducción en p significa que $|\Delta|_p = 0$, y cuando esto vale las dos curvas E_1 y E_2, al ser isomorfas, tenemos que tienen la misma p-torsión y por lo tanto tienen el mismo tipo de reducción (ordinaria o supersingular). En el caso en que tengan reducción mala, es decir, el caso en el que $|\Delta|_p > 0$ sale directo por la Proposición 4.1.6 y al tener el mismo c_4.

Definimos ahora el conductor de mi curva elíptica.

Definición 4.6.7. Sea $E/\mathbb{Q}$ una curva elíptica. Definimos el *conductor* de E como $N_E = \prod_p p^{f_p}$ donde

$$f_p = \begin{cases} 0 & \text{si } E \text{ tiene buena reducción en } p, \\ 1 & \text{si } E \text{ tiene reducción multiplicativa en } p, \\ 2 & \text{si } E \text{ tiene reducción aditiva en } p \text{ y } p \notin \{2,3\}, \\ 2+\delta_p & \text{si } E \text{ tiene reducción aditiva en } p \text{ y } p \in \{2,3\}. \end{cases}$$

con $\delta_2 \leq 6$ y $\delta_3 \leq 3$. En nuestro caso particular solamente estaremos interesados en ver curvas elípticas semiestables, por lo que podremos obviar definir este último caso. Para una definición explícita del conductor en el caso de reducción aditiva en $p = 2, 3$ ver [Tat75].

Observación 4.6.8. En el caso en el que la curva elíptica $E/\mathbb{Q}$ sea semiestable, tendremos que su conductor N_E será el producto de los primos donde E tenga reducción mala. Es decir, el producto de los primos que dividen al discriminante de E.

4.6.2. L-serie de una curva elíptica

Para definir la L serie de una curva elíptica E sobre $\mathbb{Q}$ vamos a tomar dicha curva en alguna de sus formas de Weierstrass globalmente minimales. En dicha definición estará involucrada $\#E_p(\mathbb{F}_p)$ y Δ, por lo que debemos probar que dichos valores se mantienen invariantes. Sean E_1 y E_2 dos formas de Weierstrass globalmente minimales de E. Probamos en la Observación 4.6.6 que ambas curvas tienen el mismo discriminante. Además por el Teorema 4.6.2 tenemos que ambas van a estar relacionadas mediante un cambio de variable admisible con entradas enteras. Por lo que dicho cambio de variable admisible desciende, reduciendo dichas entradas módulo p, a un cambio de variable admisible entre $(E_1)_p$ y $(E_2)_p$, por lo que $\#(E_1)_p(\mathbb{F}_p) = \#(E_2)_p(\mathbb{F}_p)$. Luego el valor $\#E_p(\mathbb{F}_p)$ se mantendrá invariante.

Por la Observación 4.5.8 E_p es no singular si y solo si $p \nmid \Delta$ con Δ el discriminante de E (notar que la curva $\widetilde{E}$ construida en dicha observación estaba en forma de Weierstrass minimal).

Definimos $a_p(E) = p + 1 - \#E_p(\mathbb{F}_p)$.

Proposición 4.6.9. Sea $a_p(E)$ definido como arriba. Luego se cumple que

(a) Para cada primo p, $|a_p(E)| \leq p$.

(b) Para $p \nmid \Delta$ tenemos que las raices recíprocas de $1 - a_p(E)u + pu^2$ son menores o iguales a p en valor absoluto.

Demostración. (a) Sabemos que $\infty \in E_p(\mathbb{F}_p)$ y además para cada $x \in \mathbb{F}_p$ hay dos posibles valores para y de forma tal que $(x, y) \in E_p(\mathbb{F}_p)$. Luego $1 \leq \#E_p(\mathbb{F}_p) \leq 2p + 1$ y entonces $-p \leq a_p(E) = p + 1 - \#E_p(\mathbb{F}_p) \leq p$, es decir que $|a_p(E)| \leq p$.

(b) Las raices recíprocas (ver Sección A.2) son $\frac{1}{2}\left(a_p(E) \pm \sqrt{a_p(E)^2 - 4p}\right)$, que claramente son menores ó iguales a $|a_p(E)|$ en valor absoluto, y luego por parte (a) tenemos lo que queríamos. □

Definición 4.6.10. Sea E una curva elíptica y $a_p(E)$ como arriba. El *factor local* L para el primo p está dada por

$$L_p(u) = \begin{cases} \frac{1}{1-a_p(E)u+pu^2} & si \quad p \nmid \Delta, \\ \\ \frac{1}{1-a_p(E)u} & si \quad p|\Delta. \end{cases}$$

La **L-serie** de E es el producto de los factores locales L, con u reemplazado en el factor p por p^{-s}. Es decir

$$L(s,E) = \prod_{p|\Delta} \left[\frac{1}{1-a_p(E)p^{-s}}\right] \prod_{p\nmid\Delta} \left[\frac{1}{1-a_p(E)p^{-s}+p^{1-2s}}\right].$$

Proposición 4.6.11. El producto de Euler definido por $L(s,E)$ converge para $\operatorname{Re} s > 2$ y está dado por una serie de Dirichlet absolutamente convergente.

Demostración. Por parte (a) de la Proposición 4.6.9 y por la Proposición A.2.5 (usando que a_p es la raiz recíproca de $1-a_pX$) obtenemos que $\prod_{p|\Delta} \left[\frac{1}{1-a_pp^{-s}}\right]$ va a converger absolutamente para $\operatorname{Re} s > 2$ y define una serie de Dirichlet $\sum a_n n^{-s}$ de forma tal que dicho producto de Euler sea igual a la serie de Dirichlet.

Veamos que vale lo mismo para la otra productoria. La productoria $\prod_{p\nmid\Delta} \left[\frac{1}{1-a_p(E)p^{-s}+p^{1-2s}}\right]$ podemos describirla como $\prod_{p\nmid\Delta} \left[\frac{1}{1-P_p(p^{-s})}\right]$ donde $P_p(u) = a_p(E)u - pu^2$. Luego, por la parte (b) de la Proposición 4.6.9, tenemos que las raices recíprocas $r_p^{(j)}$ de $1-P_p(u)$ cumplen que $|r_p^{(j)}| \leq p$ para todo primo $p \nmid \Delta$. Luego usando la Proposición A.2.5 tendremos que $\prod_{p\nmid\Delta} \left[\frac{1}{1-a_p(E)p^{-s}+p^{1-2s}}\right]$ va a converger absolutamente para $\operatorname{Re} s > 2$ y define una serie de Dirichlet $\sum b_n n^{-s}$ de forma tal que dicho producto de Euler sea igual a la serie de Dirichlet. Luego usando el Teorema A.1.3 sale lo que queremos. □

Observación 4.6.12. En ambos casos donde se usó la Proposición A.2.5, se usó sin ocurrir que la productoria estuviese definida para todo primo. Sin embargo, podemos usar dicho resultado igualmente. Esto se debe a que podemos redefinir nuestras productorias para que sean sobre todo los primos, multiplicando por 1 en los primos donde no se esta definida la productoria, es decir tomando $P_p(x) = 0$ cuando p no aparezca en la productoria. En ese caso $1/(1-P_p(p^{-s})) = 1$. Luego como las raices recíprocas de $P_p(x) = 0$ son 0, sigue valiendo la desigualdad requerida en la Proposición A.2.5 y estamos.

Teorema 4.6.13. (Hasse) Sea E una curva elíptica sobre $\mathbb{Q}$ con coeficientes enteros. Para cada $p \nmid \Delta$, sea E_p la reducción módulo p de E. Entonces

$$|a_p(E)| < 2\sqrt{p}. \tag{4.9}$$

Corolario 4.6.14. El producto de Euler definido por $L(s,E)$ converge para $\operatorname{Re} s > \frac{3}{2}$ y está dado por una serie de Dirichlet absolutamente convergente.

Demostración. Sea $p \nmid \Delta$, y $a_p(E)$ definido previamente como $a_p(E) = p + 1 - \#E_p(\mathbb{F}_p)$. Luego las raices recíprocas de $1 - a_p(E)u + pu^2$ son $r = \frac{1}{2}\left(a_p(E) \pm \sqrt{a_p(E)^2 - 4p}\right)$. Por el teorema de Hasse $a_p(E)^2 - 4p < 0$. Por lo tanto $|r|^2 = \frac{1}{4}(a_p(E)^2 + (4p - a_p(E)^2)) = p$ y $|r| = \sqrt{p}$. Luego el resultado sigue por la Proposición A.2.5. □

Otro resultado importante respecto a las L-series es que esta se mantiene invariante por isogenías. Es decir:

Proposición 4.6.15. Sean E y E' dos curvas elípticas sobre $\mathbb{Q}$ e isógenas sobre $\mathbb{Q}$. Luego $L(s, E/\mathbb{Q}) = L(s, E'/\mathbb{Q})$.

Demostración. Ver [Kna92, §XI.9]. □

4.7. Representación de Galois

Denotaremos por $G_\mathbb{Q}$ al grupo de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ y lo llamaremos el *grupo absoluto de Galois de* $\mathbb{Q}$. Es claro que $\overline{\mathbb{Q}}$ es la unión de todos los cuerpos de números galoisianos. $\supseteq$ es clara al ser todas las extensiones de galois algebraicas, y $\subseteq$ es cierta pues si $q \in \overline{\mathbb{Q}}$ entonces $q \in F$ donde F es el cuerpo de descomposición del minimal de q en $\mathbb{Q}$, F es galois al ser el cuerpo de descomposición de un polinomio separable (toda extensión de un cuerpo de característica 0 es separable). Luego todo automorfismo $\sigma \in G_\mathbb{Q}$ fija los elementos de $\mathbb{Q}$ y se restringe a un automorfismo $\sigma|_F \in \mathrm{Gal}(F/\mathbb{Q})$ para cada cuerpo de números galoisiano F. La restricción de $G_\mathbb{Q}$ en $\mathrm{Gal}(F/\mathbb{Q})$ es suryectiva. Las restricciones son compatibles en el sentido

$$\sigma|_F = (\sigma|_{F'})|_F \text{ si } F \subset F'.$$

Recíprocamente, todo sistema compatible de automorfismos $\{\sigma_F\}$ sobre todos los cuerpos de números Galoisianos F se extiende a automorfismos en $\overline{\mathbb{Q}}$, es decir, a elementos de $G_\mathbb{Q}$. Luego lo previamente discutido describe a $G_\mathbb{Q}$ como el siguiente límite inverso

$$G_\mathbb{Q} = \varprojlim_F \{\mathrm{Gal}(F/\mathbb{Q})\}.$$

Al ser los grupos $\mathrm{Gal}(F/\mathbb{Q})$ finitos, $G_\mathbb{Q}$ es un grupo profinito. Dandole la topología discreta a $\mathrm{Gal}(F/\mathbb{Q})$, $G_\mathbb{Q}$ adquiere una topología relativa del espacio topológico (compacto por el Teorema de Tychonoff) $\prod \mathrm{Gal}(F/\mathbb{Q})$. Llamamos a esta topología la *topología de Krull* de $G_\mathbb{Q}$. Describamos una base de esta topología. Para cada $\sigma \in G_\mathbb{Q}$ y F un cuerpo de números Galois, definimos a $U_\sigma(F)$ como

$$U_\sigma(F) = \sigma \cdot \ker(G_\mathbb{Q} \to \mathrm{Gal}(F/\mathbb{Q})) = \sigma \cdot \mathrm{Gal}(\overline{\mathbb{Q}}/F).$$

Luego una base de la topología de Krull de $G_\mathbb{Q}$ resulta ser

$$\{U_\sigma(F) : \sigma \in G_\mathbb{Q}, F \text{ es un cuerpo de números Galois}\}.$$

Cada $U_{\mathrm{id}}(F)$ es un subgrupo normal abierto de $G_\mathbb{Q}$, y recíprocamente se puede ver que todo subgrupo normal abierto de $G_\mathbb{Q}$ es de la forma $U_{\mathrm{id}}(F)$ para algún cuerpo de números galois F.

Denotemos por $\overline{\mathbb{Z}}$ al anillo de enteros de $\overline{\mathbb{Q}}$, esto es $\overline{\mathbb{Z}} = \{x \in \overline{\mathbb{Q}} : x \text{ es un entero algebraico}\}$. Para cada ideal primo $\mathfrak{p}$ en $\overline{\mathbb{Z}}$ sobre p, definimos el *grupo de descomposición* de $\mathfrak{p}$, que denotaremos por $D_\mathfrak{p}$, como el subgrupo de $G_\mathbb{Q}$ que fija a $\mathfrak{p}$, es decir

$$D_\mathfrak{p} = \{\sigma \in G_\mathbb{Q} : \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

En particular, $D_\mathfrak{p}$ resulta ser un subgrupo de $G_\mathbb{Q}$. Luego cada $\sigma \in D_\mathfrak{p}$ actúa en $\overline{\mathbb{Z}}/\mathfrak{p}$ como $\sigma(x + \mathfrak{p}) = \sigma(x) + \mathfrak{p}$, y esto puede ser visto como una acción en $\overline{\mathbb{F}}_p$ (al ser $\overline{\mathbb{Z}}/\mathfrak{p} \cong \overline{\mathbb{F}}_p$). Se puede ver que la reducción

$$D_\mathfrak{p} \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$$

es continua y suryectiva. Luego llamamos un *Frobenius absoluto* sobre p a cualquier elemento $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$ en la preimagen del automorfismo de Frobenius $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Luego $\mathrm{Frob}_{\mathfrak{p}}$ está definido salvo un elemento en el núcleo de la reducción $D_{\mathfrak{p}} \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. A dicho núcleo lo llamaremos el grupo de inercia de $\mathfrak{p}$ y resulta ser

$$I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} : \sigma(x) \equiv x \pmod{\mathfrak{p}} \text{ para todo } x \in \bar{\mathbb{Z}}\}.$$

Enunciemos ahora las definiciones de representaciones del grupo $G_{\mathbb{Q}}$

Definición 4.7.1. Una n-representación de Galois de $G_{\mathbb{Q}}$ es un homomorfismo de grupos

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(k)$$

donde k es un cuerpo. (Más adelante se consideraran representaciones en donde solo le pedimos a k que sea un anillo). Si k es un cuerpo topológico nos centraremos en las representaciones que además de ser morfismos de $G_{\mathbb{Q}}$ en $\mathrm{GL}_n(k)$ (como grupos), son funciones continuas (viendo a $G_{\mathbb{Q}}$ con la Topología de Krull). Si $\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_n(k)$ es otra representación y existe una matriz $m \in \mathrm{GL}_n(k)$ tal que $\rho'(\sigma) = m^{-1}\rho(\sigma)m$ para todo $\sigma \in G_{\mathbb{Q}}$ entonces ρ y ρ' se dicen *equivalentes*. La equivalencia se denota por $\rho \sim \rho'$.

Si ρ es una representación de galois de dimensión n sobre k entonces decimos que es de *Artin* si $k \subseteq \mathbb{C}$ y *l-ádica* si $k \subseteq \bar{\mathbb{Q}}_\ell$.

Definición 4.7.2. Sea ρ una representación de Galois y sea p primo. Entonces ρ se dice *no ramificada en p* si $I_{\mathfrak{p}} \subset \ker \rho$ para todo ideal primo $\mathfrak{p} \in \overline{\mathbb{Z}}$ sobre p. En caso contrario se dice que ramifica en p.

Definición 4.7.3. Sea ρ una representación n-dimensional de Galois de $G_{\mathbb{Q}}$ sobre el cuerpo k. Sea $V = k^n$ el k-espacio vectorial estandard de dimensión n. Mediante la acción de $G_{\mathbb{Q}}$ en V dada por $\sigma \cdot v = \rho(\sigma)v$, V es un $k[G_{\mathbb{Q}}]$-módulo. Decimos que ρ es *irreducible* si el único k-subespacio $W \lneq V$ tal que $\sigma W \subseteq W$ para todo $\sigma \in G_{\mathbb{Q}}$ es el subespacio nulo.

4.8. Representación de Galois asociada a curvas elípticas

En la presente sección estaremos interesados en asociarle a cada curva elíptica sobre $\mathbb{Q}$ una representación de Galois. Sea $E/\mathbb{Q}$ una curva elíptica. Nos gustaría describir una acción de $G_{\mathbb{Q}}$ en $E[n]$, pues, de esta forma, podremos definir una representación asociada a E. Vimos en el Teorema 4.4.9 que $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. Sea entonces $\{P_1, P_2\}$ una base de $E[n]$ y $\sigma \in G_{\mathbb{Q}}$. Como σ es un isomorfismo, $\sigma(P_1)$ y $\sigma(P_2)$ volverán a ser elementos de $E[n]$. Por lo que

$$(\sigma(P_1), \sigma(P_2)) = (P_1, P_2)\begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}$$

donde $\alpha_\sigma, \beta_\sigma, \gamma_\sigma, \delta_\sigma$ son elementos en $\mathbb{Z}/n\mathbb{Z}$, unívocamente determinados por σ. Luego la acción de $G_{\mathbb{Q}}$ en $E[n]$ está dada por $\sigma \cdot (P_1, P_2) = (\sigma(P_1), \sigma(P_2))$.

Se puede chequear facilmente (ver [Tat92, VI.3]) que, si $\psi \in G_{\mathbb{Q}}$, entonces

$$\begin{pmatrix} \alpha_{\sigma\circ\psi} & \beta_{\sigma\circ\psi} \\ \gamma_{\sigma\circ\psi} & \delta_{\sigma\circ\psi} \end{pmatrix} = \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}\begin{pmatrix} \alpha_\psi & \beta_\psi \\ \gamma_\psi & \delta_\psi \end{pmatrix}.$$

Luego,

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}\alpha_{\sigma^{-1}} & \beta_{\sigma^{-1}}\\ \gamma_{\sigma^{-1}} & \delta_{\sigma^{-1}}\end{pmatrix}\begin{pmatrix}\alpha_{\sigma} & \beta_{\sigma}\\ \gamma_{\sigma} & \delta_{\sigma}\end{pmatrix} = \begin{pmatrix}\alpha_{\sigma} & \beta_{\sigma}\\ \gamma_{\sigma} & \delta_{\sigma}\end{pmatrix}\begin{pmatrix}\alpha_{\sigma^{-1}} & \beta_{\sigma^{-1}}\\ \gamma_{\sigma^{-1}} & \delta_{\sigma^{-1}}\end{pmatrix}$$

por lo que cada matriz $\begin{pmatrix}\alpha_{\sigma} & \beta_{\sigma}\\ \gamma_{\sigma} & \delta_{\sigma}\end{pmatrix}$ pertenece a $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Luego definimos la representación

$$\bar{\rho}_{E,n} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Está bien definida y es un morfismo de grupos por lo que mencionamos anteriormente.

Enunciemos ahora un resultado respecto a este tipo de representaciones que usaremos más adelante.

Teorema 4.8.1. (Mazur) Sea $\ell \geq 5$ un primo y $E/\mathbb{Q}$ una curva elíptica semiestable. Luego, la representación $\bar{\rho}_{E,\ell}$ es irreducible.

Demostración. (Idea) Supongamos que $\bar{\rho}_{E,\ell}$ es reducible, luego existe un subespacio propio de orden p de $E[\ell]$ invariante por la acción de $\bar{\rho}_{E,\ell}(\sigma)$. Usando resultados de semiestabilidad (Ver [Ser87, Proposición 6]), se puede probar que E es isógena sobre $\mathbb{Q}$ a una curva elíptica E' con un punto racional de orden ℓ y dos puntos de orden 2, por lo que $\#E'_{\mathrm{tor}}(\mathbb{Q}) \geq 4\ell \geq 20$. Esto contradice el Teorema 4.2.4, ya que este nos dice que la parte de torsión de los puntos racionales de una curva elíptica es un grupo de orden a lo sumo 16. Por lo tanto $\bar{\rho}_{E,\ell}$ es irreducible. □

Si ℓ es un número primo, multiplicar por ℓ de $E[\ell^{k+1}]$ en $E[\ell^k]$ nos da los siguientes mapas

$$E[\ell] \longleftarrow E[\ell^2] \longleftarrow E[\ell^3] \longleftarrow \dots$$

Definimos el módulo ℓ-ádico de Tate de E como el límite inverso

$$\mathrm{Ta}_{\ell}(E) = \varprojlim_{n}\{E[\ell^n]\}.$$

Elelgimos una base (P_n, Q_n) de $E[\ell^n]$ para cada $n \in \mathbb{N}$ de tal forma que

$$[\ell]P_{n+1} = P_n \text{ y } [\ell]Q_{n+1} = Q_n,\ n \in \mathbb{N}.$$

Luego cada base determina un isomorfismo $E[\ell^n] \xrightarrow{\sim} (\mathbb{Z}/\ell^n\mathbb{Z})^2$, y luego

$$\mathrm{Ta}_{\ell}(E) \cong \mathbb{Z}_{\ell}^2.$$

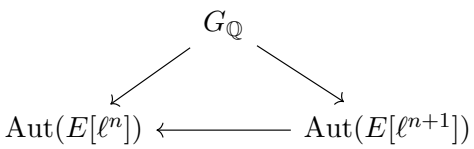
Por el Teorema 4.4.13 tenemos que, para cada $n \in \mathbb{N}$, $\mathbb{Q}(E[\ell^n])$ es un cuerpo de números Galois. Por lo que tenemos la restricción

$$\begin{aligned} G_{\mathbb{Q}} &\to \mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q})\\ \sigma &\mapsto \sigma|_{\mathbb{Q}(E[\ell^n])}\end{aligned}$$

y hay una inyección

$$\mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(E[\ell^n]).$$

Además estos mapas son compatibles en el sentido de que, para todo $n \in \mathbb{N}$, el siguiente diagrama conmuta:



Es decir,

$$\sigma|_{\mathbb{Q}(E[\ell^n])} = [l] \circ \sigma|_{\mathbb{Q}(E[\ell^{n+1}])}.$$

De esta última observación se deduce que $G_{\mathbb{Q}}$ actua en $\mathrm{Ta}_\ell(E)$. Si $(a_n)_{n\in\mathbb{N}}$ está en $\mathrm{Ta}_\ell(E)$, y $\sigma \in G_{\mathbb{Q}}$ Definimos la acción de $G_{\mathbb{Q}}$ en $\mathrm{Ta}_\ell(E)$ como

$$\sigma \cdot ((a_n)_{n\in\mathbb{N}}) = \left(\sigma|_{\mathbb{Q}(E[\ell^n])}(a_n)\right)_{n\in\mathbb{N}}$$

y esto último, por lo que observamos antes es igual a $\left([l] \circ \sigma|_{\mathbb{Q}(E[\ell^{n+1}])}(a_n)\right)_{n\in\mathbb{N}}$, lo cual pertenece a $\mathrm{Ta}_\ell(E)$ pues

$$[l]([l] \circ \sigma|_{E[\ell^{n+2}]}(a_{n+1})) = [l](\sigma|_{E[\ell^{n+1}]}(a_{n+1})).$$

Por lo tanto $\mathrm{Ta}_\ell(E)$ es un $G_{\mathbb{Q}}$-módulo.

Cada base (P_n, Q_n) determina un isomorfismo

$$\mathrm{Aut}(E[\ell^n]) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}).$$

pues teníamos el isomorfismo $E[\ell^n] \xrightarrow{\sim} (\mathbb{Z}/\ell^n\mathbb{Z})^2$, y si $\sigma \in \mathrm{Aut}(E[\ell^n])$ entonces $\sigma(P_n) = a_\sigma P_n + b_\sigma Q_n$ y $\sigma(Q_n) = c_\sigma P_n + d_\sigma Q_n$ por lo que el isomorfismo va a venir dado por

$$\sigma \mapsto \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}.$$

Por lo tanto tendremos un isomorfismo

$$\mathrm{Aut}(\mathrm{Ta}_\ell(E)) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Como $G_{\mathbb{Q}}$ actúa en $\mathrm{Ta}_\ell(E)$ resulta que tenemos un homomorfismo

$$\rho_{E,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \subset \mathrm{GL}_2(\mathbb{Q}_\ell)$$

dado de la siguiente manera: Si $\sigma \in G_{\mathbb{Q}}$ entonces σ induce un elemento en $\mathrm{Aut}(\mathrm{Ta}_\ell(E))$ dado por la acción de σ en $\mathrm{Ta}_\ell(E)$. Es un automorfismo pues $\sigma|_{\mathbb{Q}(E[\ell^n])}$ es un automorfismo de $E[\ell^n]$. Dicha asociación es un morfismo al serlo σ y por lo tanto tengo un morfismo de $G_{\mathbb{Q}}$ en $\mathrm{Aut}(\mathrm{Ta}_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$

Más aún, $\rho_{E,\ell}$ es continua. En efecto, como $\mathrm{GL}_2(\mathbb{Z}_\ell)$ resulta ser un grupo topológico basta ver que preimagen de entornos abiertos de la identidad es un abierto en $G_{\mathbb{Q}}$ con la topología de Krull. El grupo $\mathrm{GL}_2(\mathbb{Q}_\ell)$ adquiere una topología como subconjunto de $\mathbb{Q}_\ell^4$. Una base de $\mathbb{Q}_\ell$ es $\{U_x(n) = x + \ell^n\mathbb{Z}_\ell : x \in \mathbb{Q}_\ell, n \in \mathbb{N}\}$, por lo que una base de $\mathbb{Q}_\ell^4$ resulta ser $\{U_v(n) : v \in \mathbb{Q}_\ell^4, n \in \mathbb{N}\}$, donde ahora $U_v(n) = v + \ell^n\mathbb{Z}_\ell^4$ (para más detalles al respecto ver [Shu05, §IX.2]). Si $m \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ entonces $U_m(n)$ resulta ser $U_m(n) = m(\mathrm{Id} + \ell^n \mathrm{M}_2(\mathbb{Z}_\ell))$, o

$$U_m(n) = m \cdot \ker(\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})).$$

Sea $U_{\mathrm{Id}}(n)$ un entorno abierto de Id, entonces

$$\begin{aligned}\rho_{E,\ell}^{-1}(U_{\mathrm{Id}}(n)) &= \rho_{E,\ell}^{-1}(\ker(\mathrm{Aut}(\mathrm{Ta}_\ell(E)) \to \mathrm{Aut}(E[\ell^n])) \\ &= \rho_{E,\ell}^{-1}(\{\sigma \in \mathrm{Aut}(\mathrm{Ta}_\ell(E)) : \sigma|_{E[\ell^n]} = \mathrm{id}_{E[\ell^n]}\}) \\ &= \{\sigma \in G_{\mathbb{Q}} : \sigma|_{\mathbb{Q}(E[\ell^n])} = \mathrm{id}\} \\ &= \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(E[\ell^n])) \\ &= \ker\{G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q})\}\end{aligned}$$

que es un abierto en $G_{\mathbb{Q}}$ al ser $\mathbb{Q}(E[\ell^n])$ un cuerpo de números Galois. De hecho, con la notación vista cuando dimos la base de $G_{\mathbb{Q}}$, resulta ser $U_{\mathrm{id}}(\mathbb{Q}(E[\ell^n]))$.

Llamamos a $\rho_{E,\ell}$ la *representación de Galois 2-dimensional asociada a E en ℓ.*

Observación 4.8.2. Por como construimos a $\rho_{E,\ell}$ y a $\bar{\rho}_{E,\ell}$ tenemos que $\bar{\rho}_{E,\ell^n} \equiv \rho_{E,\ell} \pmod{\ell^n}$. Por lo que en particular, si $\rho_{E,\ell}$ no ramifica en ℓ entonces $\bar{\rho}_{E,\ell}$ tampoco lo hará.

Teorema 4.8.3. (Néron-Ogg-Shafarevich) Sea $E/\mathbb{Q}$ una curva elíptica. E tiene reducción buena en ℓ si y solo si $\rho_{E,p}$ no ramifica en ℓ para algún primo $p \neq \ell$ si y solo si $\rho_{E,p}$ no ramifica en ℓ para todo primo $p \neq \ell$.

Demostración. Ver [Sil09, Teorema 7.1] □

Teorema 4.8.4. Sea ℓ primo y sea $E/\mathbb{Q}$ una curva elíptica con conductor N. La representación de Galois $\rho_{E,\ell}$ no ramifica en todo primo $p \nmid \ell N$. Para dichos primos p sea $\mathfrak{p} \subset \bar{\mathbb{Z}}$ un ideal primo sobre p. Luego la ecuación característica de $\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ es

$$x^2 - a_p(E)x + p = 0.$$

La representación de Galois $\rho_{E,\ell}$ es irreducible.

Demostración. Ver [Shu05, §IX.4.] □

4.9. La curva de Hallegouarch-Frey

En esta sección introduciremos la idea introducida por Hellegourach y desarrolada por Frey que mencionamos al principio del Capítulo. Dicha idea relaciona hipotéticas soluciones al último Teorema de Fermat con ciertas curvas elípticas particulares. Suponiendo que existe una solución al Último Teorema de Fermat $a^\ell + b^\ell = c^\ell$, con $\ell \geq 5$, vamos a asociarle la curva elíptica

$$E : Y^2Z = X(X - a^\ell Z)(X + b^\ell Z).$$

A dicha curva la llamaremos Curva de Hellegourach-Frey. Como mencionamos al principio del Capítulo 1 podemos suponer que $\mathrm{mcd}(a, b, c) = 1$, por lo que nos gustaría analizar curvas de la forma

$$E : Y^2Z = X(X - AZ)(X + BZ)$$

en donde A y B son no nulos y $\mathrm{mcd}(A, B) = 1$.

Definición 4.9.1. Llamamos a una curva ABC, denotada por $E_{A,B,C}$, a la curva elíptica

$$E_{A,B,C} : Y^2Z = X(X - AZ)(X + BZ)$$

en donde A y B son no nulas, $A + B - C = 0$ y $\text{mcd}(A, B, C) = 1$. Esta ultima relación la llamaremos *relación ABC*.

Lema 4.9.2. Sean $A, B, C \in \mathbb{Z}$ que satisface la relación ABC, y sea $E_{A,B,C}$ la curva ABC correspondiente. Entonces

(a) $\Delta = 16(ABC)^2$ y $j(E_{A,B,C}) = 2^8(A^2 + BC)^3(ABC)^{-2}$.

(b) El *discriminante minimal* $\Delta_{E_{A,B,C}}$ de E está dado por

$$\Delta_{E_{A,B,C}} = 16(ABC)^2 \text{ o } \Delta_{E_{A,B,C}} = 2^{-8}(ABC)^2$$

(c) Si p es un primo impar entonces la curva $E_{A,B,C}$ tiene reducción buena módulo p si $p \nmid ABC$, y tiene reducción multiplicativa módulo p para todo primo impar que divida a ABC.

(d) El conductor de $E_{A,B,C}$ es

$$N_{E_{A,B,C}} = \prod_{p|ABC} p.$$

Demostración. (a) De la expresión de $E_{A,B,C}$ tenemos que su discriminante es

$$\Delta = 16A^2B^2(A + B)^2 = 16A^2B^2C^2 = 16(ABC)^2.$$

Además, nuevamente de la expresión de la curva $E_{A,B,C}$ tenemos que $c_4 = 16(A^2 + AB + B^2)$. Luego

$$j(E_{A,B,C}) = \frac{c_4^3}{\Delta} = \frac{(16(A^2 + AB + B^2))^3}{16(ABC)^2} = 2^8(A^2 + BC)^3(ABC)^{-2}.$$

(b) Ver [Sil09, Lema 11.3].

(c) Sale de la parte (a) y usando el Teorema 4.6.4. En efecto, si $p \nmid ABC$ entonces $p \nmid \Delta$ y por dicho teorema $E_{A,B,C}$ tendrá reducción buena en p. Si $p|ABC$ entonces $p|\Delta$. Si $p|A$ o $p|B$, entonces, como $\text{mcd}(A, B) = 1$, tenemos que $p \nmid c_4$, por lo que $E_{A,B,C}$ tiene reducción multiplicativa en p. De forma similar, si $p|C$, entonces $A + B \equiv 0 \pmod{p}$, luego $c_4 \equiv 16A^2 \pmod{p}$, y por lo tanto nuevamente $p \nmid c_4$ y $E_{A,B,C}$ tiene reducción multiplicativa en p.

(d) Inmediato de (c) y de la Observación 4.6.8. □

En el caso de las curvas de Frey, permutando a, b, c, podemos suponer que b es par. Más aún podemos suponer que $a \equiv -1 \pmod{4}$. En efecto si $a \equiv 1 \pmod{4}$ entonces tomamos la solución $(-a, -b, -c)$ en donde $-a \equiv -1 \pmod{4}$. Luego en particular, al ser $\ell \geq 5$, $a^\ell \equiv -1 \pmod{4}$ y $b^\ell \equiv 0 \pmod{32}$. Nos gustaría ver ahora entonces, propiedades acerca de la reducción de curvas ABC en donde $A \equiv -1 \pmod{4}$ y $B \equiv 0 \pmod{32}$. Más aún, vamos a probar que la reducción siempre va a ser a lo sumo multiplicativa para $A \equiv -1 \pmod{4}$ y $B \equiv 0 \pmod{16}$.

Supongamos que tenemos entonces una curva ABC en donde $A \equiv -1 \pmod 4$ y $B \equiv 0 \pmod{16}$. Tenemos, mediante el cambio de variable admisible $X = 4X', Y = 8Y' + 4X'$, la curva

$$Y^2Z + XYZ = X^3 + \frac{B - A - 1}{4}X^2Z - \frac{AB}{16}XZ^2 \tag{4.10}$$

cuyo discriminante resulta ser $2^{-8}ABC$. Por el Lema 4.9.2 (b) tenemos que dicha curva será una forma de Weierstrass globalmente minimal de $E_{A,B,C}$. Además, por la parte (c) de dicho Lema tiene reducción buena o multiplicativa para todo primo p impar. Veamos que también sucede lo mismo para el primo $p = 2$. Reduciendo la curva minimal (4.10) módulo 2, y usando que $A \equiv -1 \pmod 4$ y $B \equiv 0 \pmod{16}$ tenemos que

$$Y^2Z + XYZ = \begin{cases} X^3 & si \quad A \equiv 7 \pmod 8, \\ X^3 + X^2Z & si \quad A \equiv 3 \pmod 8. \end{cases}$$

Calculando las derivadas parciales correspondientes se ve que el punto singular de la curva es el $[0, 0, 1]$. Mirando a la curva en su forma afín tenemos que

$$x^3 = \begin{cases} y(x + y) & si \quad A \equiv 7 \pmod 8, \\ (y - \alpha x)(y - \beta x) & si \quad A \equiv 3 \pmod 8, \end{cases}$$

donde β es raíz de $\beta^2 + \beta - 1$ y $\alpha = -1 - \beta$. Se ve que entonces en ambos casos que las dos rectas tangentes en el $(0, 0)$ son distintas, por lo que tendrá un nodo en dicho punto singular. Por lo tanto $E_{A,B,C}$ tiene reducción multiplicativa en 2. Podemos enunciar entonces el siguiente resultado:

Teorema 4.9.3. Si $A \equiv -1 \pmod 4$ y $B \equiv 0 \pmod{16}$, entonces $E_{A,B,C}$ es semiestable y su conductor es el producto de los primos que dividen a ABC.

Corolario 4.9.4. Toda curva de Hellegourach-Frey es semiestable.

4.10. Curva de Tate y ramificación de $\bar{\rho}_{E,\ell}$

En esta sección nos gustaría estudiar la ramificación de la representación $\bar{\rho}_{E,\ell}$ definida en la Sección 4.8. Para esto enunciaremos primero unos resultados probados por Tate.

Denotaremos por $q \in \mathbb{Q}_p$ a un número p-ádico tal que $|q|_p < 1$, y a $\langle q \rangle$ al subgrupo de $\mathbb{Q}_p^*$ generado por q.

Dado $q \in \mathbb{Q}_p^*$ con $|q|_p < 1$, Tate construye la siguiente curva, llamada la *Curva de Tate*

$$E_q : y^2 + xy = x^3 + a_4x + a_6$$

cuyos coeficientes vienen dados por las siguientes series de potencias

$$a_4(q) = -5\sum_{n=1}^{\infty}\frac{n^3q^n}{1 - q^n}, \quad a_6(q) = -\frac{1}{12}\sum_{n=1}^{\infty}\frac{(7n^5 + 5n^3)q^n}{1 - q^n}.$$

Proposición 4.10.1. Las series $a_4(q)$ y $a_6(q)$ convergen en $\mathbb{Q}_p$ a elementos en $\mathbb{Z}_p$ y el discriminante y j-invariante de E_q vienen dados por

$$\Delta = q\prod_{n\geq 1}(1 - q^n)^{24} \text{ y } j(E_q) = \frac{1}{q} + 744 + 196884q + \dots$$

Demostración. Ver [Tat93]. □

Además Tate prueba también el siguiente resultado:

Proposición 4.10.2. (Tate) Sea $q \in \mathbb{Q}_p^*$ con $|q|_p < 1$. Entonces
(a) Existe un isomorfismo $\phi : \bar{\mathbb{Q}}_p^*/\langle q \rangle \xrightarrow{\sim} E_q(\bar{\mathbb{Q}}_p)$.
(b) El ismomorfismo ϕ es compatible con la acción de $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. Es decir

$$\phi(u^\sigma) = \phi(u)^\sigma \text{ para todo } u \in \bar{\mathbb{Q}}_p^*,\ \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p).$$

En particular, para cualquier extensión algebraica $L/\mathbb{Q}_p$ tenemos el siguiente isomorfismo inducido por ϕ,

$$\phi : L^*/\langle q \rangle \xrightarrow{\sim} E_q(L).$$

Demostración. Ver [Tat93, Teorema 1]. □

Observación 4.10.3. Tate no solo prueba la Proposición 4.10.2 para $\mathbb{Q}_p$, si no para cualquier completación respecto a una valuación discreta.

De estas dos últimas proposiciones se deduce que $|j(E_q)|_p > 1$ por lo que $j(E_q) \notin \mathbb{Z}_p$. La reducción mod p de E_q queda la curva

$$y^2 + xy = x^3.$$

Se ve de forma fácil que esta curva admite un punto singular en $(0,0)$ cuyas rectas tangentes son las rectas $y = 0$ y $x + y = 0$. Por lo tanto la curva E_q tiene reducción multiplicativa partida en p con tangentes racionales en el punto $(0,0)$. Más aún, se tiene la siguiente recíproca a lo previamente enunciado:

Teorema 4.10.4. (Tate) Se cumplen los siguientes resultados
(a) Sea $j_0 \in \mathbb{Q}_p^*$ tal que $|j_0|_p > 1$. Luego existe $q \in \mathbb{Q}_p^*$ con $|q|_p < 1$ tal que $E_q/\mathbb{Q}_p$ tiene j-invariante j_0. La curva E_q es caracterizada salvo isomorfismo sobre $\mathbb{Q}_p$ por $j(E_q)$ y el hecho de que tiene reducción multiplicativa partida en p.
(b) Supongamos que $E/\mathbb{Q}_p$ es una curva elíptica con $|j(E)|_p > 1$ que no tiene reducción multiplicativa partida en p. Por el item (a) existe un elemento $q \in \mathbb{Q}_p^*$ tal que $j(E) = j(E_q)$. Luego existe una única extensión cuadrática $L/\mathbb{Q}_p$ tal que E es isomorfa E_q sobre L. La extensión $L/\mathbb{Q}_p$ es no ramificada si y solo si E tiene reducción multiplicativa (no partida).

Demostración. Ver [Sil09, §C.14, Teorema 14.1]. □

Sea $E = E_{a^p,b^p,c^p}$ una curva de Hellegourach-Frey asociada a una solución del Teorema de Fermat para $p \geq 5$. Denotemos por K_p al cuerpo de números $\mathbb{Q}(E[p])$. Vimos en el Teorema 4.4.13 y en la Proposición 4.4.14 que K_p es un cuerpo de números y que contiene a una raiz p-primitiva de la unidad ζ_p. Nos gustaría analizar la ramificación de K_p en 2 y en p ya que, como veremos en la demostración del Corolario 4.10.6, ésta estará relacionada con la ramificación de $\bar{\rho}_{E,p}$.

Teorema 4.10.5. (Hallegouarch) Sea ℓ un primo dividiendo a abc. Luego el cuerpo K_p asociado a la curva elíptica $E = E_{a^p,b^p,c^p}$ puede ser considerado como un subcuepro de $\mathbb{Q}_\ell(\zeta_p, 2^{1/p})$ (o de $\mathbb{Q}_\ell(\alpha^{1/2}, \zeta_p, 2^{1/p})$ donde $\mathbb{Q}_\ell(\alpha^{1/2})$ es no ramificada).

Demostración. Por la Proposición 4.4.14 K_p contiene a una raiz p-primitiva de la unidad ζ_p. Por el Lema 4.9.2 (a) tenemos que $j(E) = 2^8(a^{2p} + b^p c^p)^3(abc)^{-2p}$. Luego, usando que $\mathrm{mcd}(a, b, c) = 1$ tenemos que $v_2(j(E)) = 8 - 2pv_2(abc)$ y $v_\ell(j(E)) = -2pv_\ell(abc)$ cuando $\ell \neq 2$. En ambos casos, al ser $p \geq 5$, tenemos que $v_\ell(j(E)) < 0$, por lo que $|j|_\ell > 1$, y que son coprimos dos a dos, para todo primo ℓ. Como $\ell | abc$ tenemos por el Lema 4.9.2 que E tiene reducción multiplicativa en ℓ. Luego por el Teorema 4.10.4 tenemos que E es isomorfa a una curva E_q sobre $\mathbb{Q}_\ell$ o sobre una extensión cuadrática de $\mathbb{Q}_\ell$ no ramificada.

Supongamos que el isomorfismo es sobre $\mathbb{Q}_\ell$ y denotemos por L al cuerpo $\mathbb{Q}_\ell(\zeta_p, 2^{1/p})$. Luego por la Proposición 4.10.2 (c) tenemos que $E_q(L)$ es isomorfo a $L^*/\langle q \rangle$. Como $j(E)$ es salvo isomorfismo una potencia p-ésima en L, lo mismo vale para q. Luego existe $q' \in L$ y una unidad u tal que $q = u(q')^p$. Por lo tanto $L^*/\langle q \rangle$ contiene al grupo $\langle q', \zeta_p \rangle / \langle q \rangle$ que es isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong E[p]$. Por lo que $E[p] \subset L^*/\langle q \rangle \cong E_q(L)$, obteniendo que $K_p \subset L$. Para el caso en el cual el isomorfismo sea sobre una extensión cuadrática no ramificada $\mathbb{Q}(\alpha^{1/2})$ se toma $L = \mathbb{Q}_\ell(\alpha^{1/2}, \zeta_p, 2^{1/p})$ y se repite el mismo procedimiento. □

Corolario 4.10.6. Para $p \geq 5$, la representación $\bar{\rho}_{E_{a^p,b^p,c^p},p}$ no ramifica fuera de $2p$.

Demostración. Sea $\ell \neq p$. Si $l \nmid abc$ entonces, por el Lema 4.9.2, $l \nmid \Delta$ y E tiene reducción buena en ℓ. Por el Teorema 4.8.3 $\rho_{E,p}$ no ramifica en ℓ, y luego por la Observación 4.8.2 $\bar{\rho}_{E,p}$ tampoco lo hará. Si $\ell | abc$ entonces por el Teorema 4.10.5 tenemos que K_p no ramifica en ℓ si $\ell \neq 2, p$. Luego sigue, de la Teoría Algebraica de Números, que K_p tiene grupo de inercia I (sobre ℓ) trivial, lo cual implica que la acción de I en $E[p]$ es trivial. Sigue entonces, de la definición de $\bar{\rho}_{E,p}$, que $\bar{\rho}_{E,p}$ no ramifica en ℓ con $\ell \neq 2, p$. Por lo tanto $\bar{\rho}_{E,p}$ no ramifica fuera de $2p$. □

Capítulo 5

Formas Modulares

En este Capítulo se hablará acerca de las formas modulares. Estas funciones van a jugar un gran rol importante en lo que fue el Trabajo de Eichler-Shimura [Shi71], el cual vincula ciertas formas modulares con curvas elípticas. Este trabajo motivaría la conjetura de Shimura-Taniyama (ahora Teorema) que jugaría un rol importante en la demostración del Último Teorema de Fermat. La bibliografía en la cual nos centraremos en el presente capítulo es la siguiente: [Kna92] y [Shu05].

5.1. Subgrupos de Hecke

Definición 5.1.1. Definamos para cada $N \in \mathbb{N}$ el subgrupo de congruencia $\Gamma_0(N)$ de $\mathrm{SL}_2(\mathbb{Z})$ como

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod \mathrm{N} \right\},$$

Al subgrupo $\Gamma_0(N)$ se lo llama el *subgrupo de Hecke de nivel N* . Denotemos a las matrices de $M_{2\times 2}(\mathbb{Z})$ de determinante N como $M(N)$, a las matrices primitivas de $M(N)$ como $M^*(N)$ y a $\mathcal{H} = \{z \in \mathbb{C} | \operatorname{Im} z > 0\}$ al semiplano complejo superior.

Lema 5.1.2. $M^* = \cup_\alpha \mathrm{SL}_2(\mathbb{Z})\alpha$ donde α recorre todas las matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ donde $ad = N$, $d > 0$, $0 \leq b < d$, y a, b, c coprimos dos a dos.

5.2. Formas Modulares y Cuspidales

Definimos la acción de $\mathrm{SL}_2(\mathbb{Z})$ en $\mathcal{H}$ de la siguiente forma:

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d} \quad \text{con} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Primero, para ver que es una acción, deberíamos ver que está bien definida. Sea $\tau = x+iy \in \mathcal{H}$ y $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Luego, realizando cuentas, podemos ver que

$$\operatorname{Im}(\gamma\tau) = \frac{(ad - bc)y}{(cx + d)^2 + (cy)^2} = \frac{y}{(cx + d)^2 + (cy)^2} > 0,$$

por lo que está bien definida. Veamos que es una acción. Claramente $\mathrm{Id}\,\tau = \tau$. Sean ahora $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ y $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ matrices en $\mathrm{SL}_2(\mathbb{Z})$. Luego

$$\begin{aligned} \gamma(\gamma'\tau) &= \frac{a\left(\frac{a'\tau+b'}{c'\tau+d'}\right)+b}{c\left(\frac{a'\tau+b'}{c'\tau+d'}\right)+d} \\ &= \frac{(aa'+bc')\tau+(ab'+bd')}{(ca'+dc')\tau+(cb'+dd')} \\ &= (\gamma\gamma')\tau. \end{aligned}$$

Por lo tanto es una acción.

Es conveniente extender esta acción a la Esfera de Riemann $\mathbb{C}\cup\{\infty\}$ definiendo $\gamma(\infty) = \frac{a}{c}$ y $\gamma(-\frac{d}{c}) = \infty$.

Denotemos ahora $\delta(\gamma,\tau) = c\tau + d$ con $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Notar que $\delta(\gamma,\tau)$ satisface

$$\delta(\gamma_1\gamma_2,\tau) = \delta(\gamma_1,\gamma_2\tau)\delta(\gamma_2,\tau), \tag{5.1}$$

$$\delta(\gamma,\tau)^{-1} = \delta(\gamma^{-1},\gamma\tau). \tag{5.2}$$

Además si $f : \mathcal{H} \to \mathbb{C}$ es holomorfa, $\beta \in \mathrm{SL}_2(\mathbb{Z})$ y $k \in \mathbb{Z}$ definiremos a $f|_k[\beta] : \mathcal{H} \to \mathbb{C}$ como $f|_k[\beta](\tau) = \delta(\beta,\tau)^{-k} f(\beta\tau)$.

Observación 5.2.1. Denotando por C al conjunto de funciones holomorfas $f : \mathcal{H} \to \mathbb{C}$ y fijando $k \in \mathbb{Z}$, tenemos que la aplicación $\mathrm{SL}_2(\mathbb{Z}) \times C \to C$ dada por $(\alpha, f) \mapsto f|_k[\alpha]$ es una acción de $\mathrm{SL}_2(\mathbb{Z})$ en C. En efecto $f|_k(\mathrm{Id})(\tau) = \delta(\mathrm{Id},\tau)^{-k} f(\tau) = (0\tau + 1)^{-k} f(\tau) = f(\tau)$ y si $\alpha, \beta \in \Gamma$ entonces, utilizando (5.1), tenemos que $(f|_k[\alpha])|_k[\beta](\tau) = \delta(\beta,k)^{-k}\delta(\alpha,\beta\tau)^{-k} f(\alpha\beta\tau) = \delta(\alpha\beta,\tau)^{-k} f(\alpha\beta,\tau) = f|_k[\alpha\beta](\tau)$.

Para una matriz α de determinante positivo denotamos $\alpha^{\#} = (\det\alpha)^{-\frac{1}{2}}\alpha$. De esa forma definimos $f|_k[\alpha] = f|_k[\alpha^{\#}]$ para cualquier α matriz 2×2 con determinante positivo.

Definición 5.2.2. Sea $k \in \mathbb{Z}$. Una función holomorfa en $\mathcal{H}$ que satisfaga

$$f = f|_k[\gamma] \text{ para todo } \gamma \in \Gamma_0(N)$$

es llamada una *forma modular sin restricción* de *peso* k respecto a $\Gamma_0(N)$.

Observación 5.2.3. Notar que tomando $\gamma = -\mathrm{Id} \in \Gamma_0(N)$ obtenemos que $f(\tau) = f(\gamma\tau) = \delta(\gamma,\tau)^k f(\tau) = (-1)^k f(\tau)$ para todo $\tau \in \mathcal{H}$. Si k es impar esto vale solo para la función nula, por lo cual basta considerar las formas modulares sin restricción de peso par.

Denotamos el dominio fundamental de la acción de $\mathrm{SL}_2(\mathbb{Z})$ en $\mathcal{H}$ como R. Claramente cada $\beta^{-1}R$ con $\beta \in \mathrm{SL}_2(\mathbb{Z})$ vuelve a ser de nuevo dominio fundamental. Consideremos a ∞ como el punto de borde de $\mathcal{H}$. De esta forma $\beta^{-1}(\infty) = \frac{a}{c}$.[1]

[1] Tomamos $\beta^{-1}(\infty) = \infty$ cuando $c = 0$.

Definición 5.2.4. Definimos como *cúspides* a las clases de equivalencias de $\mathbb{Q}\cup\{\infty\} = \mathbb{P}^1(\mathbb{Q})$ bajo la acción de $\Gamma_0(N)$.

Como $\beta^{-1}(\infty) = \frac{a}{c}$, podemos pensar a las cúspides como elementos de la forma $\beta^{-1}(\infty)$ con $\beta \in \mathrm{SL}_2(\mathbb{Z})$. Luego dos elementos $\alpha, \beta \in \mathrm{SL}_2(\mathbb{Z})$ representan la misma cúspide si existe algún $\gamma \in \Gamma_0(N)$ tal que $\alpha^{-1}(\infty) = \gamma\beta^{-1}(\infty)$.

Sea f una forma modular no restrictiva de peso k y nivel N. Luego se puede probar, realizando su desarrollo de Fourier, que

$$f|_k[\beta^{-1}](\tau) = \sum_{n=-\infty}^{\infty} c_n^{(\beta)} q_N^n \quad \text{con} \quad q_N = e^{\frac{2\pi i\tau}{N}}. \tag{5.3}$$

Decimos que f es *holomorfa en la cúspides* $\beta^{-1}(\infty)$ si $c_n^{(\beta)} = 0$ para todo $n < 0$ y decimos que se *anula en la cúspide* $\beta^{-1}(\infty)$ si es holomorfa en dicha cúspide y $c_0^{(\beta)} = 0$.

Definición 5.2.5. Sea f una forma modular no restrictiva de peso k y nivel N. Decimos que f es una *forma modular* si es holomorfa en las cúspides (de $\Gamma_0(N)$) y se dice *forma cuspidal* si se anula en las cúspides (de $\Gamma_0(N)$).

Para ver la buena definición tenemos que probar que si $\beta_1^{-1}(\infty)$ y $\beta_2^{-1}(\infty)$ representan la misma cúspide entonces, si f es holomorfa (se anula) en una, lo es en la otra. Como $\beta_1^{-1}(\infty)$ y $\beta_2^{-1}(\infty)$ representan la misma cúspide existe $\gamma \in \Gamma_0(N)$ tal que $\beta_i\gamma\beta_j^{-1} = \pm\begin{pmatrix}1 & l\\ 0 & 1\end{pmatrix}$, para algún $l \in \mathbb{Z}$. Luego haciendo cuentas se ve que $f|_k[\beta_i^{-1}]\left(\begin{pmatrix}1 & l\\ 0 & 1\end{pmatrix}\tau\right) = f|_k[\beta_j^{-1}](\tau)$ lo cual prueba lo que queríamos ver.

Como $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] < \infty$,podemos escribir $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{j\in I} \beta_j\Gamma_0(N)$, con $|I| < \infty$. De la definición de cúspide se desprende que las cúspides pueden ser representadas por $\beta_j^{-1}(\infty)$ con los β_j dados arriba. Luego para ver si una función f es modular o cuspidal basta analizarla en dichas cúspides.

Observación 5.2.6. Si f es una forma modular de peso k y nivel N entonces podemos escribir a f en su desarrollo en expansión de $q = e^{2\pi i\tau}$ como $f(\tau) = \sum_{n=0}^{\infty} a_n(f)q^n$. En efecto, como $\beta = \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix} \in \Gamma_0(N)$, entonces $f = f|_k[\beta]$. Luego $f(\tau) = f|_k[\beta](\tau) = \delta(\beta,\tau)^{-k}f(\beta\tau) = f(\tau+1)$.

Notación 5.2.7. A los espacios de las formulas modulares y las formas cuspidales de peso k y nivel N se los denotará por $M_k(\Gamma_0(N))$ y $S_k(\Gamma_0(N))$ respectivamente.

5.3. L-serie de una forma cuspidal

Definición 5.3.1. Sea $f \in S_k(\Gamma_0(N))$ una forma cuspidal, y sea $f(\tau) = \sum_{n=1}^{\infty} a_n(f)q^n$ su expansión en $q = e^{2\pi i\tau}$ mencionada en la Observación 5.2.6. Definimos la *L-serie* de f a la serie de Dirichlet

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

La L serie de f puede ser obtenida a partir de f mediante una transformación de Mellin.

Definición 5.3.2. Si $F : (0, \infty) \to \mathbb{C}$ es una función dada, la transformación de Mellin de F es la función $g(s)$ definida por

$$g(s) = \int_0^\infty F(t) t^s \frac{dt}{t}.$$

Apliquemos la transformación de Mellin a $F(t) = f(it)$, con f forma cuspidal. Obtenemos:

$$\begin{aligned}
\int_0^\infty f(i\sigma)\sigma^s \frac{d\sigma}{\sigma} &= \int_0^\infty \sum_{n=1}^\infty a_n(f) e^{-2\pi n\sigma} \sigma^s \frac{d\sigma}{\sigma} \\
&= \sum_{n=1}^\infty a_n(f) \int_0^\infty e^{-t} (2\pi n)^{-s} t^s \frac{dt}{t} \\
&= (2\pi)^{-s} \left(\sum_{n=1}^\infty \frac{a_n(f)}{n^s} \right) \int_0^\infty e^{-t} t^{s-1} dt \\
&= (2\pi)^{-s} L(s, f)\Gamma(s) \qquad (5.4)
\end{aligned}$$

para todo s tal que dicha integral converja y donde $\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$ es la función Gamma.

Enunciemos el siguiente lema que nos va a hacer falta para probar el resultado que nos interesa acerca de la L serie de una forma cuspidal.

Lema 5.3.3. Sea $\tau \in \mathcal{H}$ y $f \in S_k(\Gamma_0(N))$ con expansión en $q = e^{2\pi i\tau}$ dada por $f(\tau) = \sum_{n=1}^\infty a_n(f) q^n$. Entonces $|f(\tau)|y^{k/2}$ es acotada en $\mathcal{H}$ e invariante por $\Gamma_0(N)$. Además de esto último sigue que $|a_n(f)| \leq Cn^{k/2}$.

Demostración. Ver [Kna92, Lema 9.6]. □

Definición 5.3.4. Sea $\alpha_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ y $f \in M_k(\Gamma_0(N))$. Definamos el operador w_N definido en las formas modulares como $w_N f = f|_k[\alpha_N]$.

Observación 5.3.5. Si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ entonces $\alpha_N \gamma \alpha_N^{-1} = \begin{pmatrix} d & -c/N \\ -Nb & a \end{pmatrix}$. Por lo que $\alpha_N \Gamma_0(N) \alpha_N^{-1} \subseteq \Gamma_0(N)$.

Nos gustaría poder descomponer a $S_k(\Gamma_0(N))$ como suma de autoespacios de w_N, por lo cual enunciemos primero el siguiente resultado.

Proposición 5.3.6. La función w_N manda a $M_k(\Gamma_0(N))$ y a $S_k(\Gamma_0(N))$ en si mismos.

Demostración. Sea $f \in M_k(\Gamma_0(N))$, observemos que $w_N f$ es una forma modular no restrictiva de peso k y nivel N. En efecto, si $\gamma \in \Gamma_0(N)$ tenemos que

$$\begin{aligned}
(w_N f)|_k[\gamma] &= (f|_k[\alpha_N])|_k[\gamma] \\
&= (f|_k[\alpha_N \gamma \alpha_N^{-1}])|_k[\alpha_N] \\
&= f|_k[\alpha_N] \\
&= w_N f.
\end{aligned}$$

En la tercera igualdad usamos que f es modular y la Observación 5.3.5 Por el Lema 5.1.2 existe $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ y $\widetilde{\alpha} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ en $M(N)$ tal que $\alpha_N \beta^{-1} = \gamma^{-1}\widetilde{\alpha}$. Luego, usando además que podemos escribir $f|_k[\gamma^{-1}](\tau) = \sum_{n=0}^{\infty} a_n(f) e^{2\pi i n\tau/N}$ al ser f una forma modular de peso k y nivel N, tenemos que

$$\begin{aligned}
(w_N f)|_k[\beta^{-1}](\tau) &= (f|_k[\alpha_N])|_k[\beta^{-1}](\tau) \\
&= (f|_k[\gamma^{-1}])|_k[\widetilde{\alpha}](\tau) \\
&= (N^{-1/2}d)^{-k} f|_k[\gamma^{-1}]\left(\frac{a\tau + b}{d}\right) \\
&= (N^{-1/2}d)^{-k} \sum_{n=0}^{\infty} a_n(f) e^{2\pi i n b/(Nd)} e^{2\pi i n a^2 \tau/N^2} \\
&= \sum_{n=0}^{\infty} a_n(f)' e^{2\pi i n\tau/N^2}. \qquad (5.5)
\end{aligned}$$

Pero por otro lado, sabemos que $w_n f$ es una forma modular no restrictiva para $\Gamma_0(N)$, por lo que $(w_N f)|_k[\beta^{-1}](\tau)$ tiene período N. Por lo tanto los coeficientes de (5.5) van a ser 0 salvo que $N|n$. Luego $(w_N f)|_k[\beta^{-1}](\tau) = \sum\limits_{n=0}^{\infty} a_n(f)' e^{2\pi i n\tau/N}$ y entonces $w_N f$ es holomorfa en las cúpsides β^{-1} de $\Gamma_0(N)$. Por lo que $w_N f \in M_k(\Gamma_0(N))$. De forma similar se ve que si f está en $S_k(\Gamma_0(N))$ entonces $w_N f$ está en $S_k(\Gamma_0(N))$. □

Notemos ahora que $(\alpha_N^{\#})^2 = -\mathrm{Id}$. Luego

$$w_N^2 f(\tau) = ((f|_k[\alpha_N])|_k[\alpha_N])(\tau) = (f|_k[(\alpha_N^{\#})^2])(\tau) = (-1)^{-k} f(\tau) = f(\tau).$$

La segunda igualdad vale por la Observación 5.2.1 y la última igualdad del hecho de que el peso de nuestra forma modular siempre va a ser par. Luego viendo a $M_k(\Gamma_0(N))$ y a $S_k(\Gamma_0(N))$ como $\mathbb{C}$-espacios vectoriales y a w_N como operador lineal tenemos que este último será una involución. Por lo tanto podemos escribir a dichos espacios como suma directa de los autoespacios correspondientes a los autovalores de w_N (1 y -1). Para el caso de $S_k(\Gamma_0(N))$ llamamos a estos autoespacios $S_k^{\pm}(\Gamma_0(N))$. Ahora enunciemos y probemos el Teorema de interés.

Teorema 5.3.7. (Hecke) Sea $f \in S_k(\Gamma_0(N))$ una forma cuspidal en alguno de los autoespacios $S_k^{\varepsilon}(\Gamma_0(N))$ de w_N, con $\varepsilon = \pm$. Luego $L(s, f)$ esta definida para $\mathrm{Re}\, s > \frac{k}{2} + 1$ y se extiende a todo $\mathbb{C}$ de forma analítica. Más aún, la función

$$\Lambda(s, f) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(s, f) \qquad (5.6)$$

satisface la ecuación funcional

$$\Lambda(s, f) = \varepsilon(-1)^{k/2}\Lambda(k - s, f). \qquad (5.7)$$

Demostración. Por los Lemas 5.3.3 y A.2.4 tenemos que la región inicial de convergencia de $L(s, f)$ es Re $s > \frac{k}{2} + 1$. Como $\varepsilon f(i\sigma) = w_N f(i\sigma) = \left(\frac{N}{\sqrt{N}}\sigma i\right)^{-k} f(\frac{i}{N\sigma})$ obtenemos que

$$f\left(\frac{i}{N\sigma}\right) = \varepsilon N^{k/2} i^k \sigma^k f(i\sigma). \qquad (5.8)$$

Por la Ecuación (5.4) tenemos que

$$\Lambda(s,f) = N^{s/2}\int_0^\infty f(i\sigma)\sigma^{s-1}d\sigma. \tag{5.9}$$

Usando que $|f(\tau)| \leq C_j e^{-2\pi(\operatorname{Im}\tau)/N}$ para todo τ con $\operatorname{Im}\tau \geq 2$, se prueba que

$$\int_{1/\sqrt{N}}^\infty f(i\sigma)\sigma^{s-1}d\sigma \tag{5.10}$$

converge para todo $s \in \mathbb{C}$ y luego define una función entera. Reescribimos la Ecuación (5.9) para $\operatorname{Re} s > \frac{k}{2}+1$ como

$$\Lambda(s,f) = N^{s/2}\int_0^{1/\sqrt{N}} f(i\sigma)\sigma^{s-1}d\sigma + N^{s/2}\int_{1/\sqrt{N}}^\infty f(i\sigma)\sigma^{s-1}d\sigma.$$

En el primer término, reemplazamos σ por $(N\sigma)^{-1}$ y luego usamos la Ecuación (5.8). Por lo tanto nos queda

$$\Lambda(s,f) = \varepsilon N^{\frac{1}{2}(k-s)}i^k\int_{1/\sqrt{N}}^\infty f(i\sigma)\sigma^{k-s-1}d\sigma + N^{s/2}\int_{1/\sqrt{N}}^\infty f(i\sigma)\sigma^{s-1}d\sigma. \tag{5.11}$$

Luego, de esta última expresión, y de la Ecuación (5.10), obtenemos que $\Lambda(s,f)$ se extiende de forma entera. Como $\Gamma(s) \neq 0$ para todo $s \in \mathbb{C}$ tenemos que entonces $L(s,f)$ se extiende de forma entera. Reemplazando s por $k-s$ en la Ecuación (5.11) y multiplicando por $\varepsilon i^k = \varepsilon(-1)^{k/2}$, obtenemos que

$$\varepsilon(-1)^{k/2}\Lambda(k-s,f) = N^{\frac{1}{2}s}\int_{1/\sqrt{N}}^\infty f(i\sigma)\sigma^{s-1}d\sigma + \varepsilon N^{\frac{1}{2}(k-s)}i^k\int_{1/\sqrt{N}}^\infty f(i\sigma)\sigma^{k-s-1}d\sigma.$$

Comparando con la Ecuación (5.11) obtenemos la Ecuación (5.7).

□

5.4. Operadores de Hecke

Definición 5.4.1. Sea $M(n)$ el conjunto de matrices enteras 2×2 con determinante n. Luego definimos

$$M(n,N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(n) |\ c \equiv 0 \pmod{\text{N}} \text{ y } \operatorname{mcd}(a,N) = 1 \right\}.$$

Notar que el grupo $\Gamma_0(N)$ actúa en $M(n,N)$. Además el conjunto de representantes de $\Gamma_0(N)\backslash M(n,N)$ es finito. En efecto, el conjunto

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = n, d > 0, \operatorname{mcd}(a,N) = 1, 0 \leq b < d \right\}$$

es un conjunto completo de representantes de las coclases a derecha de $\Gamma_0(N)$ en $M(n,N)$. Luego definimos los operadores de Hecke en $S_k(\Gamma_0(N))$ de la siguiente forma.

Definición 5.4.2. Sea $\{\alpha_i\}$ un conjunto completo de representantes de $\Gamma_0(N)\backslash M(n,N)$. Si $f \in M_k(\Gamma_0(N))$, entonces definimos al operador de Hecke $T_n : M_k(\Gamma_0(N)) \to M_k(\Gamma_0(N))$ como

$$T_n f = n^{\frac{k}{2}-1} \sum_i f|_k[\alpha_i]. \tag{5.12}$$

Proposición 5.4.3. Si $f \in M_k(\Gamma_0(N))$ entonces $T_n f$ es una forma modular no restrictiva de peso k y nivel N.

Demostración. Ver [Kna92, Proposición 8.14]. □

Corolario 5.4.4. El operador de Hecke T_n satisface que $T_n(M_k(\Gamma_0(N))) = M_k(\Gamma_0(N))$ y $T_n(S_k(\Gamma_0(N))) = S_k(\Gamma_0(N))$.

Proposición 5.4.5. Sea $f \in M_k(\Gamma_0(N))$ con expansión en q dada por $f(\tau) = \sum_{n=0}^{\infty} a_n(f) q^n$. Luego $T_m f$ tiene expansión en q $T_m f(\tau) = \sum_{n=0}^{\infty} b_n q^n$ con

$$b_n = \begin{cases} a_0(f) \displaystyle\sum_{\substack{a|m, a>0 \\ (a,N)=1}} a^{k-1} & \text{si } n = 0 \\ a_m(f) & \text{si } n = 1 \\ \displaystyle\sum_{\substack{a|(n,m) \\ (a,N)=1}} a^{k-1} a_{nm/a^2}(f) & \text{si } n > 1 \end{cases}$$

Demostración. Ver [Kna92, Proposición 9.15]. □

Teorema 5.4.6. (Hecke) En el espacio $M_k(\Gamma_0(N))$, los operadores de Hecke satisfacen

(a) Para cada potencia de un primo p^r con $r \geq 1$ tal que $p \nmid N$, $T_k(p^r)T_k(p) = T_k(p^{r+1}) + p^{k-1}T_k(p^{r-1})$. Por lo tanto $T_k(p^r)$ es un polinomio en $T_k(p)$ con coeficientes enteros.

(b) Para una potencia de un primo p^r con $r \geq 1$ tal que $p|N$, $T_k(p^r) = T_k(p)^r$.

(c) $T_m T_n = T_{mn}$ si m y n son coprimos.

(d) El álgebra generada por T_n con $n \in \mathbb{N}$ es generada por los T_p con p primo y es conmutativa.

Demostración. Ver [Kna92, Lema 9.16]. □

Como consecuencia del Lema 5.3.3 podemos definir el *producto interno de Petersson* en $S_k(\Gamma_0(N))$ dado por

$$\langle f, h \rangle = \int_{R_N} f(\tau)\overline{h(\tau)} y^k \frac{dxdy}{y^2}$$

donde R_N es el dominio fundamental de $\Gamma_0(N)$ y $\tau = x + iy$.

Luego se puede probar lo siguiente

Teorema 5.4.7. (Petersson) Sean $n, N \in \mathbb{N}$ tales que $(n, N) = 1$. Luego los operadores de Hecke T_n, en $S_k(\Gamma_0(N))$, son autoadjuntos respecto al producto interno de Petterson.

Como los operadores de Hecke T_n con $\text{mcd}(n, N) = 1$ conmutan por lo visto en el Teorema 5.4.6 y son autoadjuntos en $S_k(\Gamma_0(N))$ por el teorema recien mencionado, tenemos (por el teorema de diagonalización simultanea) que podemos descomponer a $S_k(\Gamma_0(N))$ como suma directa de autoespacios simultaneos para los operadores T_n con $\text{mcd}(n, N) = 1$. Es decir

$$S_k(\Gamma_0(N)) = \bigoplus V_i \tag{5.13}$$

donde V_i son espacios ortogonales y cada uno es es un autoespacio simultaneo para todo T_n con $\text{mcd}(n, N) = 1$. Un autovector en $S_k(\Gamma_0(N))$ simultaneo para los operadores de Hecke T_n con $\text{mcd}(n, N) = 1$ se llama una *autoforma*; dos autoformas en el mismo autoespacio se dicen que son *equivalentes*.

Proposición 5.4.8. La involución w_N de $S_k(\Gamma_0(N))$ definida en 5.3.4 es autoadjunta y conmuta con todo T_n tal que $\text{mcd}(n, N) = 1$.

Demostración. Ver [Kna92, Proposición 9.19]. □

De esta última proposición se desprende que la descomposición de $S_k(\Gamma_0(N))$ en espacios de autoformas equivalentes es compatible con la descomposición de $S_k(\Gamma_0(N))$ en los autoespacios $S_k^{\pm}(\Gamma_0(N))$ descriptos anteriormente.

Los operadoes de Hecke T_n con $\text{mcd}(n, N) \neq 1$ conmutan con los demás T_n y luego envían los espacios de autoformas equivalentes en ellos mismos. Además en cada espacio de autoformas equivalentes va a haber al menos un autovector para todo T_n.

Proposición 5.4.9. Supongamos que $f \in S_k(\Gamma_0(N))$ es una autoforma que es un autovector para todo T_n, digamos $T_n f = \lambda(n) f$. Si la expansión de f en el ∞ es $f(\tau) = \sum_{n=1}^{\infty} a_n(f) q^n$, entonces

$$a_n(f) = \lambda(n) a_1(f). \tag{5.14}$$

Por lo que $f \not\equiv 0$ implica que $a_1(f) \neq 0$ y el sistema de autovalores $\{\lambda(n)\}$ determina a f salvo un escalar.

Observación 5.4.10. Bajo la suposición de la proposición anterior podemos normalizar a la expansión en q de f de forma tal que $a_1(f) = 1$. Luego la Ecuación (5.14) nos dice que $a_n(f)$ es él autovalor para T_n. Por lo tanto por el Teorema 5.4.6 vemos que que se cumple la siguiente relación entre los autovalores $a_n(f)$.

$$\begin{aligned} a_{p^r}(f) a_p(f) &= a_{p^{r+1}}(f) + p^{k-1} a_{p^{r-1}}(f) && \text{si } p \text{ es primo, } p \nmid N, \\ a_{p^r}(f) &= a_p^r(f) && \text{si } p \text{ es primo, } p | N, \\ a_m(f) a_n(f) &= a_{mn}(f) && \text{si } \text{mcd}(m, n) = 1. \end{aligned}$$

Luego dicha observación nos permite afirmar que la L-serie de f la puedo escribir como un producto de Euler.

Teorema 5.4.11. (Hecke-Petersson). El espacio $S_k(\Gamma_0(N))$ de formas cuspidales es la suma ortogonal de espacios de autoformas equivalentes. Cada espacio de autoformas equivalentes tiene un miembro que es autovector para todo los T_n. Toda autoforma f en $S_k(\Gamma_0(N))$ que es un autovector para todos los T_n puede ser normalizado de forma tal que su expansión en $q = e^{2\pi i/N}$ $f(\tau) = \sum_{n=1}^{\infty} a_n(f) q^n$ tiene $a_1(f) = 1$. Con tal normalización los coeficientes

satisfacen las igualdades mencionadas en la Observación 5.4.10. Más aún, la L serie de f tiene una expansión en producto de Euler de la siguiente forma

$$L(s,f) = \prod_{\substack{\text{p primo} \\ p|N}} \left[\frac{1}{1-a_p(f)p^{-s}}\right] \prod_{\substack{\text{p primo} \\ p\nmid N}} \left[\frac{1}{1-a_p(f)p^{-s}+p^{k-1-2s}}\right]$$

convergente para $\operatorname{Re} s > \frac{k}{2}+1$.

Nos gustaría ahora extender la descomposición en (5.13) para los operadores de Hecke T_p con $p|N$, pero dicha descomposición solo va a ser válida para ciertos subespacios de $S_k(\Gamma_0(N))$. En efecto, observar que si $M|N$, entonces $\Gamma_0(M) \supset \Gamma_0(N)$, y luego $S_k(\Gamma_0(M)) \subset S_k(\Gamma_0(N))$.

Definición 5.4.12. Sean N, M, d naturales tal que, $M|N$, $M < N$ y $d|N/M$. Decimos que una autoforma $f(\tau)$ es *vieja de nivel* N si $f \in S_k(\Gamma_0(N/dM))$, lo cual implica a su vez que $f(d\tau) \in \Gamma_0(N)$ (ver [Kna92] §IX.7). Las formas viejas forman un subespacio $S_k^{\text{old}}(\Gamma_0(N))$ de $S_k(\Gamma_0(N))$, y su complemento ortogonal, denotado por $S_k^{\text{new}}(\Gamma_0(N))$, es llamado el espacio de las formas *nuevas*. Las autoformas en $S_k^{\text{new}}(\Gamma_0(N))$ se llaman formas *nuevas* para $\Gamma_0(N)$.

Como T_n es autoadjunto cuando $\operatorname{mcd}(n,N) = 1$ y conmutan, podemos descomponer a $S_k^{\text{new}}(\Gamma_0(N))$ como suma directa de autoespacios generados por formas nuevas. Más aún, cada subespacio va a ser de dimensión 1 por el siguiente Teorema.

Teorema 5.4.13. (Atkin-Lehner) Si $f \in S_k(\Gamma_0(N))$ es una forma nueva, entonces su espacio de formas nuevas equivalentes tiene dimensión 1, es decir que consiste de múltiplos de f.

Luego podemos descomponer a $S_k^{\text{new}}(\Gamma_0(N))$ como

$$S_k^{\text{new}}(\Gamma_0(N)) = \bigoplus W_i$$

donde cada W_i tiene dimensión 1, y es un autoespacio simultaneo para los T_n con $\operatorname{mcd}(n,N) = 1$. Como los operadores T_p con $p|N$ conmutan con todos los operadores de Hecke T_n, tenemos que T_p deja estable a los autoespacios W_i. Además, como cada W_i tiene dimensión 1, también tendrán que ser autoespacios para los operadores de Hecke T_p, con $p|N$. Por lo tanto las formas nuevas terminan siendo autovectores para todos los operadores de Hecke T_n.

Capítulo 6

Eichler-Shimura

El objetivo de este capítulo es mostrar los resultados probados por Eichler y Shimura, que involucra cómo construir curvas elípticas a partir de formas modulares de peso 2. Comenzaremos mencionando propiedades acerca de la superficie de Riemann $X_0(N)$, seguiremos probando propiedades acerca de la variedad de Jacobi, para finalizar enunciando el Teorema de Eichler Shimura. Las referencias utilizadas en este Capítulo son las siguientes: [Shu05], [Shi71], [Kna92] y [Ste11].

6.1. Superficies de Riemann y el mapa de Jacobi

Definición 6.1.1. Una superficie de Riemann es una variedad compleja, conexa y de dimensión 1.

Topológicamente, toda superficie de Riemann compacta es homeomorfa a un g-toro, con g entero no negativo. Llamaremos a dicho g el *género* de la superficie de Riemann.

Definamos ahora a la superficie de Riemann que vamos a estudiar.

Definición 6.1.2. Sea $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Definimos a $X_0(N)$ como el espacio cociente $\Gamma_0(N)\backslash\mathcal{H}^*$, con la acción descripta en el capítulo anterior.

Observación 6.1.3. El espacio $X_0(N)$ es el dominio fundamental dado por la acción de $\Gamma_0(N)$ en $\mathcal{H}$, sumandole las cúspides descriptas por dicha acción.

Proposición 6.1.4. $X_0(N)$ es conexo, Hausdorff y compacto.

Demostración. Ver [Shu05, Proposición 2.4.2]. □

Más aún, podemos asociarle a $X_0(N)$ una estructura de variedad compleja de dimensión 1. Por lo que $X_0(N)$ termina siendo una superficie de Riemann compacta.

El siguiente resultado, desarrollado en [Shu05, §III.1], nos dice el género de $X_0(N)$, resultado que será de vital importancia para probar el Último Teorema de Fermat.

Teorema 6.1.5. Sea p primo, luego el género g de $X_0(p)$ viene dado por:

$$g = \begin{cases} \lfloor \frac{p+1}{12} \rfloor - 1 & \text{si } p \equiv 1 \pmod{12} \\ \lfloor \frac{p+1}{12} \rfloor & \text{caso contrario} \end{cases}$$

Corolario 6.1.6. El género de $X_0(2)$ es 0.

Si X es una superficie de Riemann compacta entonces el espacio de funciones meromorfas de X forman un cuerpo, que lo denotaremos por $K(X)$. Definamos ahora el conjunto de diferenciales holomorfos de una superifice de Riemann.

En una superficie de Riemann, toda 1-forma diferenciable compleja, se puede escribir localmente como $\omega = f(z,\bar{z})dz + g(z,\bar{z})d\bar{z}$, con f y g funciones diferenciables y z un entorno coordenado. Denotamos por $\Omega^{1,0}$ al subespacio de 1-formas diferenciables complejas que, localmente, solo sean de la forma $f(z,\bar{z})dz$ y $\Omega^{0,1}$ al subespacio que, localmente, solo sean de la forma $g(z,\bar{z})d\bar{z}$. Por las ecuaciones de Cauchy Riemann se ve que los espacios $\Omega^{1,0}$ y $\Omega^{0,1}$ son estables mediante un cambio de coordenadas holomorfo. Luego, denotando a $E^1(X)$ al espacio de 1-formas diferenciables complejas de X tendremos que $E^1(X) = \Omega^{1,0} \oplus \Omega^{0,1}$.

Definición 6.1.7. Sea X una superficie de Riemann, una 1-forma diferenciable compleja $\omega = f(z,\bar{z})dz$ en X, con z entorno coordenado, se dice *holomorfa* si $\bar{\partial}\omega = 0$, donde $\bar{\partial}\omega = \frac{\partial f}{\partial \bar{z}} d\bar{z} \wedge dz$.

En otras palabras, ω es un diferencial holomorfo si $\partial f/\partial \bar{z} = 0$. Escribimos $f(z,\bar{z}) = f(z)$ cuando $\partial f/\partial \bar{z} = 0$. Por lo tanto, un diferencial holomorfo ω, está localemente representado por $f(z)dz$, con $f(z)$ función holomorfa. Denotaremos a dicho espacio como $H^0(X, \omega_X)$.

Teorema 6.1.8. Sea X superficie de Riemann compacta de género g, entonces tenemos que $\dim_{\mathbb{C}} H^0(X, \omega_X) = g$.

En $X_0(N)$, podemos dar explícitamente el espacio de diferenciales holomorfos. Sea $\pi : \mathcal{H}^* \to X_0(N)$ la proyección al cociente. Luego para cada diferencial holomorfo w de $X_0(N)$ tenemos que $\pi^* w = f_w dz$, donde π^* es el pull-back de 1-formas diferenciales complejas en $X_0(N)$ a 1-formas diferenciales complejas en $\mathcal{H}^*$. Se puede ver que f_w es una forma modular de peso 2 y nivel N. Luego tenemos una asociación $w \mapsto f_w$ entre $H^0(X_0(N), \omega_{X_0(N)})$ y $S_2(\Gamma_0(N))$. Más aún, dicha asociación es un isomorfismo.

Proposición 6.1.9. $H^0(X_0(N), \omega_{X_0(N)}) \cong S_2(\Gamma_0(N))$.

Demostración. Ver [Kna92, Proposición 11.6]. □

De esta Proposición se desprende el siguiente Corolario, que será importante para probar el Último Teorema de Fermat.

Corolario 6.1.10. $S_2(\Gamma_0(2)) = \{0\}$.

Demostración. Por el Teorema 6.1.9 tenemos que $S_2(\Gamma_0(2)) \cong H^0(X_0(2), \omega_{X_0(2)})$, y por el Teorema 6.1.8, $\dim_{\mathbb{C}} H^0(X_0(2), \omega_{X_0(2)}) = g$, donde g es el género de $X_0(2)$. Luego, como $g = 0$ por el Corolario 6.1.6, tenemos que $S_2(\Gamma_0(2)) = \{0\}$. □

Definamos ahora la integral de una forma holomorfa sobre un 1-simplex. Sea $\gamma : [0,1] \to X$ un 1-simplex tal que $\gamma([0,1]) \subset U$ donde (ϕ, U) es un entorno coordenado de X, con $\phi : U \to V \subseteq \mathbb{C}$ y con $\omega|_V = f(q)dq$. En tal caso definimos la integral de un diferencial holomorfo ω sobre γ como

$$\int_\gamma \omega = \int_{\phi\circ\gamma} \omega|_V = \int_{\phi\circ\gamma} f(q)dq.$$

Veamos que esta definición no es ambigua. Supongamos que $\gamma([0,1]) \subset U_1 \cap U_2$ con (U_1, ϕ_1) y (U_2, ϕ_2) entornos coordenados. Denotemos $V_{1,2} = \phi_1(U_1 \cap U_2)$ y $V_{2,1} = \phi_2(U_1 \cap U_2)$, y $\phi_{2,1} : V_{1,2} \to V_{2,1}$ la función de transición entre los dos entornos coordenados. Por definición de la función de transición, y por la fórmula de cambio de variable, y por la condición de compatibilidad $\phi_{2,1}^*(\omega|_{V_2}) = \omega|_{V_1}$,

$$\int_{\phi_2 \circ \gamma} \omega|_{V_2} = \int_{\phi_{2,1} \circ \phi_1 \circ \gamma} \omega|_{V_2} = \int_{\phi_1 \circ \gamma} \phi_{2,1}^*(\omega|_{V_2}) = \int_{\phi_1 \circ \gamma} \omega|_{V_1}.$$

En general, el dominio $[0,1]$ de γ se particiona en una cantidad finita de intervalos, los cuales tienen imagen en uno de los entornos coordenados de X. La integral sobre γ es definida como la correspondiente suma de las integrales locales, y es facil ver que el resultado está bien definido.

Esta definición se puede extender al grupo de homología $H_1(X;\mathbb{Z})$. Enunciemos el siguiente teorema que nos dará la buena definición

Teorema 6.1.11. (Stokes para cadenas) Si c es una p-cadena en una variedad diferenciable M, y una w es una $(p-1)$-forma diferenciable en M, entonces

$$\int_{\partial c} \omega = \int_c d\omega.$$

Supongamos ahora que $[\gamma] \in H_1(X;\mathbb{Z})$, definimos

$$\int_{[\gamma]} \omega = \int_\gamma \omega.$$

Veamos que está bien definido. Supongamos ahora que, $[\sigma_1] = [\sigma_2]$, entonces $\sigma_1 - \sigma_2 = \partial S$, con S un 2-simplex. Luego por 6.1.11

$$\int_{\sigma_1 - \sigma_2} \omega = \int_{\partial S} \omega = \int_S d\omega = 0 \Longrightarrow \int_{\sigma_1} \omega = \int_{\sigma_2} \omega_2.$$

Definamos ahora el siguiente mapa

$$\begin{aligned} H_1(X;\mathbb{Z}) &\to H^0(X, \omega_X)^\wedge \\ [\gamma] &\mapsto \left(\omega \mapsto \int_\gamma \omega\right). \end{aligned} \tag{6.1}$$

Dicho mapa está bien definido por lo que mencionamos antes. Además, usando algunos resultados de cohomologías y dualidad (como el Teorema del coeficiente universal), se puede probar la siguiente afirmación:

Afirmación 6.1.12. El mapa definido en (6.1) es inyectivo.

Demostración. Ver [Bir13, Lema 11.1.1]. □

Ahora, al ser $H_1(X,\mathbb{Z})$ grupo abeliano libre en $2g$ generadores sobre $\mathbb{Z}$ (pues X es homeomorfo a un g-toro), y al ser $H^0(X,\omega_X)^\wedge$ de dimensión g como $\mathbb{C}$-espacio vectorial, tenemos, mediante la inyección probada, que $H_1(X,\mathbb{Z})$ es un retículo en $H^0(X,\omega_X)^\wedge$. Definimos entonces la variedad de Jacobi de X de la siguiente forma.

Definición 6.1.13. Sea X superficie de Riemann de género g, definimos su variedad de Jacobi $\mathrm{Jac}(X)$ como el toro complejo g-dimensional

$$\mathrm{Jac}(X) = H^0(X,\omega_X)^\wedge / H_1(X,\mathbb{Z}) \cong \mathbb{C}^g/\Lambda.$$

donde Λ es el retículo formado por los $2g$ vectores $v_k = \begin{pmatrix} \int_{c_k}\omega_1 \\ \vdots \\ \int_{c_k}\omega_g \end{pmatrix}$ donde $c_1,\dots,c_{2g}$ es una base de $H_1(X,\mathbb{Z})$ y $\omega_1,\dots,\omega_g$ es una base de $H^0(X,\omega_X)$.

Los vectores v_k van a formar en efecto un retículo ya que por la Proposición 6.1.12 tenemos que

$$\begin{aligned} H_1(X;\mathbb{Z}) \times H^0(X,\omega_X) &\to \mathbb{C} \\ ([\gamma],\omega) &\mapsto \int_\gamma w \end{aligned}$$

será no degenerada. Lo cual implicará que los vectores v_k dados en la definición sean LI sobre $\mathbb{R}$.

Sea ahora $C(X)$ el cuerpo de funciones de X. El grupo de divisores de grado 0 de X se define como

$$\mathrm{Div}^0(X) = \left\{ \sum_{x\in X} n_x x : n_x \in \mathbb{Z}, n_x = 0 \text{ para casi todo } x, \sum_x n_x = 0 \right\}.$$

Si $f \in C(X)^\times$ y $x \in X$, elegimos un entorno coordenado (U_i,φ_i) y definimos

$$\mathrm{ord}_x(f) = \mathrm{ord}_{\varphi_i(x)}(f\circ\varphi_i^{-1}).$$

El lado de la derecha es 0 si $\varphi_i(x)$ no es raíz ni polo de $f\circ\varphi_i^{-1}$. Si $\varphi_i(x)$ es polo de orden n de $f\circ\varphi_i^{-1}$ entonces el lado derecho será igual a $-n$ y si es raíz de orden n el lado derecho será igual a n. Esta definición no depende de φ_i debido a la compatibilidad de los entornos coordenados. Definimos el *divisor de* f como

$$\mathrm{div}(f) = \sum_{x\in X} \mathrm{ord}_x(f)x.$$

Definimos entonces el subgrupo de divisores principales como

$$\mathrm{Div}^\ell(X) = \left\{ \delta \in \mathrm{Div}^0(X) : \delta = \mathrm{div}(f) \text{ para alguna función } f \in C(X) \right\}.$$

Definimos el *grupo de Picard* (de grado 0) como el cociente de dichos grupos

$$\mathrm{Pic}^0(X) = \mathrm{Div}^0(X)/\mathrm{Div}^\ell(X).$$

Sea $x_0 \in X$ fijo. Luego X se inyecta en el grupo de picard mediante el mapa

$$X \to \mathrm{Pic}^0(X), \quad x \mapsto [x - x_0],$$

donde $[x - x_0]$ denota la clase de equivalencia de $x - x_0$ en $\mathrm{Pic}^0(X)$. Asumiendo que el género de X es mayor a 0 dicho mapa será inyectivo (ver [Bir13, página 320]). Definimos el *mapa de Jacobi* de $\mathrm{Div}^0(X)$ a $\mathrm{Jac}(X)$ como

$$\mathrm{Div}^0(X) \to \mathrm{Jac}(X), \quad \sum_x n_x x \mapsto \left(\omega \mapsto \sum_x n_x \int_{x_0}^{x} \omega \right).$$

Se prueba que dicho mapa está bien definido, es decir, no depende del punto x_0 ni del camino de x_0 a x que se tome para integrar. Dicho mapa desciende al grupo de Picard. Más aún

Teorema 6.1.14. El mapa de Jacobi desciende al grupo de Picard, e induce un isomorfismo

$$\mathrm{Pic}^0(X) \xrightarrow{\sim} \mathrm{Jac}(X), \quad \left[\sum_x n_x x \right] \mapsto \left(\omega \mapsto \sum_x n_x \int_{x_0}^{x} \omega \right).$$

6.2. Teorema de Eichler-Shimura

Antes de enunciar el Teorema de Eichler-Shimura, veamos ahora como actúa el álgebra de Hecke en los Jacobianos definidos previamente, y como influye esto en la demostración del resultado probado por Eichler Shimura.

Definición 6.2.1. Definimos el *álgebra de Hecke* $\mathbb{T}_{\mathbb{Z}}$, como la $\mathbb{Z}$-subálgebra de endomorfismos de $S_2(\Gamma_0(N))$ generada por los operadores de Hecke T_n. Es decir

$$\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}[\{T_n : n \in \mathbb{N}\}].$$

Observación 6.2.2. Por el Teorema 5.4.6 tenemos que dicha álgebra será conmutativa y generada por los operadores de Hecke T_p con p primo.

Definición 6.2.3. Definimos la subálgebra de Hecke $\mathbb{T}_0$ como la subálgebra de $\mathbb{T}_{\mathbb{Z}}$ generada por los operadores T_n con $(n, N) = 1$.

Observar que como $H^0(X_0(N), \omega_{X_0(N)}) \cong S_2(\Gamma_0(N))$, tenemos que

$$\mathrm{Jac}(X_0(N)) \cong S_2(\Gamma_0(N))^\wedge / H_1(X_0(N), \mathbb{Z}).$$

Al expresar el jacobiano de $X_0(N)$ de esta forma vamos a poder definir, de forma natural, una acción del álgebra de Hecke en el mismo. En efecto, tenemos la acción transitiva del álgebra de Hecke $\mathbb{T}_{\mathbb{Z}}$ en $S_2(\Gamma_0(N))^\wedge$ dada por

$$\begin{aligned} T : S_2(\Gamma_0(N))^\wedge &\to S_2(\Gamma_0(N))^\wedge, \quad T \in \mathbb{T}_{\mathbb{Z}} \\ f &\mapsto f \circ T. \end{aligned}$$

Esta acción desciende bien al cociente por $H_1(X_0(N),\mathbb{Z})$, es decir al Jacobiano de $X_0(N)$ (ver [Shu05, Proposición 6.3.2]).

$$\begin{aligned} T : \mathrm{Jac}(X_0(N)) &\to \mathrm{Jac}(X_0(N)) \\ [\psi] &\mapsto [\psi \circ T]. \end{aligned}$$

En el caso particular de los operadores de Hecke T_n actuando en $\mathrm{Jac}(X_0(N))$, los denotaremos por t_n.

Veamos ahora dos resultados que me garantizarán que tanto $X_0(N)$, como $\mathrm{Jac}(X_0(N))$ adquieren una estructura de variedad abeliana sobre $\mathbb{Q}$.

Teorema 6.2.4. Existe una curva proyectiva $C/\mathbb{Q}$ suave y una funcion biholomorfa $\phi : X_0(N) \to C(\mathbb{Q})$. Dicha curva es única salvo isomorfismo sobre $\mathbb{Q}$.

Por lo tanto podemos pensar a la curva modular $X_0(N)$ como una curva proyectiva sobre $\mathbb{Q}$. En ese caso la denotaremos por $X_0(N)_{\mathbb{Q}}$.

Enunciemos ahora un Teorema que nos garantizará poder ver a $\mathrm{Jac}(X_0(N))$ como variedad abeliana sobre $\mathbb{Q}$. Antes de enunciar el Teorema haremos una observación.

Observación 6.2.5. Si C es una curva proyectiva suave sobre $\mathbb{C}$, entonces, usando el teorema de la función implícita, $C(\mathbb{C})$ tiene una estrucutra de superficie de Riemann subyacente (ver [Mir95, §II.2]).

Teorema 6.2.6. (Lefschetz, Weil, Chow) Sea C una curva proyectiva suave sobre $\mathbb{C}$ y sea $\mathrm{Jac}(C)$ la variedad Jacobiana de la estructura de superficie de Riemann subyacente de C, y $\phi : C \to \mathrm{Jac}(C)$ el mapa de Jacobi con punto fijo x_0. Luego $\mathrm{Jac}(C)$ admite una estructura de variedad proyectiva suave de forma tal que

(a) Su estructura de grupo lo vuelve una variedad abeliana.
(b) ϕ es un morfismo.

Más aún, si C está definida sobre $\mathbb{Q}$, entonces $\mathrm{Jac}(C)$ puede ser definida sobre $\mathbb{Q}$ de forma tal que (a) y (b) son validas con estructuras definidas sobre $\mathbb{Q}$.

Luego de este último Teorema y de 6.2.4, tenemos que $\mathrm{Jac}(X_0(N))$ admite una estructura de variedad abeliana sobre $\mathbb{Q}$. En ese caso la denotaremos por $\mathrm{Jac}(X_0(N))_{\mathbb{Q}}$. Una observación importante es la siguiente.

Proposición 6.2.7. Para cada $T \in \mathbb{T}_{\mathbb{Z}}$, el morfismo $T : \mathrm{Jac}(X_0(N)) \to \mathrm{Jac}(X_0(N))$ se restringe a un morfismo $T : \mathrm{Jac}(X_0(N))_{\mathbb{Q}} \to \mathrm{Jac}(X_0(N))_{\mathbb{Q}}$.

Enunciemos ahora el Teorema de Eichler-Shimura.

Teorema 6.2.8. (Eichler-Shimura) Sea $f = \sum_{n=0}^{\infty} a_n(f) q^n \in S_2^{\mathrm{new}}(\Gamma_0(N))$ una forma nueva normalizada de nivel N. Sea K_f el cuerpo de números $K_f = \mathbb{Q}(\{a_n(f) : n \geq 0\})$. Luego existe un par (A_f, ν) tal que

(a) A_f es una variedad abeliana definida sobre $\mathbb{Q}$ de dimensión $[K_f : \mathbb{Q}]$ y tal que existe un morfismo sobreyectivo

$$\mathrm{Jac}(X_0(N)) \twoheadrightarrow A_f$$

definido sobre $\mathbb{Q}$;

(b) ν es un isomorfismo de K_f en $\mathrm{End}(A_f)\otimes\mathbb{Q}$. Los operadores de Hecke t_n en $\mathrm{End}(\mathrm{Jac}(X_0(N)))$ actúan en A_f por multiplicación por a_n, es decir, $\nu(a_n)$ es la restricción a A_f del operador de Hecke t_n actuando en $\mathrm{Jac}(X_0(N))$;
(c) Las dos propiedades previamente mencionadas caracterizan a (A,ν) salvo isomorfismos sobre $\mathbb{Q}$;
(d) $L(s,A_f/\mathbb{Q}) = L(s,f)$ como productos de Euler salvo por un número finito de factores de Euler,

donde la L-serie de la variedad abeliana A_f, $L(s,A_f)$, se define de forma similar a la L-serie de una curva elíptica, es decir como un producto de factores locales (ver [CA86], §II). Dicha definición extiende a la definición de L-series de curvas elípticas para variedades abelianas de dimensión mayor a 1. Sin embargo no entraremos en demasiados detalles ya que solo probaremos el apartado (a) del Teorema, es decir, construiremos dicha variedad abeliana. Para una demostración completa respecto a los demás apartados ver [Shi71] §VII.5.

Observación 6.2.9. La demostración del Teorema no usa que f sea una forma nueva. Basta con pedirle que f sea una autoforma de peso 2 para todos los operadores de Hecke T_n, condición que se cumple para las formas nuevas.

En el Teorema de Eichler Shimura se menciona que K_f es un cuerpo de números, por lo que deberemos probar que es, en efecto, una extensión finita de $\mathbb{Q}$. Para ello definamos el siguiente morfismo de $\mathbb{Z}$-álgebras, que servirá luego para definir la variedad abeliana A_f.

Definición 6.2.10. Sea $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ una forma nueva normalizada. Definimos el siguiente homomorfismo de álgebras

$$\begin{aligned}\lambda_f : \mathbb{T}_{\mathbb{Z}} &\to \mathbb{C}\\ T &\mapsto \text{autovalor de } T \text{ en } f.\end{aligned}$$

Dicho momorfismo está bien definido ya que toda forma nueva es autovector simultaneo de todos los operadores de Hecke. Observar además que al ser f normalizada, tenemos, debido a la Proposición 5.4.9, que $T_n(f) = a_n$ donde a_n es el n-ésimo coeficiente en la expansión en $q = e^{2\pi i\tau/N}$ de f. Luego $\mathrm{Im}\,\lambda_f = \mathbb{Z}[\{a_n : n \geq 0\}]$.

Proposición 6.2.11. Sea $f = \sum_{n=0}^{\infty} a_n q^n \in S_2^{\mathrm{new}}(\Gamma_0(N))$. Luego el anillo $\mathbb{Z}[\{a_n : n \geq 0\}]$ es finitamente generado y $K_f = \mathbb{Q}(\{a_n : n \geq 0\})$ es un cuerpo de números de grado igual al rango de $\mathbb{Z}[\{a_n : n \geq 0\}]$.

Demostración. El álgebra de Hecke actúa en $\mathrm{Jac}(X_0(N)) = S_2(\Gamma_0(N))^\wedge/H_1(X_0(N);\mathbb{Z})$. Por lo tanto podemos ver a $\mathbb{T}_{\mathbb{Z}}$ como un subanillo de endomorfismos de $\mathrm{End}(H_1(X_0(N);\mathbb{Z}))$. Como $H_1(X_0(N);\mathbb{Z})$ es un $\mathbb{Z}$-módulo finitamente generado, tendremos que el anillo de endomorfismos del mismo también lo será. Por lo tanto $\mathbb{T}_{\mathbb{Z}}$ es una $\mathbb{Z}$-álgebra finitamente generada, por lo que $\lambda(\mathbb{T}_{\mathbb{Z}})$ también lo será. Finalmente

$$\begin{aligned}\dim_{\mathbb{Q}}(K_f) &= \dim_{\mathbb{Q}}(\mathbb{Q}(\{a_n : n \geq 0\}))\\ &= \dim_{\mathbb{Q}}(\mathbb{Z}[\{a_n : n \geq 0\}] \otimes_{\mathbb{Z}} \mathbb{Q})\\ &= \mathrm{rank}\ \mathbb{Z}[\{a_n : n \geq 0\}]\\ &= \lambda(\mathbb{T}_{\mathbb{Z}}) < \infty.\end{aligned}$$

□

Por lo tanto, $K_f = \mathbb{Q}(\{a_n : n \geq 0\})$ es un cuerpo de números.

Como vimos que el álgebra de Hecke $\mathbb{T}$ actúa mediante morfismos en $\mathrm{Jac}(X_0(N))$, entonces $\ker(\lambda_f)(\mathrm{Jac}(X_0(N)))$ es una subvariedad abeliana de $\mathrm{Jac}(X_0(N))$. Denotando $I_f := \ker \lambda_f$ definimos la variedad abeliana que queríamos.

Definición 6.2.12. Definimos la *variedad abeliana A_f asociada a la forma nueva f* como

$$A_f = \frac{\mathrm{Jac}(X_0(N))}{I_f(\mathrm{Jac}(X_0(N)))}.$$

A priori, dicha variedad abeliana es compleja. Sin embargo podemos definirla sobre $\mathbb{Q}$. En efecto, mencionamos que $\mathrm{Jac}(X_0(N))$ podía definirse sobre $\mathbb{Q}$ y por 6.2.7 $I_f(\mathrm{Jac}(X_0(N)))$ también podrá definirse como una subvariedad abeliana de $\mathrm{Jac}(X_0(N))$ sobre $\mathbb{Q}$. Luego, como el cociente entre una variedad abeliana definida sobre $\mathbb{Q}$ y una subvariedad de la misma también definida sobre $\mathbb{Q}$, vuelve a ser una variedad abeliana definida sobre $\mathbb{Q}$ (ver [Kna92, Proposición 11.69]), A_f podrá definirse sobre $\mathbb{Q}$. Para probar que la dimensión de dicho espacio es en efecto $[K_f : \mathbb{Q}]$, enunciemos primero un Lema.

Lema 6.2.13. Denotemos a $\mathbb{T}_{\mathbb{C}}$ como $\mathbb{T}_{\mathbb{Z}} \otimes \mathbb{C}$. Luego existe un "pairing" no degenerado en cada entrada $\mathbb{T}_{\mathbb{C}} \times S_2(\Gamma_0(N)) \to \mathbb{C}$, que induce un isomorfismo de $\mathbb{T}_{\mathbb{Z}}$-módulos $\mathbb{T}_{\mathbb{C}} \cong S_2(\Gamma_0(N))^{\wedge}$.

Demostración. Definimos $\Phi : \mathbb{T}_{\mathbb{C}} \times S_2(\Gamma_0(N)) \to \mathbb{C}$ como $\Phi(T, f) = a_1(Tf)$ donde $a_n(f)$ representarán los coeficientes de f en su expansión en q. Dicho pairing es claramente $\mathbb{C}$-lineal en ambas coordenadas. Luego, para probar la no degeneridad, usamos el hecho de que para todo $T \in \mathbb{T}_{\mathbb{C}}$ y $f \in S_2(\Gamma_0(N))$, tenemos, por 5.4.5 que $a_1(T_n f) = a_n(f)$ para todo $n \geq 0$. Si $f \in S_2(\Gamma_0(N))$ es tal que $\phi(T, f) = 0$ para todo $T \in \mathbb{T}_{\mathbb{C}}$, entonces $a_n(f) = a_1(T_n f) = \Phi(T_n, f) = 0$ para todo $n \geq 0$, luego $f = 0$. Por otro lado, si $T \in \mathbb{T}_{\mathbb{C}}$ es tal que $\Phi(T, f) = 0$ para todo $f \in S_2(\Gamma_0(N))$, tenemos que $a_n(Tf) = a_1(T_n T f) = a_1(T_n T f) = \Phi(T, T_n f) = 0$ para todo f y $n \geq 0$, lo cual implica que T es el operador 0 en $S_2(\Gamma_0(N))$. Luego el isomorfismo viene dado por $g \mapsto (T \mapsto a_1(Tg))$. □

El siguiente resultado nos dirá que el conjunto de inyecciones de K_f en $\mathbb{C}$ actúa en el conjunto de autoformas de $S_2(\Gamma_0(N))$.

Definición 6.2.14. Para $f = \sum_n a_n(f) q^n \in S_2(\Gamma_0(N))$ y $\sigma : K_f \to \mathbb{C}$ una inyección, denotamos por f^σ a la función $\sum_n \sigma(a_n(f)) q^n$.

Teorema 6.2.15. Sea $f \in S_2(\Gamma_0(N))$ es una autoforma normalizada. Si $\sigma : K_f \to \mathbb{C}$ es una inyección de K_f en $\mathbb{C}$, entonces f^σ pertenece a $S_2(\Gamma_0(N))$. Más aún, si f es una forma nueva, entonces f^σ también lo es.

Demostración. Ver [Shu05, Teorema 6.5.4]. □

Por lo tanto, a partir del Teorema 6.2.15, podemos definir una relación de equivalencia entre formas nuevas en $S_2(\Gamma_0(N))$. Sean f y $\widetilde{f}$ formas nuevas. Decimos que $\widetilde{f} \sim f$ si $\widetilde{f} = f^\sigma$ con $\sigma : \mathbb{C} \to \mathbb{C}$ es un automorfismo. Denotamos por $[f] = \{f^\sigma |\ \sigma \in \mathrm{Aut}(\mathbb{C})\}$ la clase de equivalencia de f mediante esta relación. Luego la cardinalidad de dicha clase de equivalencia es la cantidad de incrustaciones $\sigma : K_f \to \mathbb{C}$. Denotaremos por V_f al subespacio de $S_2(\Gamma_0(N))$ de dimensión $[K_f : \mathbb{Q}]$ generado por $[f]$, es decir, $V_f = \langle [f] \rangle$.

Proposición 6.2.16. A_f tiene dimensión $[K_f : \mathbb{Q}]$.

Demostración. Por simplicidad denotaremos a S_2 por $S_2(\Gamma_0(N))$ y a Λ al retículo que describe $H_1(X_0(N);\mathbb{Z})$ en $S_2(\Gamma_0(N))^\wedge$, es decir al retículo de períodos dado por $\langle u_i : i = 1, \dots, 2g\rangle$ donde

$$u_i = \left(f \mapsto \int_{c_i} f(z)dz\right)$$

donde $\{c_i : i = 1, \dots 2g\}$ es una base de $H_1(X;\mathbb{Z})$. Denotamos también a $\bar{\Lambda}$ como la imagen de Λ en $S_2^\wedge/I_f(S_2^\wedge)$. Luego tenemos que

$$A_f \cong \frac{S_2^\wedge/\Lambda}{I_f(S_2^\wedge/\Lambda)} \cong \frac{S_2^\wedge/\Lambda}{(I_f S_2^\wedge + \Lambda)/\Lambda)} \cong \frac{S_2^\wedge}{I_f(S_2^\wedge) + \Lambda} \cong \frac{S_2^\wedge/I_f(S_2^\wedge)}{\bar{\Lambda}} \cong \frac{S_2[I_f]^\wedge}{\Lambda|_{S_2[I_f]}}.$$

como grupos de Lie complejos, donde $S_2[I_f]$ denota a los elementos de S_2 anulados por I_f. Además tenemos una suryección $(\mathbb{T}_\mathbb{Z}/I_f) \otimes \mathbb{C} \to \mathbb{T}_\mathbb{C}/I_f\mathbb{T}_\mathbb{C}$. Luego, usando el Lema 6.2.13 tenemos que

$$\dim(S_2[I_f]^\wedge) \leq \dim((\mathbb{T}_\mathbb{Z}/I_f) \otimes \mathbb{C}) = \operatorname{rank}(\mathbb{T}_\mathbb{Z}/I_f) = \operatorname{rank}(\mathbb{Z}[a_n(f) : n \geq 0]) = [K_f : \mathbb{Q}]$$

Luego como el espacio V_f previamente mencionado está en $S_2[I_f]$ y tiene dimensión $[K_f : \mathbb{Q}]$ concluimos que $V_f = S_2[I_f]$, por lo que $V_f^\wedge = S_2[I_f]^\wedge$. Por lo tanto

$$A_f \cong V_f^\wedge/\Lambda_f$$

como grupos de Lie complejos, donde $\Lambda_f = \Lambda|_{V_f}$. Además se puede ver que Λ_f termina siendo un retículo en $V_f^\wedge$ (ver [Shu05, §VI.6]). Por lo tanto A_f termina siendo isomorfo a un toro complejo de dimensión $[K_f : \mathbb{Q}]$, por lo que tendrá dimensión $[K_f : \mathbb{Q}]$ como variedad compleja. □

Observación 6.2.17. En el caso particular que A_f tiene dimensión 1 quedará isomorfa a un toro complejo de dimensión 1, es decir a una curva elíptica. Además notar que si $[K_f : \mathbb{Q}] = 1$ entonces $V_f = \langle f\rangle$, es decir, será generado por una sola forma nueva, que es justamente f. Luego A_f quedará

$$A_f = V_f^\wedge/\Lambda_f = \langle f\rangle^\wedge/\Lambda_f \cong \mathbb{C}/\Lambda$$

donde $\Lambda = \langle\int_\gamma f\rangle_\mathbb{Z}$. Por lo cual se verifica lo que afirmábamos.

Mencionar además que $\mathrm{Jac}(X_0(N)) \twoheadrightarrow A_f$, es justamente la proyección al cociente por $I_f(\mathrm{Jac}(X_0(N)))$ por lo que será sobreyectiva y morfismo sobre $\mathbb{Q}$, al ser A_f y $\mathrm{Jac}(X_0(N))$ variedades abelianas definidas sobre $\mathbb{Q}$. Con esto se prueba el apartado (a) del Teorema de Eichler-Shimura. Para una demostración de los demás apartados ver [Shi71, §VII.5].

Como mencionamos en la Observación 6.2.17, cuando $[K_f : \mathbb{Q}] = 1$ nos queda que A_f es una curva elíptica. Observar que esto sucede cuando la forma nueva f tiene los coeficientes de su expansión de q en $\mathbb{Q}$. Más aún, cuando los coeficientes de f son todos enteros, entonces las L series coinciden exactamente y además N termina siendo el conductor de la curva elíptica.

Teorema 6.2.18. (Carayol) Sea $f \in S_2(\Gamma_0(N))$ una forma nueva normalizada cuyos coeficientes de Fourier son enteros, y sea E la curva elíptica sobre $\mathbb{Q}$ asociada a f por Eichler Shimura. Entonces $L(s,E) = L(s,f)$ y N es el conductor de E.

Demostración. Sale como Corolario del Teorema A en [Car86] §XII. □

Por lo que nos queda el siguiente teorema:

Teorema 6.2.19. (Eichler-Shimura) Sea $f = \sum_{n=0}^{\infty} a_n(f)q^n \in S_2^{\text{new}}(\Gamma_0(N))$ una forma nueva normalizada de nivel N tal que $a_n(f) \in \mathbb{Z}$ para todo n. Luego existe un par (E_f, ν) tal que

(a) E_f es una curva elíptica definida sobre $\mathbb{Q}$ y

$$\text{Jac}(X_0(N)) \twoheadrightarrow E_f$$

es un morfismo sobreyectivo definido sobre $\mathbb{Q}$;

(b) ν es un isomorfismo de $\mathbb{Q}$ en $\text{End}(E_f) \otimes \mathbb{Q}$; Los operadores de Hecke t_n en $\text{End}(\text{Jac}(X_0(N)))$ actúan en E_f por multiplicación por a_n;

(c) Las dos propiedades previamente mencionadas caracterizan a (E_f, ν) salvo isomorfismos sobre $\mathbb{Q}$;

(d) $L(s, E_f/\mathbb{Q}) = L(s,f)$.

6.3. El recíproco de Eichler-Shimura

Al final de la sección anterior vimos que, a toda forma nueva normalizada $f \in S_2^{\text{new}}(\Gamma_0(N))$ con coeficientes racionales le puedo asociar de forma única, salvo isomorfismos sobre $\mathbb{Q}$, una curva elíptica sobre $\mathbb{Q}$ tal que sus L-series coinciden. Nos preguntamos si vale la recíproca. Es decir, si toda curva elíptica sobre $\mathbb{Q}$ viene dada por una forma nueva f como en el teorema de Eichler-Shimura.

Sea E una curva elíptica sobre $\mathbb{Q}$, y sea N_E su conductor. Entonces tenemos el siguiente resultado.

Proposición 6.3.1. Son equivalentes

(a) E es isógena sobre $\mathbb{Q}$ a una curva elíptica E_f dada por el Teorema de Eichler Shimura, con $f \in S_2^{\text{new}}(\Gamma_0(N_E))$.

(b) Existe un morfismo no constante sobre $\mathbb{Q}$, de $X_0(N_E)$ en E.

Demostración. Ver [DT95, §I.8.] □

Una curva elíptica sobre $\mathbb{Q}$ con dicha propiedad se dice que es *modular*.

Teorema 6.3.2. (Teorema de Modularidad, Versión $X_{\mathbb{Q}}$) Toda curva elíptica sobre $\mathbb{Q}$ es modular.

Este teorema fue conjeturado por Shimura-Taniyama en 1957. Existen otras versiones del Teorema de modularidad, dos de ellas las discutiremos a continuación y las otras dos en el Capítulo 7. Todas estas versiones van a terminar siendo equivalentes. La conjetura fue probada primeramente para los casos de curvas elípticas semiestables, mediante los trabajos de Wiles [Wil95] y Taylor-Wiles [Tay95], más precisamente se probó la versión R

de modularidad. Unos años más adelante Brian Conrad, Fred Diamond y Richard Taylor, basándose en los trabajos previamente citados, probaron la conjetura de Shimura-Taniyama para toda curva elíptica sobre $\mathbb{Q}$.

Una de las implicaciones del Teorema de modularidad, a parte de formar parte de la demostración del Último Teorema de Fermat, es la extensión de forma entera de las L-series de las curvas elípticas. En efecto,

Proposición 6.3.3. Si $E/\mathbb{Q}$ es modular, es decir, asociada a una forma nueva $f \in S_2^{\text{new}}(\Gamma_0(N))$ mediante la construcción de Eichler-Shimura, entonces

$$L(s, E/\mathbb{Q}) = L(f, s).$$

En particular, $L(s, E/\mathbb{Q})$ tiene una extensión analítica a todo el plano complejo. Más aún, la función

$$\Lambda(s, f) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(s, E/\mathbb{Q})$$

satisface la ecuación funcional

$$\Lambda(s, f) = -\varepsilon\Lambda(2 - s, E/\mathbb{Q}).$$

Demostración. (Idea) Como $E/\mathbb{Q}$ es modular, existe una curva elíptica $E_f/\mathbb{Q}$ asociada a una forma nueva $f \in S_2^{\text{new}}(\Gamma_0(N_E))$ (con N_E el conductor de E_f) tal que $E/\mathbb{Q}$ y $E_f/\mathbb{Q}$ son isógenas sobre $\mathbb{Q}$. Luego por la Proposición 4.6.15 tenemos que $L(s, E/\mathbb{Q}) = L(s, E_f/\mathbb{Q})$. Además por el Teorema de Eichler Shimura (la versión 6.2.19), obtenemos que $L(s, E_f/\mathbb{Q}) = L(s, f)$, por lo que $L(s, E/\mathbb{Q}) = L(f, s)$. La última afirmación sale directa del Teorema 5.3.7 reemplazando k por 2. □

Saber que la L serie de una curva elíptica se extiende de forma entera es importante ya que se conjetura que $L(s, E)$ contiene información sofisticada acerca de la estructura de grupo de E. Por ejemplo nos ayuda a intuir cuanto va a ser el rango de $E(\mathbb{Q})$.

Conjetura 6.3.4. (Conjetura débil de Birch y Swinnerton-Dyer) Sea E una curva elíptica definida sobre $\mathbb{Q}$. Luego el orden de anulación de $L(s, E)$ en $s = 1$ es el rango de $E(\mathbb{Q})$. Esto es, si $E(\mathbb{Q})$ tiene rango r entonces

$$L(s, E) = (s - 1)^r g(s),\ g(1) \neq 0, \infty.$$

Volviendo al Teorema de modularidad, existen otras dos versiones equivalentes a la Versión $X_{\mathbb{Q}}$ que son equivalentes entre si.

Teorema 6.3.5. (Teorema de Modularidad, Versión a_p) Sea E una curva elíptica sobre $\mathbb{Q}$ con conductor N_E. Entonces para alguna forma nueva $f \in S_2(\Gamma_0(N_E))$,

$$a_p(f) = a_p(E) \text{ para todo primo } p.$$

Teorema 6.3.6. (Teorema de Modularidad, Versión L) Sea E una curva elíptica sobre $\mathbb{Q}$ con conductor N_E. Entonces para alguna forma nueva $f \in S_2(\Gamma_0(N_E))$,

$$L(s, f) = L(s, E).$$

Proposición 6.3.7. Las Versiones $X_{\mathbb{Q}}$, a_p y L de modularidad son equivalentes.

Demostración. Versión $X_{\mathbb{Q}} \Longrightarrow$ Versión L. Probado en la demostración de la Proposición 6.3.3.

Versión $L \Longrightarrow$ Versión $X_{\mathbb{Q}}$. Sale usando el Toerema de Isogenías de Faltings (ver Corolario 5.2 en el Capítulo §II de [CA86]).

Versión $a_p \Longleftrightarrow$ Versión L. Sale usando las relaciones que existen entre los coeficientes $a_n(E)$ que aparecen en $L(s, E)$. Ver al final del Capítulo §XIII.8. en [Shu05]. □

En la Sección 7.1 del siguiente Capítulo probaremos la equivalencia de la Versión a_p con las versiones R, versiones las cuales será utilizadas para probar el Último Teorema de Fermat.

Capítulo 7

Representación modular de Galois

En este Capiúlo definiremos, para cada forma nueva en $S_2(\Gamma_0(N))$, una representación de Galois asociada. Definiremos el concepto de representación modular y enunciaremos la Versión R de los Teoremas de Modularidad. Nos basaremos en los resultados desarrollados en [Shu05].

Sea K un cuerpo de números, no necesariamente Galois sobre $\mathbb{Q}$ y $l \in \mathbb{N}$ primo. Sea además

$$\ell\mathcal{O}_K = \prod_{\lambda|\ell} \lambda^{e_\lambda},$$

la descomposición en ideales primos de ℓ en $\mathcal{O}_K$. Para cada λ, definimos al anillo de enteros λ-ádicos como el límite inverso

$$\mathcal{O}_{K,\lambda} = \varprojlim_n \{\mathcal{O}_K/\lambda^n\}.$$

Llamamos al *cuerpo de números λ-ádico* al cuerpo de fracciones de $\mathcal{O}_{K,\lambda}$ y lo denotamos por K_λ.

Si ℓ es un primo, entonces tenemos el siguiente isomorfismo de anillos

$$K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} K_\lambda. \tag{7.1}$$

Para una demostración de dicho isomorfismo ver [Shu05] §IX.2.

Definiremos ahora un caracter de $G_{\mathbb{Q}}$ que va a resultar ser una representación de Galois y que precisaremos más adelante. Denotamos a $\mathbb{Q}(\mu_{\ell^\infty})$ por

$$\mathbb{Q}(\mu_{\ell^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\mu_{\ell^n}),$$

donde μ_{ℓ^n} es la raíz ℓ^n-ésima de la unidad. Este es un subcuerpo de $\overline{\mathbb{Q}}$ pero no es un cuerpo de números al tener grado infinito sobre $\mathbb{Q}$. Denotamos tambíen a $G_{\mathbb{Q},\ell}$ como

$$G_{\mathbb{Q},\ell} = \mathrm{Aut}(\mathbb{Q}(\mu_{\ell^\infty})).$$

Como $\mathbb{Q}(\mu_{\ell^\infty}) \subset \overline{\mathbb{Q}}$ tenemos un epimorfismo $G_\mathbb{Q} \to G_{\mathbb{Q},\ell}$, dado por $\sigma \mapsto \sigma|_{\mathbb{Q}(\mu_{\ell^\infty})}$. Además se puede ver que $G_{\mathbb{Q},\ell} \to \mathbb{Z}_\ell^*$ dado por $\sigma \mapsto (m_1, m_2, m_3, \ldots)$ donde m_n es tal que $\sigma|_{\mathbb{Q}(\mu_{\ell^n})}(\mu_{\ell^n}) = \mu_{\ell^n}^{m_n}$, es un isomorfismo de grupos (ver [Shu05] §IX.2). Luego tenemos el caracter ciclótimico ℓ-ádico de $G_\mathbb{Q}$ dado por,

$$\chi_\ell : G_\mathbb{Q} \to \mathbb{Q}_\ell^*, \quad \sigma \mapsto (m_1, m_2, m_3, \ldots) \text{ donde } \sigma|_{\mathbb{Q}(\mu_{\ell^n})}(\mu_{\ell^n}) = \mu_{\ell^n}^{m_n} \text{ para todo } n.$$

Para probar que χ_ℓ es continuo se procede de la misma forma que vimos en la Sección 4.8 para la representación $\rho_{E,\ell}$. En efecto, podemos ver que $\chi_\ell^{-1}(U_{\mathrm{Id}}(n)) = U_{\mathrm{id}}(\mathbb{Q}(\mu_{\ell^n}))$. Luego χ_ℓ es una representación de Galois de dimensión 1.

7.1. Representación modular

Como hicimos con las curvas elípticas, vamos a querer asociarle a las formas cuspidales de peso 2 una representación de Galois. Vamos a realizar un procedimiento similar para defininir dichas representaciones. En vez de de definirlas en base a la acción de $G_\mathbb{Q}$ en el módulo de Tate asociado a una curva elíptica lo haremos en base a la acción de $G_\mathbb{Q}$ en el módulo de Tate asociado a la variedad dada por la construcción de Eichler Shimura A_f asociada a la forma nueva f.

Recordemos que en la construcción de Eichler Shimura vista en el Capítulo 6 le asociábamos a cada forma nueva $f = \sum a_n(f)q^n \in S_2^{new}(\Gamma_0(N_f))$ una variedad abeliana A_f de dimensión $[K_f : Q]$, donde K_f denotaba el cuerpo de números en $\mathbb{C}$ generado por los coeficientes de Fourier $a_n(f)$. Así como definimos el módulo de Tate para curvas elípticas se puede etender dicha definición para variedades abelianas de dimensión mayor, es decir,

$$\mathrm{Ta}_\ell(A_f) = \varprojlim_n \{A_f[\ell^n]\}.$$

Se puede ver que $\mathrm{Ta}_\ell(A_f) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ es un módulo libre de rango 2 sobre $K_f \otimes \mathbb{Q}_\ell$ (ver Lema 9.5.3 en [Shu05]). El grupo absoluto de Galois $G_\mathbb{Q}$ actua en $\mathrm{Ta}_\ell(A_f) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ de forma $K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell$-lineal, y por lo observado al principio $\mathrm{Ta}_\ell(A_f) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong (K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell)^2$. Luego eligiendo una base de $\mathrm{Ta}_\ell(A_f) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ tenemos un homomorfismo $G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell)$. Además del isomorfismo dado en (7.1) tenemos que

$$K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} K_{f,\lambda},$$

donde $K_{f,\lambda}$ denota el cuerpo de fracciones de $\mathcal{O}_{K_f,\lambda}$. Luego para cada λ sobre ℓ, podemos descomponer el homomorfismo dado mediante una proyección para obtener

$$\rho_{f,\lambda} : G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(K_{f,\lambda}).$$

que resulta ser continua, por lo que termina siendo una representación de Galois de dimensión 2. Luego obtenemos el siguiente Teorema:

Teorema 7.1.1. Sea $f \in S_2(\Gamma_0(N))$ una autofunción normalizada para todo operador de Hecke T_n, con cuerpo de números asociado K_f. Sea ℓ primo. Para cada ideal primo λ en $\mathcal{O}_{K_f}$ sobre ℓ existe una representación de Galois de dimensión 2

$$\rho_{f,\lambda} : G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(K_{f,\lambda}).$$

Esta representación no ramifica en todo primo $p \nmid \ell N$. Para dichos primos p sea $\mathfrak{p} \subset \bar{\mathbb{Z}}$ un ideal primo sobre p. Luego $\rho_{f,\lambda}(\mathrm{Frob}_\mathfrak{p})$ satisface la ecuación

$$x^2 - a_p(f)x + p = 0. \tag{7.2}$$

Demostración. La existencia de dicha representación ya la construimos, y para lo demás ver [Shu05, §IX.5]. □

Observación 7.1.2. Si $\rho \sim \rho_{f,\lambda}$ entonces $\rho(\mathrm{Frob}_\mathfrak{p})$ también satisface la ecuación (7.2). En efecto, como $\rho \sim \rho_{f,\lambda}$, existe $m \in \mathrm{GL}_2(K_{f,\lambda})$ tal que $\rho(\sigma) = m^{-1}\rho_{f,\lambda}(\sigma)m$ para todo $\sigma \in G_\mathbb{Q}$. Luego $(\rho(\mathrm{Frob}_\mathfrak{p}))^2 - a_p(f)\rho(\mathrm{Frob}_\mathfrak{p}) + p = m^{-1}((\rho_{f,\lambda}(\mathrm{Frob}_\mathfrak{p}))^2 - a_p(f)\rho_{f,\lambda}(\mathrm{Frob}_\mathfrak{p}) + p)m = 0$.

Ahora dada una representación de Galois vamos a querer saber cuando será equivalente a alguna representación $\rho_{f,\lambda}$. Definimos entonces:

Definición 7.1.3. Una representación de Galois

$$\rho : G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell)$$

tal que $\det\rho = \chi_\ell$ se dice *modular* si existe una forma nueva $f \in S_2^{new}(\Gamma_0(M_f))$ tal que $K_{f,\lambda} = \mathbb{Q}_\ell$ para algún ideal primo λ de $\mathcal{O}_{K_f}$ que esté sobre ℓ y tal que $\rho_{f,\lambda} \sim \rho$.

Las representaciones $\rho_{E,\ell}$ que vimos en la Sección 4.8 son candidatas a ser representaciones modulares. En efecto, son irreducibles por el Teorema 4.8.4 y cumplen que $\det\rho_{E,\ell} = \chi_\ell$ (ver la demostración de [Shu05, Teorema 9.4.1]). Veamos además, que esta nueva definición de modularidad para representaciones es compatible con la definición de modularidad que definimos en la Sección 6.3. Enunciamos entonces los Teoremas de Modularidad Versión R.

Teorema 7.1.4. (Teorema de Modularidad, Versión R) Sea E una curva elíptica sobre $\mathbb{Q}$. Luego $\rho_{E,\ell}$ es modular para algún ℓ.

Esta es la versión que fue probada, para las curvas elípticas semiestables en [Wil95], y [Tay95] y luego para curvas en general en [BCT01].

Teorema 7.1.5. (Teorema de Modularidad, Versión R fuerte) Sea E una curva elíptica sobre $\mathbb{Q}$ con conductor N. Entonces para alguna forma nueva $f \in S_2^{new}(\Gamma_0(N))$ con cuerpo de números $K_f = \mathbb{Q}$,

$$\rho_{f,\ell} \sim \rho_{E,\ell} \text{ para todo } \ell.$$

Veamos ahora que estas versiones del Teorema de Modularidad son equivalentes con las tres versiones vistas en la Sección 6.3.

Proposición 7.1.6. Las versiones a_p, R y R fuerte de Modularidad son equivalentes.

Demostración. Versión $R \Longrightarrow$ Versión a_p. Sea E una curva elíptica sobre $\mathbb{Q}$ con conductor N. Luego existe una forma nueva $f \in S_2^{new}(\Gamma_0(N))$ como en la Definición 7.1.3, tal que $\rho_{f,\lambda} \sim \rho_{E,\ell}$ para algún ideal primo λ sobre ℓ. Luego, por la Observación 7.1.2, tenemos que $\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})$ satisface la ecuación $x^2 - a_p(f)x + p$ para cualquier Frobenius Absoluto $\mathrm{Frob}_\mathfrak{p}$ donde $\mathfrak{p}$ es un ideal primo sobre $p \nmid \ell M_f$. Pero por el Teorema 4.8.4, el polinomio característico de $\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})$ para cualquier $\mathrm{Frob}_\mathfrak{p}$ donde $p \nmid \ell N$ es $x^2 - a_p(E) + p$. Por lo tanto $x^2 - a_p(f)x + p = x^2 - a_p(E) + p$ y entones $a_p(f) = a_p(E)$.

Versión $a_p \Longrightarrow$ Versión R fuerte. Ver [Shu05, §IX.6].

Versión R fuerte $\Longrightarrow$ Versión R. Trivial. □

Corolario 7.1.7. Sea E una curva elíptica sobre $\mathbb{Q}$. Entonces

si $\rho_{E,\ell}$ es modular para algún ℓ entonces $\rho_{E,\ell}$ es modular para todo ℓ.

Definamos ahora lo que son las representaciones modulares mod ℓ que serán de vital importancia para la demostración del Último Teorema de fermat. Sea $f \in S_2^{new}(\Gamma_0(N))$ una forma nueva y sea $\lambda \in \mathcal{O}_{K_f}$ un ideal primo sobre ℓ. Podemos suponer, salvo equivalencia, que la representación $\rho_{f,\lambda}$ tiene imagen en $\mathrm{GL}_2(\mathcal{O}_{K_f,\lambda})$. Por lo que se reduce, mod ℓ a la representación

$$\bar{\rho}_{f,\lambda} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathcal{O}_{K_f,\lambda}/\lambda\mathcal{O}_{K_f,\lambda}).$$

Más en general, consideraremos representaciónes mod ℓ, $\bar{\rho} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ donde $\overline{\mathbb{F}}_\ell$ tiene la topología discreta y $\bar{\rho}$ es continua. Como $G_{\mathbb{Q}}$ es compacta esto significa que la imagen de $\bar{\rho}$ es finita y por lo tanto está en $\mathrm{GL}_2(\mathbb{F}_{\ell^r})$ para algún r. La noción de modularidad se aplica para las representaciones mod ℓ.

Definición 7.1.8. Una representación irreducible $\bar{\rho} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ es *modular de nivel* N si existe una forma nueva $f \in S_2(\Gamma_0(N))$ y un ideal primo λ en $\mathcal{O}_{K_f}$ sobre ℓ tal que $\bar{\rho}_{f,\lambda} \sim \bar{\rho}$.

Observación 7.1.9. Si $\rho_{E,\ell}$ es modular de nivel N, entonces $\bar{\rho}_{E,\ell}$ es modular de nivel N.

Capítulo 8

El Teorema de Fermat-Wiles

En este último Capítulo comenzaremos hablando acerca de como surgió la idea de utilizar curvas elípticas para afrontar el Último Teorema de Fermat. Seguiremos hablando acerca del resultado de Frey sobre las curvas de Hellegourach-Frey, en el cual vincula la conjetura de Shimura-Taniyama con la conjetura epsilon de Serre. Finalmente, uniremos todos estos resultados junto a los Teorema de Ribet-Mazur y Wiles para probar el Último Teorema de Fermat.

8.1. La conjetura de Serre y la conexión de Frey

Como mencionamos anteriormente, el primero en vincular las curvas elípticas al Último Teorema de Fermat fue Hellegourach. Este menciona que esta idea le surgió al estar trabajando en una demostración del Teorema de Manin. Hellegourach llegó a la siguiente afirmación:

Teorema 8.1.1. Si una curva elíptica $E/\mathbb{Q}$ con 2-torsión racional admite un punto de orden p^2, entonces la curva

$$X^{2p} + Y^{2p} = Z^{2p}$$

admite $\frac{p-1}{2}$ soluciones no triviales en $\mathbb{P}^2(\mathbb{Q})$.

Por lo tanto, de forma lógica, planteó la recíproca a dicha afirmación. Es decir, partiendo de una solución al Último Teorema de Fermat, llegar a una curva elíptica y estudiar sus puntos de p-torsión. De esta forma es que asoció una solución (a, b, c) a la curva E_{a^p,b^p,c^p}. Hellegourach tuvo, además, otras motivaciones a parte de la motivación lógica para plantear esta asociación. Para más detalles al respecto ver el Apéndice de [Hel01].

Frey [Fre86], por otro lado, afirmaba que las curvas introducidas por Hellegourach no iban a ser modulares, lo cual contradecería la conjetura de Shimura-Taniyama para curvas semiestables. Frey se basó en la conjetura épsilon de Serre para apoyar su idea. Dicha conjetura había sido comunicada por Serre en una carta a Mestre en 1985 [Mes87].

Para enunciar la conjetura de Serre precisaremos de tres definiciones.

Definición 8.1.2. Diremos que una representación ρ es impar si $\det \rho(c) = -1$, donde c es la conjugación compleja

La siguiente definición no la daremos ya que es demasiado técnica, pero se puede ver en [Ser87, página 189]. Dicha definición es respecto a cuando se dice que una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ es finita en p. Bastará saber que si una curva elíptica $E/\mathbb{Q}$ tiene reducción buena en p o bien si tiene reducción multiplicativa en p con $p|v_p(\Delta_E)$, entonces $\bar{\rho}_{E,p}$ es finita en p (sale como resultado de las Proposiciones 4 y 5 en [Ser87]).

Corolario 8.1.3. Si $E = E_{a^p,b^p,c^p}$ es una curva de Hellegourach-Frey, entonces $\bar{\rho}_{E,p}$ es finita en p.

Demostración. Si $p \nmid abc$ entonces E tiene reducción buena en p por el Lema 4.9.2 (c). Si $p|abc$ entonces $p|v_p(\Delta_E)$ ya que, por el Lema 4.9.2 (a), tenemos que $\Delta_E = 16(abc)^{2p}$. En ambos casos tendremos que $\bar{\rho}_{E,p}$ es finita en p por lo último que mencionamos en el párrafo anterior a este Corolario. □

La última definición es acerca del conductor de Artin de la representación. Tampoco la daremos, por la misma razón que la definición anterior, pero se puede ver en [Ser87, página 181]. El conductor de Artin de una representación $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$, que se denotará por $N_{\bar{\rho}}$, es, en el caso que la representación sea modular de nivel N, el minimo nivel que tendrá dicha representación. Una observación importante, que sale de la Definición del conductor de Artin (ver [Ser87, Definición 1.2]), es la siguiente:

Observación 8.1.4. Sea $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ una representación de Galois, entonces $p \neq \ell$ divide a $N_{\bar{\rho}}$ si y solo si $\bar{\rho}$ ramifica en p.

Más aún se puede ver cuanto será dicho conductor para el caso de curvas elípticas semiestables.

Proposición 8.1.5. Sea $E/\mathbb{Q}$ una curva elíptica semiestable. Luego el conductor de Artin de $\bar{\rho}_{E,\ell}$ es

$$N_{\bar{\rho}_{E,\ell}} = \prod_{\substack{p \neq \ell \\ v_p(\Delta_{\min}(E)) \not\equiv 0 \pmod{\ell}}} p.$$

Demostración. Ver [Ser87, Proposición 5]. □

El conductor de Artin va a ser muy importante ya que, al bajarle el nivel a la representación, se llegará a un absurdo al suponer que existe una solución a la ecuación al Último Teorema de Fermat.

La Conjetura épsilon de Serre (ahora Teorema) se generaliza en [Ser87] de la siguiente forma:

Conjetura 8.1.6. (Serre) Sea $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ una representación modular, irreducible e impar. Entones $\bar{\rho}$ es modular de nivel $N_{\bar{\rho}}$.

Serre, en [Ser87, 3.3.1] suaviza la condición de ser irreducible sobre $\overline{\mathbb{F}}_p$ para representaciones $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$.

Conjetura 8.1.7. (Serre) Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ una representación irreducible (sobre $\mathbb{F}_p$), impar y finita en p. Entones ρ es modular de nivel N_ρ.

Estas últimas dos conjeturas son mucho más fuerte que la Conjetura épsilon. En particular estas implican la Conjetura de Shimura-Taniyama (ver [Ser87, 4.6]). Sin embargo solo bastaba con que la conjetura épsilon y la conjetura de Shimura Taniyama valieran.

Frey [Fre86], asumiendo la Conjetura épsilon de Serre, prueba, asumiendo además que es cierta la Conjetura de Shimura-Taniyama para curvas elípticas semiestabes, el último Teorema de Fermat. Es decir:

Shimura-Taniyama (caso semiestable) + Conjetura épsilon $\Rightarrow$ Último Teorema de Fermat.

Por lo que solo bastaba probar dichas conjeturas y el problema estaba resuelto.

8.2. Ribet-Mazur, Wiles y la prueba del Teorema de Fermat-Wiles

Ribet y Mazur [Rib90] probaron la conjetura épsilon de Serre, también llamada conjetura de bajada de nivel. Dejando solo por probar el Teorema de Shimura-Taniyama, para curvas semiestables, para probar Último Teorema de Fermat. El resultado que probaron fue el siguiente.

Teorema 8.2.1. (Ribet-Mazur) Sea $\ell \geq 3$ y $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ una representación irreducible, finita en p, modular de nivel N y tal que p divide exactamente a N (es decir, que $p|N$ pero que $p^2 \nmid N$). Luego ρ es modular de nivel N/p cuando valgan una o dos de las siguientes condiciones

(a) $p \not\equiv 1 \pmod{\ell}$,
(b) N es coprimo con ℓ.

Demostración. Mazur prueba este Teorema para el caso (a) en [Maz87] y Ribet prueba el caso restante en [Rib90] incluyendo, además, el caso probado por Mazur. □

Supongamos ahora que $p \nmid N_{\bar{\rho}}$, lo cual se cumple para $\bar{\rho}_{E,p}$ para curvas semiestables debido a la Proposición 8.1.5. Luego precisando esto y teniendo en cuenta la Definición del conductor de Artin, el resultado de Ribet-Mazur se puede expresar, de la siguiente forma:

Teorema 8.2.2. (Ribet-Mazur) Sea $p \geq 3$ primo. Sea $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ una representación irreducible, modular de nivel N y finita en p. Entonces $\bar{\rho}$ es modular de nivel $N_{\bar{\rho}}$ donde $N_{\bar{\rho}}$ es el conductor de Artin de $\bar{\rho}$.

Por lo tanto, como mencionamos, solo faltaba probar el la Conjetura de Shimura-Taniyama para curvas semiestables. Esta conjetura fue probada por Wiles y Taylor-Wiles en [Wil95] y [Tay95] respectivamente.

Teorema 8.2.3. (Wiles) Toda curva elíptica $E/\mathbb{Q}$ semiestable es modular.

Wiles y Taylor-Wiles, se basaron en ciertos resultados de Langlands-Tunell para probar que, si E era una curva elíptica semiestable, entonces o bien $\rho_{E,3}$, o bien $\rho_{E,5}$, iban a ser modulares. Esto prueba la Versión R del Teorema de Modularidad (7.1.4) para curvas semiestables, y por la equivalencia entre todas sus versiones prueba las demás para este caso.

Finalmente, usando los resultados de Ribet-Mazur, Wiles y la idea de Frey se prueba el resultado deseado.

Teorema 8.2.4. (Fermat-Wiles) Sea $p \geq 5$ primo. Entonces no existen soluciones primitivas no triviales a la ecuación $x^p + y^p = z^p$.

Demostración. Sea (a, b, c) una solución primitiva no tirivial a la ecuación del enunciado para algún primo $\ell \geq 5$. Como la solución es primitiva podemos suponer, salvo permutación, que $b \equiv 0 \pmod 2$ y que $a \equiv -1 \pmod 4$. Sea

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

la curva de Hellegourach-Frey asociada a dicha solución. La curva $E = E_{a^\ell, b^\ell, c^\ell}$ es semiestable por el Corolario 4.9.4 y luego, por el Teorema de Wiles 8.2.3, E será modular. Esto implica, debido a la versión R del Teorema de modularidad, que $\rho_{E,\ell}$ es modular de nivel N donde N es el conductor de E. Luego, por la Observación 7.1.9, $\bar{\rho}_{E,\ell}$ será modular de nivel N. Además, por la Proposición 4.8.1 y el Corolario 8.1.3 , $\bar{\rho}_{E,\ell}$ será irreducible y finita en ℓ. Luego $\bar{\rho}_{E,\ell}$ satisface las hipótesis del Teorema de Ribet-Mazur 8.2.2 y por lo tanto será modular de nivel $N_{\bar{\rho}_{E,\ell}}$. Por la proposición 8.1.5 tenemos que $2|N_{\bar{\rho}_{E,\ell}}$. Más aún, es el único primo que divide a $N_{\bar{\rho}_{E,\ell}}$. En efecto, si $p \neq 2, \ell$ divide a $N_{\bar{\rho}_{E,\ell}}$ entonces, por la Observación 8.1.4, $\bar{\rho}_{E,\ell}$ ramifica en p, lo cual contradice el Corolario 4.10.6. Luego $N_{\bar{\rho}_{E,\ell}} = 2$ y entonces $\bar{\rho}_{E,\ell}$ es modular de nivel 2. Es decir, existe una forma nueva $f \in S_2(\Gamma_0(2))$ y un ideal primo $\lambda \in \mathcal{O}_{K_f}$ sobre ℓ tal que $\bar{\rho}_{f,\lambda} \sim \bar{\rho}$. Pero esto es un absurdo, ya que contradice el Corolario 6.1.10. Por lo tanto no existe una solución primitiva no trivial a la ecuación $x^p + y^p = z^p$ para $p \geq 5$. □

Apéndice A

Series de Dirichlet y Productos de Euler

A.1. Series de Dirichlet

Definición A.1.1. Llamamos una serie de Dirichlet a una serie de la forma $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ con $a_n, s \in \mathbb{C}$

Proposición A.1.2. Sea $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ una serie de Dirichlet. Luego se cumple lo siguiente.

(a) Si la serie converge para $s = s_0$, luego converge uniformemente en conjuntos compactos para $\operatorname{Re} s > \operatorname{Re} s_0$, y la serie es analítica en dicha región.
(b) Si la serie es absolutamente convergente para $s = s_0$, luego es uniformemente convergente para $\operatorname{Re} s \geq \operatorname{Re} s_0$.
(c) Si la serie es convergente para $s = s_0$, luego es absolutamente convergente para $\operatorname{Re} s > \operatorname{Re} s_0 + 1$.
(d) Si la serie converge para un s_0 y suma 0 en un semiplano, entonces todos sus coeficientes son 0.

Demostración. Ver [Kna92, Proposición 7.2]. □

Teorema A.1.3. Sean $F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ y $G(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$ dos series de dirichlet convergentes absolutamente en el mismo semiplano. Luego

$$F(s)G(s) = \sum_{n=1}^{\infty} \left(\sum_{d|n} a_d b_{n/d} \right) n^{-s}$$

es una serie de dirichlet absolutamente convergente en el mismo semiplano que $F(s)$ y $G(s)$.

Demostración. Ver [Apo98, Teorema 11.5]. □

A.2. Producto de Euler

Definición A.2.1. Decimos que un producto

$$\prod_{j=1}^{\infty}(1+a_j)$$

converge si

(a) Solo un número finito de los $a_j's$ son iguales a -1.

(b) Si $N_0 > 0$ es suficientemente grande de forma tal que $a_j \neq -1$ para $j > N_0$, entonces

$$\lim_{N\to\infty} \prod_{j=N_0+1}^{N} (1+a_j)$$

existe y no es cero.

Si $\prod_{j=1}^{\infty}(1+a_j)$ converge, definimos su valor como

$$\left[\prod_{j=1}^{N_0}(1+a_j)\right] \cdot \lim_{N\to\infty} \prod_{j=N_0+1}^{N} (1+a_j).$$

Observemos el siguiente producto

$$\prod_{p \text{ primo}} (1 + a_p p^{-s} + \cdots + a_{p^m} p^{-ms} + \cdots). \tag{A.1}$$

Si $n = p_1^{r_1} \dots p_k^{r_k}$ definimos $a_n = a_{p_1^{r_1}} \dots a_{p_k^{r_k}}$. Se puede ver que

$$\prod_{p \text{ primo}} (1 + a_p p^{-s} + \cdots + a_{p^m} p^{-ms} + \cdots) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

en el semiplano donde la serie de dirichlet $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converge absolutamente.

Definición A.2.2. Decimos que una sucesión $\{a_n\}_{n=1}^{\infty}$ es multiplicativa si $a_1 = 1$ y $a_{mn} = a_m a_n$ cuando $\text{mcd}(m,n) = 1$ y escrictamente multiplicativa si $a_1 = 1$ y $a_{mn} = a_m a_n$ para todo $m, n \in \mathbb{N}$.

Si $\{a_n\}_{n=1}^{\infty}$ es multiplicativa podemos construirnos un producto como en la Ecuación (A.1) a partir de esta sucesión. Además dicho producto va a ser igual a la Serie de Dirichlet de dicha sucesión en el semiplano donde esta serie converge absolutamente. Decimos en este caso que la serie tiene un *producto de Euler*.

Si $\{a_n\}_{n=1}^{\infty}$ es estrictamente multiplicativa obtenemos que

$$1 + a_p p^{-s} + \cdots + a_{p^m} p^{-ms} + \cdots = 1 + a_p p^{-s} + \cdots + (a_p p^{-s})^m + \cdots = \frac{1}{1 - \frac{a_p}{p^s}}$$

En este caso decimos que nuestra serie de Dirichlet tiene un *producto de Euler de primer grado*.

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ primo}} \frac{1}{1 - \frac{a_p}{p^s}}$$

Recíprocamente, un producto de Euler fuerza a que la sucesión de la serie de Dirichlet sea estrictamente multiplicativa.

Definición A.2.3. Una expresión de la forma (A.1) se dice que es un *producto de Euler de grado k* si, para cada primo p, existe un polinomio $P_p(X) \in \mathbb{C}[X]$ de grado $\leq k$ y termino independiente 0 tal que

$$1 + a_p p^{-s} + \cdots + a_p^m (p^{-s})^m + \cdots = \frac{1}{1 - P_p(p^{-s})}.$$

Si factorizamos a $1 - P_p(X)$ sobre $\mathbb{C}$ de la forma $1 - P_p(X) = (1 - r_p^{(1)} X) \cdots (1 - r_p^{(k)} X)$ llamamos a los números $r_p^{(j)}$ las *raices recíprocas* de $1 - P_p(X)$.

Lema A.2.4. Sea $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ una serie de Dirichlet tal que $|a_n| \leq Cn^k$ para algunos $C, k \in \mathbb{R}$. Luego dicha serie es absolutamente convergente para $\operatorname{Re} s > k + 1$

Demostración. Inmediato pues

$$\sum_{n=1}^{\infty} \left| \frac{a_n}{n^s} \right| \leq \sum_{n=1}^{\infty} \frac{|Cn^k|}{|n^s|} = |C| \sum_{n=1}^{\infty} \frac{1}{n^{s-k}}.$$

y esta última serie converge si y solo si $\operatorname{Re}(s - k) > 1$, es decir, $\operatorname{Re} s > k + 1$. □

Proposición A.2.5. Un producto de Euler de grado k $\Pi[1 - P_p(p^{-s})]^{-1}$ cuyas raices recíprocas satisfagan que $|r_p^{(j)}| \leq p^c$ para algún $c \in \mathbb{R}$ y para todo p primo define una serie de Dirichlet absolutamente convergente para $\operatorname{Re} s > c + 1$. Para tales s la suma de la serie de Dirichlet es igual a su producto de euler

Demostración. Ver [Kna92, Proposición 7.6]. □

Bibliografía

[Apo98] T.M. Apostol. *Introduction to analytic number theory*. Springer Science & Business Media, 1998.

[BCT01] C. Breuil, B. Conrad, and F. Diamond & R. Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843–939, 2001.

[Bir13] H. Langet & C. Birkenhake. *Complex abelian varieties*, volume 302. Springer Science & Business Media, 2013.

[CA86] G. Cornell and J.H. Silverman & M. Artin. *Arithmetic geometry*, volume 14. Springer, 1986.

[Car86] H. Carayol. Sur les représentations l-adiques associées aux formes modulaires de hilbert. In *Annales scientifiques de l'École Normale Supérieure*, volume 19, pages 409–468, 1986.

[DT95] H. Darmon and F. Diamond & R. Taylor. Fermat's last theorem. *Current developments in mathematics*, 1995(1):1–154, 1995.

[Fre86] G. Frey. Links between stable elliptic curves and certain diophantine equations ann. univ. sareviensis. *Ser. Math.*, 1:1–40, 1986.

[Hel01] Y. Hellegouarch. *Invitation to the mathematics of Fermat-Wiles*. Elsevier, 2001.

[HK81] E. Hecke and J.R. Goldman & R. Kotzen. *Lectures on the theory of algebraic numbers*, volume 77. Springer, 1981.

[Hun80] T.W. Hungerford. *Algebra*. Springer, New York, 1980.

[Kna92] A.W. Knapp. *Elliptic curves*, volume 40. Princeton University Press, 1992.

[Lan13] S. Lang. *Algebraic number theory*, volume 110. Springer Science & Business Media, 2013.

[Maz77] B. Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977.

[Maz87] B. Mazur. Letter to. *J.F. Mestre (16 August 1985). Zbl*, 588, 1987.

[Mes87] J.F. Mestre. letter to. *J.P. Serre*, 8, 1987.

[Mil08] J.S. Milne. *Algebraic number theory*. JS Milne, 2008.

[Mir95] R. Miranda. *Algebraic curves and Riemann surfaces*, volume 5. American Mathematical Soc., 1995.

[Pac18] L. Dieulefait & A. Pacetti. Representaciones de galois. *Disponible en: https://www.famaf.unc.edu.ar/˜apacetti/agra3/RepGal.pdf*, 2018.

[Rib79] P. Ribenboim. *13 lectures on Fermat's last theorem*. Springer Science & Business Media, 1979.

[Rib90] K.A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Inventiones mathematicae*, 100(1):431–476, 1990.

[Ser87] J.P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Mathematical Journal*, 54(1):179–230, 1987.

[Sha86] Z.I. Borevich & I.R. Shafarevich. *Number theory*. Academic press, 1986.

[Shi71] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 1. Princeton university press, 1971.

[Shu05] F. Diamond & J. Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[Sil09] J.H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[Ste11] K.A. Ribet & W.A. Stein. Lectures on modular forms and hecke operators. *Disponible en: http://wstein.org/books/ribet-stein/main.pdf*, 2011.

[Tat75] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable IV*, pages 33–52. Springer, 1975.

[Tat92] J.H. Silverman & J. Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992.

[Tat93] J. Tate. A review of non-archimedean elliptic functions. *Elliptic Curves, Modular Forms and Fermat's Last Theorem*, pages 310–314, 1993.

[Tay95] A. Wiles & R. Taylor. Ring-theoretic properties of certain hecke algebras. *Annals of Mathematics*, pages 553–572, 1995.

[Was97] L.C. Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science & Business Media, 1997.

[Wil95] A. Wiles. Modular elliptic curves and fermat's last theorem. *Annals of mathematics*, 141(3):443–551, 1995.

Los abajos firmantes, miembros del Tribunal de evaluación de tesis, damos fe que el presente ejemplar impreso se corresponde con el aprobado por este Tribunal.