ISSN 1688-2806

Universidad de la República
Facultad de Ciencias

Conjetura de Serre y curvas elípticas en cuerpos cuadráticos reales

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

Santiago Radi

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

Director de Tesis
Gonzalo Tornaría ..... Universidad de la República

Tribunal
Gonzalo Tornaría ..... Universidad de la República
Ariel Pacetti ..... Universidad Nacional de Córdoba
Claudio Qureshi ..... Universidad de la República

Director Académico
Gonzalo Tornaría ..... Universidad de la República

Montevideo
miércoles 3 febrero, 2021

Conjetura de Serre y curvas elípticas en cuerpos cuadráticos reales, Santiago Radi.

ISSN 1688-2806

Esta tesis fue preparada en LaTeX usando la clase iietesis (v1.1).
Contiene un total de 130 páginas.
Compilada el miércoles 3 febrero, 2021.
http://www.cmat.edu.uy/

Agradecimientos

En la vida es casi imposible hacer las cosas solos. Siempre estamos necesitando de ayuda, de apoyo, de alguien con más experiencia que nos pueda guiar; y esto también se refleja en una actividad tan complicada pero interesante como es una tesis de maestría. Quiero utilizar esta sección para hacer mención a algunas personas que me marcaron el camino a lo largo de mi carrera como estudiante, y agradecerles su presencia.

Para empezar, un evento casual de este año me recordó que si a día de hoy estudio matemática es porque en 2009, cuando estaba en quinto de liceo, el profesor Andrés Miralles me mostró con su forma de enseñar lo hermosa que era esta disciplina. El se transformó en una referencia para mí en ese momento, y la razón inicial para elegir este camino de investigación.

En 2011, comencé la facultad de Ingeniería y me rodeé de personas que fueron, primero parte de mi grupo de estudio, y luego, amigos que hasta hoy conservo. En este segundo grupo, quiero destacar a Esteban Risso, Schubert Tabarez, Jona Acosta, Diego Rossi y Federico Martínez.

Ya más avanzado en la carrera de Ingeniería Eléctrica, la cantidad de estudiantes era menor, y por ende, los vínculos eran mayores. Si bien, muchas de estas personas ya fueron nombradas en mi proyecto de fin de carrera de ingeniería, quiero destacar a Franco La Paz y Martín Causa, dos personas con las que mantenemos contacto cinco años después de empezar nuestro proyecto de fin de carrera. La amistad se extendió más adelante con nuestro tutor, Julián Oreggioni.

En 2013, comencé la Licenciatura en Matemática, dispuesto a aprender lo que realmente me apasionaba. En este lugar, más pequeño en cuanto a la cantidad de estudiantes, me encontré con muchas personas con las cuales nos hemos juntado a resolver ejercicios y ayudarnos con dudas en los diferentes cursos. En esta lista, destaco a Damian Ferencz, Favio Pirán, Leandro Bentancour, Mauro Camargo, Ignacio Bustamante, Joaquín Lema, Cristian Caticha, Candido De Oliveira, Gonzalo Cousillas, Rodrigo Bottero, Agustín Castro, Josefina González, Pablo Maurente, Facundo Oliú y Alejandro Bellati.

Una vez avanzado en Teoría de Números, mis dudas se dirigían principalmente

a dos personas, que siempre se mostraron dispuestas a ayudarme, desde 2016 hasta el día de hoy. Por eso dedico este párrafo a dos personas: Gustavo Rama y Gonzalo Tornaría.

Para esta tesis de maestría, además de mi tutor Gonzalo Tornaría quién dedico muchísimo tiempo en este trabajo, quiero agradecer a los otros dos integrantes del tribunal: Ariel Pacetti y Claudio Qureshi, quienes aportaron sus conocimientos, haciendo comentarios muy valiosos que serán tenidos en cuenta para continuar la investigación.

Con respecto a la defensa, agradecer al tribunal, por permitirme hacerla un sábado (28 de noviembre de 2020) a la tarde, y a Lydia Tappa y a la Facultad de Ciencias por permitirme hacerla presencial en un año donde el Covid-19 restringía las posibilidades de defensas presenciales. También agradecer a las diecisiete personas invitadas, y a las trece personas que se conectaron por Zoom para enviarme su apoyo.

Para terminar con los agradecimientos, tengo tres grupos de personas que aún no fueron mencionados. Primero, amigos que mi carrera como docente me ha dado en estos cinco años, tanto docentes como alumnos. Destaco aquí a Marcelo Lanzilotta y a Camila Gardella. Segundo, amigos fuera de lo académico, como compañeros de banda o amigos de la infancia. Destaco aquí a David Diaz, Jeanpi Abreu, Pablo Carlis, Angela Chavasco, Nicolas Rey y Pablito armonía. Tercero, ex-novias que me acompañaron estos años: Paola Rodríguez, Mariana Rosich y Camila Alonso.

Por último y lo más importante: la familia, principalmente mis padres Sergio Radi y Beatriz Severo. Sin su apoyo, esfuerzo y amor, nunca hubiese tenido ni siquiera el tiempo para afrontar las carreras que elegí. Destaco también a Rocky Severo, Gabriela Gimenez, Mónica Severo, Oscar Poleselo, mis abuelos (IAIA y TATA) y mis primos Fernando Vidal y Abigail Poleselo.

Para todos ellos dedico este trabajo, así como todos los logros académicos que he conseguido. Todos aportaron su granito de arena para que esto fuese posible, y estaré eternamente agradecido.

"Uno puede devolver un préstamo de oro, pero está en deuda de por vida con aquellos que son amables."

Proverbio popular.

Prefacio

Este documento corresponde a mi tesis de Maestría en Matemática, más precisamente en la rama de Teoría de Números.

Se pueden marcar dos objetivos claros en este trabajo. En primer instancia, entender la Conjetura de Serre y todos los objetos matemáticos involucrados en su enunciado. Además, se agregan dos aplicaciones de la misma: el Último Teorema de Fermat y clasificar todas las curvas elípticas sobre $\mathbb{Q}$ de conductor primo.

Justamente la última aplicación motiva el segundo objetivo de este documento que es estudiar e intentar clasificar todas las curvas elípticas de conductor potencia de primo en algunos cuerpos cuadráticos reales. Este último objetivo es algo novedoso, puesto que aún no existen resultados publicados.

Con respecto a los requisitos para entender este trabajo, mencionaremos ahora algunas de las herramientas que utilizaremos libremente. Se asumirán conocidos conceptos de materias de cualquier carrera de grado de matemática. Conceptos de grupos, anillos, cuerpos y teoría de Galois, así como análisis complejo. Se asumirán también cuestiones de Geometría Algebraica clásica y Teoría de Números clásica.

Con respecto a Teoría de Números Algebraicos (TNA), se asumirán muchas ideas de cuerpos locales y globales, pero dejaremos referencia a algunos libros al comienzo del capítulo 1. Algo similar haremos con representaciones de grupos, curvas elípticas y formas modulares clásicas, en las que se hará un breve resumen de lo necesario en las secciones 2.1, 3.1 y 4.1 respectivamente, pero se dejarán algunas referencias para mayor detalle al comienzo de cada capítulo correspondiente.

El documento está dividido en 7 capítulos. Los primeros cinco serán para introducir las herramientas necesarias para los últimos dos capítulos, donde realmente se exponen los objetivos planteados al comienzo. Un teorista de números experimentado no encontrará nada realmente novedoso hasta el capítulo 4 de este documento en los que salvo excepciones, enunciaremos los teoremas necesarios referenciando la demostración.

En el capítulo , expondremos como se relacionan los objetos matemáticos que definiremos utilizando como ejemplo el Último Teorema de Fermat.

En el capítulo 1, introduciremos las extensiones no ramificadas y moderadas puesto que el estudio de su acción es importante para enunciar la Conjetura de Serre. También definiremos los grupos de ramificación en su versión más general y por último definiremos idèles, ray class group y enunciaremos el teorema fundamental de la teoría de Kummer. Los resultados expuestos en estas últimas secciones serán utilizados principalmente en el estudio de curvas con conductor potencia de primo sobre cuerpos cuadráticos reales.

En el capítulo 2 nos enfocaremos en representaciones de Galois de dimensión 2. Dedicaremos una sección breve al carácter ciclotómico puesto que aparece en las representaciones de Galois que más nos van a interesar, que son las de curvas elípticas y las de formas modulares. Las últimas secciones las dedicaremos a caracteres en $G_{\mathbb{Q}}$ e $I_{\mathfrak{l},t}$, que serán utilizados para desarrollar la Conjetura de Serre.

En el capítulo 3 daremos resultados de curvas elípticas. Primero las definiremos sobre cualquier cuerpo; luego introduciremos las representaciones de curva elípticas, daremos algunos resultados sobre isogenias y finalmente nos enfocaremos en curvas elípticas sobre cuerpos locales y cuerpos de números.

En el capítulo 4 introduciremos las formas modulares. Comenzaremos dando un breve resumen de formas modulares clásicas, para luego definir las que utilizaremos para enunciar la Conjetura de Serre, que son las formas modulares módulo ℓ. En la última sección daremos una idea de como se construyen las representaciones de Galois para formas modulares módulo ℓ.

En el capítulo 5 utilizaremos los resultados necesarios de los capítulos anteriores para enunciar la Conjetura de Serre. Las últimas dos secciones las dedicaremos para mostrar dos aplicaciones de las mismas, que fueron dadas por Jean Pierre Serre en el artículo donde presentó la conjetura. Como fue mencionado antes, estas aplicaciones son el Último Teorema de Fermat y clasificar todas las curvas elípticas sobre $\mathbb{Q}$ de conductor primo.

Por último, en el capítulo 6 encontraremos el estudio de curvas elípticas con conductor potencia de primo sobre algunos cuerpos cuadráticos reales. La primer sección será extender el concepto de formas modulares clásicas a formas modulares de Hilbert. Lo siguiente será enunciar y referenciar resultados de modularidad asociados a cuerpos cuadráticos reales conocidos y que serán utilizados en las secciones siguientes para la clasificación. Cabe mencionar que el trabajo no está terminado y los resultados obtenidos son parciales.

A lo largo del capítulo 6 utilizaremos herramientas computacionales para complementar los resultados teóricos. Es por eso que en el apéndice, adjuntamos el código de los programas realizados.

Tabla de contenidos

Introducción

Consideremos el "Último Teorema de Fermat" como puntapié a las herramientas que vamos a exponer. El "Último Teorema de Fermat", enuncia que si n es un entero mayor a 2, y existen enteros a, b, c tales que

$$a^n + b^n = c^n \tag{0.1}$$

entonces $abc = 0$.

Es claro que si, por ejemplo $b = 0$, entonces poniendo $a = c$, tenemos infinitas soluciones enteras al problema. Esto lo podemos hacer siempre que uno de los tres términos sea cero. Llamaremos soluciones triviales a este tipo de soluciones. Otra forma distinta de enunciar el teorema es decir entonces que no hay soluciones no triviales si $n > 2$.

Uno se encuentra entonces con un problema en el cual no puede "chequear" a mano todos los casos, ni de a, ni de b, ni de c, ni de n, porque son infinitos. Es aquí cuando la matemática necesita de estrategias diferentes y de nueva formas y objetos para atacar el problema.

La estrategia es simple y es la siguiente (que es muy usual en problemas matemáticos): asociarle a una posible solución no trivial un objeto con un determinado conjunto de propiedades, y luego concluir que tal objeto no puede existir. Lo difícil es claro, definir el objeto correcto y encontrarle propiedades que lleven a esa conclusión. En este problema en particular, ese trabajo llevó casi 400 años, pero permitió desarrollar una nueva forma de estudiar problemas aritméticos que se sigue utilizando a día de hoy y a la que se le siguen buscando nuevas generalizaciones para resolver problemas más difíciles.

Lo primero es que a las soluciones de ciertas ecuaciones diofánticas (esto es, una ecuación cuya solución sólo involucra números enteros), se les puede asociar curvas elípticas, que es un objeto de la forma

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

con los a_i racionales.

En este objeto, los puntos que satisfacen la ecuación de la curva elíptica se pueden sumar como es explicado en la figura 3.1 de la sección 3.1 formando un grupo abeliano con esa operación. En particular, podemos mirar sus puntos de ℓ-torsión con ℓ un número primo (es decir, puntos que al sumar ℓ veces consigo mismo dan el neutro del grupo).

Si miramos todos los puntos de ℓ-torsión de una curva elíptica, sus coordenadas (x, y) no necesariamente son racionales, por lo que podemos considerar la acción del grupo de Galois sobre las coordenadas de estos puntos. En la sección 3.2, veremos que la acción del grupo de Galois preserva la ℓ-torsión, por lo que nos restringimos a este subconjunto y la acción allí. Esto da lugar a un nuevo objeto que llamaremos la representación de Galois de una curva elíptica.

Las representaciones de Galois son un objeto de estudio en sí mismo, por lo que las representaciones de Galois de una curva elíptica son un subconjunto de estas con un interés en problemas aritméticos.

Tenemos hasta ahora un diagrama de la siguiente forma:

Por otro lado, desde principios del siglo XX, matemáticos como Felix Klein, Srinivasa Ramanujan, Godfrey Hardy, Erich Hecke entre otros, comenzaron a estudiar formas modulares. Las formas modulares, son funciones complejas holomorfas que satisfacen algunas propiedades extras de simetría. Las formas modulares se agrupan en conjuntos según dos números denominados peso y nivel, y un carácter de Dirichlet.

A lo largo del siglo XX, se demostró que dados el peso, el nivel y un carácter, las formas modulares conforman un espacio vectorial de dimensión finita (en otras palabras, hay pocas) y a su vez, es computable la dimensión en casi todos los casos y son computables las formas modulares en casi todos los casos.

Dentro de las formas modulares, hay un subconjunto relevante, que es el de las formas propias cuspidales, que también conforman un espacio vectorial de dimensión finita por ser un subconjunto del anterior.

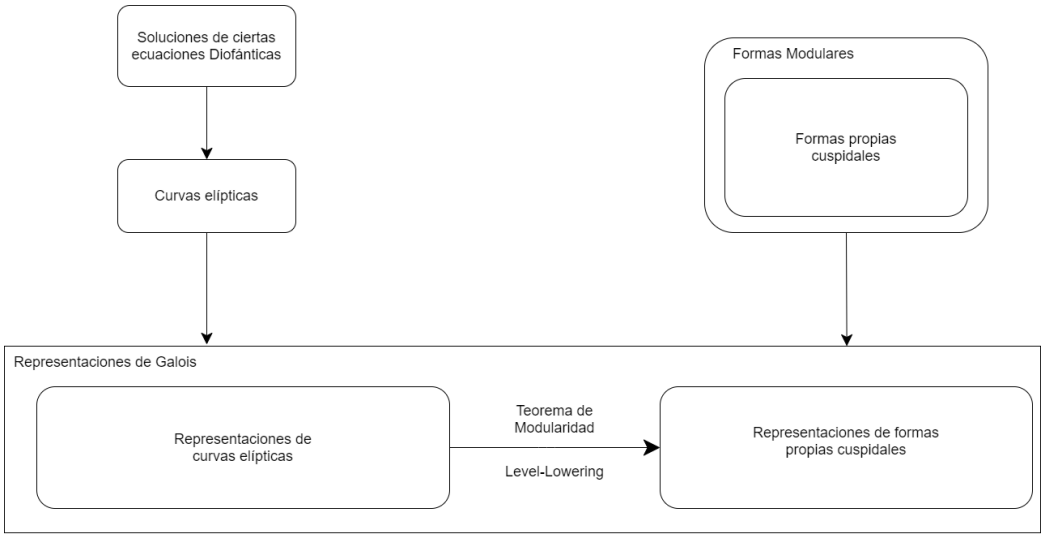
También en el siglo XX, se encontró una forma de asociar representaciones de Galois a formas propias cuspidales, dando idea de que se podía "comparar" curvas elípticas y formas modulares a través de sus representaciones de Galois.

Pero la conexión fundamental la dieron Yutaka Taniyama y Goro Shimira en 1957 cuando conjeturaron que a cada curva elíptica se le podía corresponder una forma propia cuspidal y Jean Pierre Serre cuando conjeturó que las representaciones de Galois de cada objeto debían ser iguales. Dado que se conocía el espacio de formas propias cuspidales, un resultado de este estilo, acotaba las opciones de curvas elípticas que podían existir. El problema, es que en esta conjetura, se indicaba que la forma modular debía ser de peso 2 y que el carácter era 1, pero no se indicaba de que nivel debía ser la forma propia cuspidal.

En 1990, Keneth Ribet, complementó las Conjeturas demostrando un teorema de "Level-Lowering" (ver [39]). Este teorema, enuncia que si una curva elíptica es modular para algún nivel, entonces se puede bajar el nivel según algunas propiedades de la curva elíptica. Esto permitía en muchos casos, conocer en que espacio de formas propias cuspidales se debía buscar.

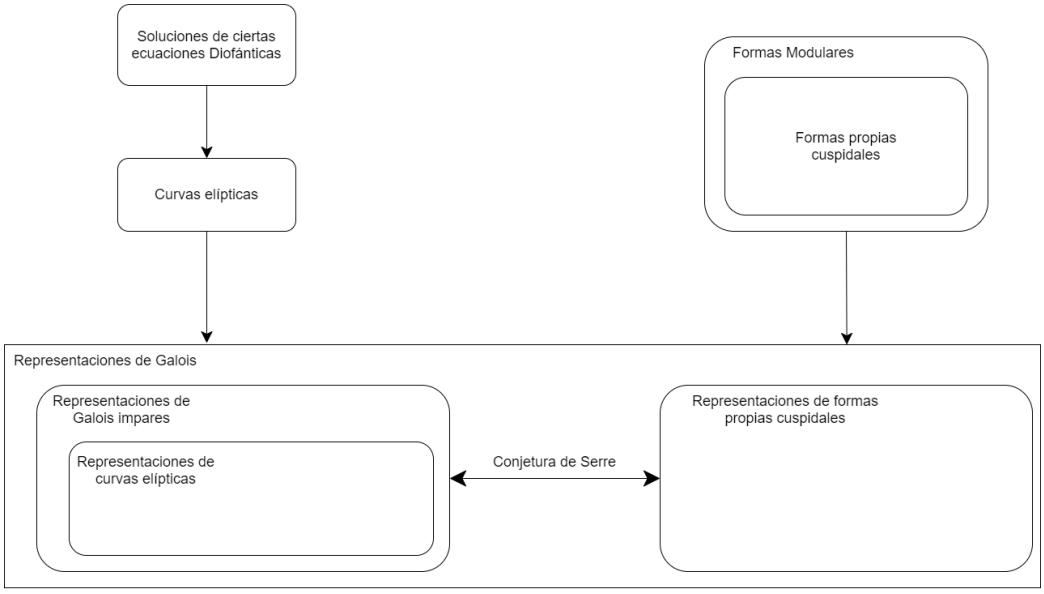
En 1995, Andrew Wiles demostró parcialmente la Conjetura de Taniyama-Shimura (ver [51] y [49]) y finalmente Brian Conrad, Fred Diamond, Richard Taylor y Christopher Breuli en 2001, la demostraron totalmente, dando paso al teorema de Modularidad (ver [4]).

El esquema resultante es el siguiente:



Con el afán de generalizar los resultados de Modularidad y Level-Lowering para cualquier tipo de representación de Galois y no sólo las que provienen de curvas elípticas, en 1987, Jean Pierre Serre conjeturó que todas las representaciones de Galois impares e irreducibles eran iguales a una representación de Galois que provenía de una forma propia cuspidal (ver [43]). Las representaciones de Galois impares incluía por supuesto, a las representaciones de Galois que provenían de curvas elípticas. Lo que era aún más interesante, es que en la Conjetura de Serre se daba una forma de calcular el peso, el nivel y el carácter en el que debía buscarse la forma propia cuspidal, en función de la representación de Galois.

El diagrama final es el siguiente:



La Conjetura de Serre fue demostrada en 2009 por los trabajos de Chandrashekhar Khare y Jean-Pierre Wintenberger (ver [20], [21] y [22]).

En la seccion 5.3 daremos una demostración detallada del Último Teorema de Fermat utilizando la Conjetura de Serre, pero veamos ahora un esquema de la prueba utilizando los objetos mencionados:

Supongamos que $n = \ell \geq 5$ primo y que (a, b, c) es una solución no trivial de la ecuación 0.1.

Consideremos la curva elíptica

$$E : y^2 = x(x + a^n)(x - b^n)$$

que es conocida como la curva elíptica de Frey. Según lo anterior, podemos asociar a esta curva elíptica una representación de Galois si estudiamos su ℓ-torsión.

Estudiando las propiedades de la representación de Galois de esta curva elíptica de Frey, la Conjetura de Serre establece que debe ser igual a una representación de Galois de una forma propia cuspidal de peso 2, nivel 2 y carácter 1. Dado que es conocido que el espacio de formas propias cuspidales de peso 2, nivel 2 y carácter 1 es trivial, concluimos que tal curva no existe, dando paso a la demostración.

Esta estrategia de demostración, sigue siendo poderosa incluso si el espacio de formas propias cuspidales al que se asocia nuestro problema es no trivial, puesto que nos da información de la curva elíptica y de sus puntos. El teorema de modularidad y el teorema de Level-Lowering no sólo son útiles para dar resultados de no existencia de soluciones.

En la sección 5.4 veremos cómo usar la Conjetura de Serre para clasificar todas las curvas elípticas de conductor primo sobre $\mathbb{Q}$.

Lo siguiente sería buscar resultados análogos para cuerpos más grandes que $\mathbb{Q}$. Es por eso, que en el capítulo 6 estudiamos las curvas elípticas sobre cuerpos cuadráticos reales con conductor potencia de un primo. Como se verá, las estrategias son las mismas. Utilizar la existencia de un teorema de modularidad y un teorema de Level-Lowering en cuerpos cuadráticos reales para acotar las opciones de curvas elípticas en los cuerpos que estudiamos.

Esta página ha sido intencionalmente dejada en blanco.

Capítulo 1

Conceptos básicos de TNA

A partir de ahora y para todo el documento, fijemos una clausura algebraica $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ y para cada primo ℓ fijemos clausuras algebraicas $\overline{\mathbb{Q}_\ell}$. Fijemos también inmersiones $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_\ell} \hookrightarrow \mathbb{C}$.

Como era mencionado en el Prefacio, asumiremos que el lector conoce resultados de Teoría de Números Algebraica (TNA). Sin embargo, si no tiene los conocimientos o quiere repasarlos antes de empezar, recomendamos los capítulos 2 y 3 de [30]. Si desea repasar sobre cuerpos locales puede leer el capítulo 7 de [30], aunque en este capítulo introduciremos brevemente ideas de cuerpos locales.

Finalmente, asumiremos que el lector conoce el automorfismo de Frobenius y sus levantados. Para más información sobre el mismo y sus propiedades recomendamos la lectura de "The Frobenius element" en el capítulo 8 de [30].

1.1. Extensiones no ramificadas y moderadas

Sea K cuerpo de números, $\mathcal{O}_K$ su anillo de enteros y $\mathfrak{l}$ un ideal primo de $\mathcal{O}_K$ sobre un primo ℓ de $\mathbb{Q}$. Definimos la valuación

$$\nu_\mathfrak{l} : K^\times \to \mathbb{Z} : \ \ \nu_\ell(x) = \text{máx}\left\{k \in \mathbb{Z} : x \in \mathfrak{l}^k\right\}.$$

Veamos que está bien definida. En efecto, si $x \in K$, el ideal $x\mathcal{O}_K$ tiene factorización única en ideales primos como ideal fraccional (ver Teorema 3.7 de [30]), y el exponente que le corresponda a $\mathfrak{l}$ en esa factorización será el valor de $\nu_\mathfrak{l}$. La valuación $\nu_\mathfrak{l}$ se extiende a K definiendo $\nu_\mathfrak{l}(0) = \infty$.

Algunas propiedades de $\nu_\mathfrak{l}$ son (ver proposición 7, cáp. 1 de [42].):

1. $\nu_\mathfrak{l}(xy) = \nu_\mathfrak{l}(x) + \nu_\mathfrak{l}(y)$ para todo $x, y \in K$

2. $\nu_{\mathfrak{l}}(x+y) \geq \min\{\nu_{\mathfrak{l}}(x), \nu_{\mathfrak{l}}(y)\}$ para todo $x, y \in K$. De hecho vale la igualdad si $\nu_{\mathfrak{l}}(x) \neq \nu_{\mathfrak{l}}(y)$

Definamos $R = \{x \in K : \nu_{\mathfrak{l}}(x) \geq 0\}$. No es difícil chequear con las propiedades anteriores que R es un anillo. Más aún, $\mathfrak{M} = \{x \in K : \nu_{\mathfrak{l}}(x) > 0\}$ es un ideal y como su complemento es el conjunto de unidades de R, entonces R es un anillo local con $\mathfrak{M}$ como ideal maximal. También es interesante mencionar que $\mathcal{O}_K \subseteq R$ puesto que la descomposición en ideales primos de $x\mathcal{O}_K$ tiene exponentes no negativos.

Sea $k = R/\mathfrak{M}$. A k lo llamaremos el **cuerpo residual de** K. Como $\mathfrak{l} \mid \ell$ en R, entonces $\ell \in \mathfrak{M}$ y por lo tanto $\mathrm{char}(k) = \ell > 0$. Además, k es un cuerpo finito, puesto que la extensión de anillo $\mathcal{O}_K/\mathbb{Z}$ tiene finitos generadores por ser K un cuerpo de números y esos generadores son generadores de la extensión $k/\mathbb{F}_\ell$.

Definición **1.1.** *Denominamos* ***uniformizador*** *a un elemento de R con valuación positiva mínima.*

Es claro que con la definición anterior, el uniformizador es un elemento de $\nu_{\mathfrak{l}}^{-1}(1)$. También, si $\mathfrak{l}$ es principal, entonces su generador es un uniformizador. Llamemos π a un uniformizador de $\nu_{\mathfrak{l}}$ de ahora en adelante. Se cumple (ver Proposición 7.6 de [30]) que $\mathfrak{M} = \pi R$.

La valuación $\nu_{\mathfrak{l}}$ permite definir un valor absoluto no arquimediano discreto[1] a través de la fórmula

$$|x|_{\mathfrak{l}} = N(\mathfrak{l})^{-\nu_{\mathfrak{l}}(x)} \tag{1.1}$$

siendo $N(\mathfrak{l}) = \#k$ la norma del ideal.

Llamaremos $K_{\mathfrak{l}}$ a la completación de K con respecto a $|.|_\ell$ definida anteriormente. Observar que $|.|_\ell$ y $\nu_{\mathfrak{l}}$ se pueden extender a $K_{\mathfrak{l}}$ simplemente como

$$\lim_{n\to\infty} \nu_{\mathfrak{l}}(x_n) = \nu_{\mathfrak{l}}(\lim_{n\to\infty} x_n)$$

$$\lim_{n\to\infty} |x_n|_{\mathfrak{l}} = \left|\lim_{n\to\infty} x_n\right|_{\mathfrak{l}}$$

para cualquier sucesión de Cauchy.

Como la imagen de $\nu_{\mathfrak{l}}$ en K es $\mathbb{Z}$, esto seguirá ocurriendo en $K_{\mathfrak{l}}$ debido a la definición anterior, por lo que π sigue siendo uniformizador en $K_{\mathfrak{l}}$.

Nos preocupamos ahora de algunas propiedades sobre extensiones de $K_{\mathfrak{l}}$:

[1] Un valor absoluto es no arquimediano o cumple la condición ultramétrica si $|x+y| \leq \max\{|x|, |y|\}$ para todo $x, y \in K$. Es discreto porque $\mathrm{Im}(\nu_{\mathfrak{l}}) = \mathbb{Z}$ es un conjunto discreto.

Teorema **1.2.** *Sea $L/K_\mathfrak{l}$ una extensión algebraica (separable) finita, entonces existe un único valor absoluto no arquimediano discreto $|.|_L$ de L que extiende a $|.|_{K_\mathfrak{l}}$. Además L es completo con respecto a $|.|_L$ y para todo $x \in L$,*

$$|x|_L = \left|N_{L/K_\mathfrak{l}}(x)\right|_\mathfrak{l}^{\frac{1}{[L:K_\mathfrak{l}]}} \tag{1.2}$$

o en términos de valuaciones, existe una única valuación ν_L tal que

$$\nu_L(x) = \frac{1}{f(L/K_\mathfrak{l})}\,\nu_\mathfrak{l}(N_{L/K_\mathfrak{l}}(x)) \tag{1.3}$$

siendo $f(L/K_\mathfrak{l}) = [k_L : k]$. Llamaremos ***valuación normalizada*** *a la valuación anterior.*

Demostración. Ver Teorema 7.38, cáp. 7 de [30]. □

Como se observa en la ecuación (1.3), L sigue teniendo una valuación discreta y de hecho su imagen es $\mathbb{Z}$. Observar también que la ecuación (1.2) es compatible en extensiones, es decir si uno tiene $x \in L$ y F/L es una extensión finita, entonces $|x|_F = |x|_L$. Esto permite extender el valor absoluto de forma única a $\overline{K_\mathfrak{l}}$ la clausura algebraica de $K_\mathfrak{l}$. La valuación resultante sin embargo, no es discreta (ver Remark 7.7 en [30]).

De forma análoga a lo hecho en K, podemos definir R_L, $\mathfrak{M}_L$ y k_L.

Definición **1.3.** *Sea $L/K_\mathfrak{l}$ una extensión algebraica (separable) finita, ν_L la valuación normalizada que extiende a $\nu_\mathfrak{l}$ y π el uniformizador de K. Definimos el* ***índice de ramificación*** *como $e(L/K_\mathfrak{l}) = \nu_L(\pi)$ y el* ***grado de ramificación*** *$f(L/K_\mathfrak{l})$ como el grado de la extensión de los cuerpos residuales k_L/k.*

Se cumple también que $[L : K_\mathfrak{l}] = e(L/K_\mathfrak{l})f(L/K_\mathfrak{l})$ (ver Corolario 7.42 de [30]).

Definición **1.4.** *Una extensión finita $L/K_\mathfrak{l}$ se dice* ***no ramificada*** *si $e(L/K_\mathfrak{l}) = 1$.*

Observar que si la extensión $L/K_\mathfrak{l}$ es no ramificada, entonces π sigue siendo uniformizador en L.

Teorema **1.5.** *Si $L_1/K_\mathfrak{l}$ y $L_2/K_\mathfrak{l}$ son dos extensiones no ramificadas, entonces $L_1L_2/K_\mathfrak{l}$ es no ramificada. En particular, si $L/K_\mathfrak{l}$ es no ramificada y F es la clausura de Galois de L entonces, $F/K_\mathfrak{l}$ es no ramificada.*

Demostración. Ver proposición 8 capítulo 2, pág. 49 de [25]. □

El Teorema 1.5 junto con el Corolario 1, cap 3, pág. 54 de [42], nos permite construir una extensión no ramificada maximal $K_\mathfrak{l}^{nr}$ como la unión de todas las extensiones finitas no ramificadas de $K_\mathfrak{l}$, donde además $K_\mathfrak{l}^{nr}/K_\mathfrak{l}$ es una extensión Galois y $\mathrm{Gal}(K_\mathfrak{l}^{nr}/K_\mathfrak{l}) \simeq \mathrm{Gal}(\overline{\mathbb{F}_\ell}/k)$ siendo $\overline{\mathbb{F}_\ell}$ una clausura algebraica de k.

De forma muy similar:

Definición **1.6.** *Una extensión $L/K_{\mathfrak{l}}$ finita es* ***moderada*** *si $e(L/K_{\mathfrak{l}})$ es coprimo a* $\mathrm{char}(k) = \ell$.

Teorema **1.7.** *Si $L_1/K_{\mathfrak{l}}$ y $L_2/K_{\mathfrak{l}}$ son dos extensiones moderadas, entonces $L_1L_2/K_{\mathfrak{l}}$ es moderada. En particular, si $L/K_{\mathfrak{l}}$ es moderada y F es la clausura de Galois de L entonces, $F/K_{\mathfrak{l}}$ es moderada.*

Demostración. Ver proposición 13 capítulo 2, pág. 54 de [25]. □

Al igual que con $K_{\mathfrak{l}}^{nr}$ construimos una extensión maximal como la unión de todas las extensiones moderadas y llamaremos $K_{\mathfrak{l}}^{t}$ a ese cuerpo. A partir de las definiciones 1.4 y 1.6 no es difícil ver que $K_{\mathfrak{l}}^{nr} \subseteq K_{\mathfrak{l}}^{t}$.

Definición **1.8.** *Denotaremos $I_{\mathfrak{l}} = \mathrm{Gal}(\overline{K_{\mathfrak{l}}}/K_{\mathfrak{l}}^{nr})$ y lo llamaremos* ***grupo de inercia de*** $\mathfrak{l}$ *y $P_{\mathfrak{l}} = \mathrm{Gal}(\overline{K_{\mathfrak{l}}}/K_{\mathfrak{l}}^{t})$ y lo llamaremos* ***grupo de inercia salvaje de*** $\mathfrak{l}$.

Teorema **1.9.** *$P_{\mathfrak{l}}$ es el pro-ℓ-subgrupo maximal de $I_{\mathfrak{l}}$ (ver definiciones en nota al pie[2]) .*

Demostración. De la definición de ser una extensión moderada, es claro que $P_{\mathfrak{l}} \leq I_{\mathfrak{l}}$.

Por otro lado,

$$P_{\mathfrak{l}} = \varprojlim \mathrm{Gal}(L/K^{t})$$

con $L/K_{\mathfrak{l}}^{t}$ extensión finita Galois.

Sea $[L : K_{\mathfrak{l}}^{t}] = e(L/K_{\mathfrak{l}}^{t})f(L/K_{\mathfrak{l}}^{t})$. Para empezar, $f(L/K_{\mathfrak{l}}^{t}) = 1$ pues $K_{\mathfrak{l}}^{t}$ contiene a $K_{\mathfrak{l}}^{nr}$ y $k^{nr} = \overline{\mathbb{F}_{\ell}}$, por lo que no se puede extender más allá.

Ahora, supongamos que $[L : K_{\mathfrak{l}}^{t}] = \ell^{r}m$ con $m > 1$ y coprimo a ℓ y consideremos, H el ℓ-Sylow de $\mathrm{Gal}(L/K_{\mathfrak{l}}^{t})$ y $F = L^{H}$ el cuerpo dentro de L fijo por acción de H. Entonces tenemos la torre de cuerpos $L/F/K_{\mathfrak{l}}^{t}$ y $e(F/K_{\mathfrak{l}}^{t}) \mid m$ que es coprimo con ℓ. Entonces $F/K_{\mathfrak{l}}^{t}$ es una extensión moderada, lo que contradice la maximalidad de $K_{\mathfrak{l}}^{t}$.

Para probar que $P_{\mathfrak{l}}$ es maximal entre los pro-ℓ-subgrupos de $I_{\mathfrak{l}}$, supongamos que existe $\sigma \in I_{\mathfrak{l}} \setminus P_{\mathfrak{l}}$ tal que $\sigma^{\ell^{k}} = \mathrm{id}$ para algún $k > 1$. Llamemos $H = \langle P_{\mathfrak{l}}, \sigma \rangle$ y consideremos $F = (\overline{K})^{H}$. Entonces $H/P_{\mathfrak{l}} = \mathrm{Gal}(K_{\mathfrak{l}}^{t}/F)$ es un grupo finito de orden potencia de ℓ. Pongamos que $|H/P_{\mathfrak{l}}| = \ell^{r} = d$.

Como $K_{\mathfrak{l}}^{t}/F$ es una extensión finita, por el teorema de la raíz primitiva, existe $\alpha \in K_{\mathfrak{l}}^{t}$ tal que $K_{\mathfrak{l}}^{t} = F(\alpha)$. Sea $m_{\alpha} \in F[x]$ el polinomio irreducible de α sobre

[2]Esto es, si escribimos a $P_{\mathfrak{l}}$ como un límite inverso de grupos finitos, cada uno de ellos es un ℓ-grupo. Recordar que un ℓ-grupo H es un grupo para el cual todo elemento tiene orden una potencia de ℓ. El hecho de que sea maximal implica que si g es un elemento de orden potencia de ℓ, entonces $g \in H$.

F. Entonces, $m_\alpha(x) = \sum_{i=0}^{d} a_i x^i$ donde los a_i son algebraicos por estar contenidos en $\overline{K_\mathfrak{l}}$. Consideremos $L = K_\mathfrak{l}^{nr}(a_0, ..., a_d)$. Como los coeficientes son algebraicos, la extensión es finita de grado n. El diagrama de extensiones queda como se muestra en la figura 1.1.

$$\begin{tikzcd}
 & K_\mathfrak{l}^t = F(\alpha) \arrow[dl, dash, "\ell^r"'] \arrow[dr, dash] & \\
F \arrow[dr, dash] \arrow[ddr, dash] & & L(\alpha) \arrow[dl, dash, "\ell^r"] \arrow[ddl, dash, "n\ell^r"] \\
 & L \arrow[d, dash, "n"] & \\
 & K_\mathfrak{l}^{nr} &
\end{tikzcd}$$

Figura 1.1: Diagrama para la demostración del Teorema 1.9

Como estamos con cuerpos que contienen a $K_\mathfrak{l}^{nr}$, el grado de inercia es 1 en todas las extensiones, y en particular $e(L(\alpha)/K^{nr}) = n\ell^r$ lo que implica que $L(\alpha)/K_\mathfrak{l}^{nr}$ no es moderada, contradiciendo el hecho de que $L(\alpha) \subseteq K_\mathfrak{l}^t$ [3]. □

Teorema **1.10.** *Sea $\mathfrak{l}$ ideal primo de $\mathcal{O}_K$. Entonces:*

1. $I_\mathfrak{l} \lhd G_{K_\mathfrak{l}}$,
2. $P_\mathfrak{l} \lhd I_\mathfrak{l}$,
3. $P_\mathfrak{l} \lhd G_{K_\mathfrak{l}}$.

donde $G_{K_\mathfrak{l}} = \mathrm{Gal}(\overline{K_\mathfrak{l}}/K_\mathfrak{l})$

Demostración. 1. Es porque $K_\mathfrak{l}^{nr}/K_\mathfrak{l}$ es una extensión Galois.

2. Es una consecuencia de 3.

3. Podemos ver que es normal demostrando que la extensión $K_\mathfrak{l}^t/K_\mathfrak{l}$ es normal, es decir, que para todo $x \in K_\mathfrak{l}^t$ y $\sigma \in G_{K_\mathfrak{l}}$, entonces $\sigma(x) \in K_\mathfrak{l}^t$. Tomemos entonces $x \in K_\mathfrak{l}^t$ y sea F la clausura de Galois del cuerpo $K(x)$. Como $x \in K_\mathfrak{l}^t$, entonces $K(x)/K$ es moderado, así que por el Teorema 1.7 también lo es F/K y por lo tanto $\sigma(x) \in F \subseteq K_\mathfrak{l}^t$. □

[3] Se construyen todos estos cuerpos porque lo que se necesita es un cuerpo que sea una extensión finita de $K_\mathfrak{l}^{nr}$ y F no lo es. El cuerpo $L(\alpha)$ tiene lo importante para la prueba, que es que el grado de extensión es divisible por ℓ.

En particular, usando la teoría de correspondencia de Galois, $K_{\mathfrak{l}}^t/K_{\mathfrak{l}}$ es una extensión Galois. La torre de cuerpos asociada es la siguiente:

$$\begin{array}{c}
\overline{K_{\mathfrak{l}}} \\
\Big| \; P_{\mathfrak{l}} \\
K_{\mathfrak{l}}^t \\
\Big| \; I_{\mathfrak{l}}/P_{\mathfrak{l}} \\
K_{\mathfrak{l}}^{nr} \\
\Big| \; G_{K_{\mathfrak{l}}}/I_{\mathfrak{l}} \\
K_{\mathfrak{l}}
\end{array}$$

1.1.1. Construcción de $K_{\mathfrak{l}}^t$ como límite directo

Sea $\pi \in K_{\mathfrak{l}}^{nr}$ uniformizador (se puede tomar el uniformizador de K porque la extensión es no ramificada, ver párrafo posterior a la definición 1.4), $d \in \mathbb{N}$ coprimo con ℓ y definamos $K_d = K_{\mathfrak{l}}^{nr}(\pi^{1/d})$. Como π es un uniformizador, $\pi^{1/d}$ tiene valuación menor, así que $\pi^{1/d} \notin K_{\mathfrak{l}}^{nr}$. Por definición de $K_{\mathfrak{l}}^{nr}$, $K_d/K_{\mathfrak{l}}^{nr}$ es totalmente ramificada, y además es claro que las raíces del polinomio $x^d - \pi$, que es irreducible por el criterio de Eisenstein (ver proposición 3.53 de [30]) son de la forma $\xi_d^k \pi^{1/d}$ con $k = 0, ..., d-1$ donde ξ_d es una raíz primitiva d-ésima de la unidad. Al ser d coprimo con ℓ, entonces $\xi_d \in K_{\mathfrak{l}}^{nr}$ y por ende todas las raíces de ese polinomio están en K_d. Esto nos permite concluir que esa extensión es Galois y de grado d.

Como los automorfismos de $\mathrm{Gal}(K_d/K_{\mathfrak{l}}^{nr})$ preservan las raíces de $x^d - \pi$, tenemos un morfismo $\theta_d : \mathrm{Gal}(K_d/K_{\mathfrak{l}}^{nr}) \to \mu_d$ tal que

$$\sigma(\pi^{1/d}) = \theta_d(\sigma)\pi^{1/d}$$

donde μ_d es el grupo de las raíces d-ésimas de la unidad. Es claro que es inyectivo y como $\mathrm{Gal}(K_d/K_{\mathfrak{l}}^{nr})$ y μ_d tienen el mismo cardinal, entonces θ_d es un isomorfismo.

Teorema **1.11.**

$$K_{\mathfrak{l}}^t = \bigcup_{d:\gcd(d,\ell)=1} K_d$$

Demostración. Lo primero es observar que $K_\mathfrak{l}^t = (K_\mathfrak{l}^{nr})^t$. Esto prueba que $K_d \subseteq K_\mathfrak{l}^t$ puesto que $[K_d : K_\mathfrak{l}^{nr}]$ es coprimo con ℓ.

Para la otra inclusión, hay que usar la Proposición 12, página 52 de [25] que establece (los nombres de las variables fueron modificados):

> Si E es una extensión totalmente ramificada y moderada sobre un cuerpo F, entonces existe un uniformizador π_E que satisface una ecuación
>
> $$x^d - \pi' = 0$$
>
> con π' un uniformizador de F.

De esta forma, si E es una extensión finita de $K_\mathfrak{l}^{nr}$, tenemos que $E = K_\mathfrak{l}(\pi'^{1/d})$ por la proposición mencionada. Como π y π' son ambos uniformizadores de $K_\mathfrak{l}^{nr}$, tenemos que $\pi' = \pi/u$ con $u \in R^\times_{K_\mathfrak{l}^{nr}}$ y entonces $x^d - \pi' = \frac{1}{u}(ux^d - \pi)$. Como $u \in R^\times_{K_\mathfrak{l}^{nr}}$, entonces existe $s \in K_\mathfrak{l}^{nr}$ tal que $s^d = u$, y entonces $ux^d - \pi = (sx)^d - \pi = y^d - pi$ tomando el cambio de variable $y = sx$. De esta forma, obtenemos que $E = K_\mathfrak{l}(\pi'^{1/d}) = K_d$. □

El siguiente resultado nos será útil en la sección 5.2.

Teorema **1.12.** *Sea s una preimagen del automorfismo de Frobenius en $G_{K_\mathfrak{l}}$ y sea $\sigma \in I_\mathfrak{l}$, entonces $s\sigma s^{-1} \equiv \sigma^\ell \mod P_\mathfrak{l}$*

Demostración. Lo primero es observar que dos morfismos de Galois σ_1, σ_2 cumplen que $\sigma_1 \equiv \sigma_2 \pmod{P_\mathfrak{l}}$ sí y solo sí $\sigma_1\sigma_2^{-1} \in P_\mathfrak{l}$ y esto sí y solo sí $\sigma_1\sigma_2^{-1}$ fija $K_\mathfrak{l}^t$, que es lo mismo que $\sigma_1 |_{K_\mathfrak{l}^t} = \sigma_2 |_{K_\mathfrak{l}^t}$.

Observar que como $\sigma \in I_\mathfrak{l}$, su acción es trivial en $K_\mathfrak{l}^{nr}$ y entonces

$$s\sigma s^{-1} |_{K_\mathfrak{l}^{nr}} = \mathrm{id} = \sigma^\ell |_{K_\mathfrak{l}^{nr}}, \tag{1.4}$$

por lo que podemos trabajar desde la extensión $K_\mathfrak{l}^t/K_\mathfrak{l}^{nr}$. Tenemos de hecho dos simplificaciones más. La primera, es que por el Teorema 1.11, basta con probar la ecuación (1.4) para cada elemento de $x \in K_d$, y la segunda es que $K_d = K_\mathfrak{l}^{nr}(\pi^{1/d})$, por lo que alcanza con probar la ecuación (1.4) para $\pi^{1/d}$ con $\gcd(d, \ell) = 1$.

Como $\pi^{1/d}$ es una raíz de $x^d - \pi$, entonces $\sigma(\pi^{1/d}) = \xi_d^r \pi^{1/d}$ para algún $r \in \mathbb{Z}$ y lo mismo ocurre con s, teniendo que $s(\pi^{1/d}) = \xi_d^u \pi^{1/d}$ para algún $u \in \mathbb{Z}$, siendo ξ_d una raíz d-ésima de la unidad. Como $\xi_d \in K_\mathfrak{l}^{nr}$ y $\sigma \in I_\ell$ entonces $\sigma(\xi_d) = \xi_d$. Para s, tenemos que $s(\xi_d)$ es otra raíz d-ésima de la unidad. Dado que s es una preimagen del mapa de Frobenius, $s(\xi_d) = \xi_d^\ell \pmod{\pi^{1/d}}$. Como $\gcd(d, \ell) = 1$, las raíces d-ésimas de la unidad son todas distintas módulo $\pi^{1/d}$ y necesariamente $s(\xi_d) = \xi_d^\ell$.

Entonces
$$s\sigma(\pi^{1/d}) = s(\xi_d^r \pi^{1/d}) = \xi_d^{\ell r+u}\pi^{1/d}.$$
Por otro lado,
$$\begin{aligned}\sigma^\ell s(\pi^{1/d}) = \sigma^\ell(\xi_d^u \pi^{1/d}) = \xi_d^u \sigma^\ell(\pi^{1/d}) = \xi_d^u \sigma^{\ell-1}(\sigma(\pi^{1/d})) = \xi_d^u \sigma^{\ell-1}(\xi_d^r \pi^{1/d}) \\ = \xi_d^u \xi_d^r \sigma^{\ell-1}(\pi^{1/d}) = ... = \xi_d^{u+\ell r}\pi^{1/d}\end{aligned}$$

obteniendo la igualdad. □

Definición **1.13.** *Definimos* $I_{\mathfrak{l},t} = I_{\mathfrak{l}}/P_{\mathfrak{l}}$ *el* ***grupo de inercia moderado de*** $\mathfrak{l}$.

De la correspondencia de Galois y del Teorema 1.11, obtenemos que
$$I_{\mathfrak{l},t} = \mathrm{Gal}(K_{\mathfrak{l}}^t/K_{\mathfrak{l}}^{nr}) \simeq \varprojlim \mathrm{Gal}(K_d/K_{\mathfrak{l}}^{nr}) \simeq \varprojlim \mu_d \tag{1.5}$$
donde $\gcd(d,\ell) = 1$ y el isomorfismo es dado por la compatibilidad de los mapas θ_d.

Teorema **1.14.** *Sea* K *cuerpo de números y* $\mathfrak{l}$ *ideal primo de* $\mathcal{O}_K$. *Entonces*
$$I_{\mathfrak{l},t} \simeq \varprojlim \mathbb{F}_q^\times$$
con $q = \ell^r$ *y* $r \in \mathbb{Z}_{>0}$

Demostración. Demostremos que
$$\varprojlim \mu_d = \varprojlim \mathbb{F}_q^\times.$$

Para ello ahondemos más en sus construcciones. El grupo
$$\mu_d = \left\{ g_d^k : k = 0, ..., d-1 \right\}$$
donde g_d tiene orden d. Si consideramos el orden parcial, $d < d' \Leftrightarrow d \mid d'$ y los mapas $\phi_{d'd} : \mu_{d'} \to \mu_d$ dados por $g_{d'}^k \mapsto g_d^k$ tenemos un sistema inverso. Para el otro, tomamos el orden parcial $\ell^m < \ell^n \Leftrightarrow m \mid n$ y los mapas $\varphi_{mn} : \mathbb{F}_{\ell^n}^\times \to \mathbb{F}_{\ell^m}^\times$ dados por $x \mapsto N_{\mathbb{F}_{\ell^n}/\mathbb{F}_{\ell^m}}(x)$ siendo $N_{\mathbb{F}_{\ell^n}/\mathbb{F}_{\ell^m}}$ la norma relativa de una extensión a otra.

Dado ℓ^n, tenemos que $\mu_{\ell^n-1} \simeq \mathbb{F}_{\ell^n}^\times$ y dado d entero positivo, tenemos que $d \mid (\ell^n)^{\varphi(d)} - 1$ por el Teorema de Euler. Tomando $d' = (\ell^n)^{\varphi(d)} - 1$, entonces $\mu_{d'} \simeq \mathbb{F}_{(\ell^n)^{\varphi(d)}}^\times$ y $\mu_d \subseteq \mu_{d'}$. □

1.2. Grupos de Ramificación

Como antes, sea K un cuerpo de números, sea $\mathfrak{p}$ un ideal primo de K arriba de un primo racional p y consideremos $K_\mathfrak{p}$ la completación de K como en la sección 1.1. Para hacer una definición general de los grupos de ramificación, es necesario primero definir el caso de extensiones finitas:

Definición **1.15.** *Sea $L/K_\mathfrak{p}$ extensión Galois, separable y finita, $G = \mathrm{Gal}(L/K_\mathfrak{p})$, ν_L la valuación normalizada de L y $w \in [-1, +\infty)$. Definimos*

$$G_w = \{\sigma \in \mathrm{Gal}(L/K_\mathfrak{p}) : \nu_L(\sigma(x) - x) \geq w + 1 \ \ \forall x \in R_L\}.$$

En el lema 1, cáp. 4, pág. 61 de [42], se prueba que si π_L es el uniformizador, entonces

$$G_w = \{\sigma \in \mathrm{Gal}(L/K_\mathfrak{p}) : \nu_L(\sigma(\pi_L) - \pi_L) \geq w + 1\}$$

Teorema **1.16.** *Sea $L/K_\mathfrak{p}$ extensión Galois, separable y finita, $G = \mathrm{Gal}(L/K_\mathfrak{p})$ y G_w los grupos definidos previamente. Entonces:*

1. *Si $w \leq w'$ entonces $G_w \supseteq G_{w'}$,*
2. *$G_w = G_{\lceil w \rceil}$, donde $\lceil w \rceil$ es la función techo*[4]
3. *$G_{-1} = \mathrm{Gal}(L/K_\mathfrak{p})$,*
4. *$G_0 = I_\mathfrak{p}/(I_\mathfrak{p} \cap \mathrm{Gal}(\overline{K_\mathfrak{p}}/L))$. En otras palabras G_0 es la inercia restricta a la extensión $L/K_\mathfrak{p}$.*
5. *G_0/G_1 es isomorfo a un subgrupo de $\mathbb{F}_\mathfrak{P}^\times$ siendo $\mathfrak{P}$ el primo sobre $\mathfrak{p}$ en R_L.*
6. *G_k/G_{k+1} para k entero positivo es isomorfo a un subgrupo de $\mathbb{F}_\mathfrak{P}$ siendo $\mathfrak{P}$ el primo sobre $\mathfrak{p}$ en R_L.*
7. *$G_1 = P_\mathfrak{p}/(P_\mathfrak{p} \cap \mathrm{Gal}(\overline{K_\mathfrak{p}}/L))$. En otras palabras G_1 es la inercia moderada restricta a la extensión $L/K_\mathfrak{p}$,*
8. *$G_w \lhd G$ para todo w.*

Demostración. 1, 2 y 3 son fáciles de chequear con la definición. Para 4, de teoría de números algebraica, tenemos que el grupo de inercia en una extenión finita son los $\sigma \in \mathrm{Gal}(L/K_\mathfrak{p})$ tales que $\sigma(x) \equiv x \pmod{\mathfrak{P}}$ para todo $x \in R_L$, que es equivalente a que $\nu_L(\sigma(x) - x) \geq 1$.

[4] La función techo se define como $\lceil w \rceil = \min\{k \in \mathbb{Z} : x \leq k\}$

Para 5 hay que probar que el mapa $G_0 \to \mathbb{F}_{\mathfrak{P}}^{\times}$ dado por

$$\sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L} \pmod{\mathfrak{P}}$$

es un morfismo de grupos con núcleo G_1.

De forma análoga para 6, pero con el mapa $G_k \to \mathbb{F}_{\mathfrak{P}}$ dado por

$$\sigma \mapsto \frac{\sigma(\pi_L) - \pi_L}{\pi_L^{k+1}} \pmod{\mathfrak{P}}$$

viendo que su núcleo es G_{k+1}.

Para 7, basta ver que $p \nmid |G_0/G_1|$ por el punto 5, por lo que G_1 es el p-subgrupo maximal de $\mathrm{Gal}(L/K_{\mathfrak{p}})$ y es entonces la inercia salvaje restringida a $L/K_{\mathfrak{p}}$ por el Teorema 1.9.

Finalmente para 8, sean $\sigma \in G_w$, $\tau \in G$ y $x \in R_L$. Entonces $\nu_L(\tau\sigma\tau^{-1}(x) - x) = \nu_L(\tau(\sigma(y) - y))$ con $y = \tau^{-1}(x)$. Por el Teorema 1.2, ν_L es única, por lo que $\nu_L(\tau(\sigma(y) - y)) = \nu_L(\sigma(y) - y) \geq w + 1$ porque $\sigma \in G_w$ $\square$

Nuestro objetivo es cambiar L por $\overline{K_{\mathfrak{p}}}$. Sin embargo, como mencionábamos posterior al Teorema 1.2, la valuación de $\overline{K_{\mathfrak{p}}}$ no es discreta, y por lo tanto no puede normalizarse. La siguiente idea, sería utilizar límites inversos de grupos de ramificación con extensiones finitas. Sin embargo para que esta idea funcione, necesitamos que haya compatibilidad entre los grupos de ramificación cuando consideramos extensiones relativas. Esto no ocurre con esta numeración de los grupos de ramificación salvo el algunos casos particulares (ver Corolario en pág. 64 y Remark posterior en [42]). Necesitamos entonces hacer una reenumeración:

Definición **1.17.** *Sea $L/K_{\mathfrak{p}}$ extensión separable finita y G_w los grupos de ramificación de la definición 1.15. Definimos la* ***función de Herbrand*** *como $\varphi : [-1, +\infty) \to [-1, +\infty)$ tal que*

$$\varphi(w) = \int_0^w \frac{dt}{[G_0 : G_t]}$$

con la convención de que $[G_0 : G_t] = [G_{-1} : G_0]^{-1}$ cuando $t \in [-1, 0]$.

Como el integrando es una función positiva constante a trozos, entonces φ es un homeomorfismo creciente lineal a trozos.

Definición **1.18.** *Sea $L/K_{\mathfrak{p}}$ extensión separable finita y $G = \mathrm{Gal}(L/K_{\mathfrak{p}})$. Definimos los* ***grupos de ramificación en extensiones finitas*** *(reenumerados) como*

$$G^u = G_{\varphi^{-1}(u)}$$

Desde el punto de vista notacional, escribiremos con supraíndice los grupos de ramificación de la definición 1.18 y con subíndice los de la definición 1.15.

Teorema **1.19.** *Sea $L/K_{\mathfrak{p}}$ extensión separable finita, $G = \mathrm{Gal}(L/K_{\mathfrak{p}})$ y $H \lhd G$. Entonces $(G/H)^u = G^u/(H \cap G^u)$ para todo $u \in [-1, \infty)$*

Demostración. Ver Proposición 14, pág. 74 de [42]. □

Definición **1.20.** *Sea $K_{\mathfrak{p}}$ el completado de K con respecto a $\mathfrak{p}$. Definimos los* ***grupos de ramificación*** *absolutos de K como*

$$I_{\mathfrak{p}}^u = \varprojlim \mathrm{Gal}(L/K_{\mathfrak{p}})^u$$

para $L/K_{\mathfrak{p}}$ extensión finita Galois.

El Teorema 1.19 asegura que los grupos de ramificación conforman un sistema inverso con las extensiones relativas puesto que por Teoría de Galois, si $F/L/K_{\mathfrak{p}}$ es una torre de cuerpos Galois, entonces $\mathrm{Gal}(F/L) \lhd \mathrm{Gal}(L/K_{\mathfrak{p}})$ y

$$\mathrm{Gal}(L/K_{\mathfrak{p}})^u = (\mathrm{Gal}(F/K_{\mathfrak{p}})/\mathrm{Gal}(F/L))^u = \\ \mathrm{Gal}(F/K_{\mathfrak{p}})^u/(\mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/K_{\mathfrak{p}})^u)$$

A partir de ahora, y en lo que queda del documento, cuando nos referimos a los grupos de ramificación, estaremos haciendo referencia a los de la definición 1.20, quedando los otros como un paso intermedio para la definición de los que realmente nos importan.

Teorema **1.21.** *Sea $K_{\mathfrak{p}}$ el completado de de K con respecto a $\mathfrak{p}$ e $I_{\mathfrak{p}}^u$ los grupos de ramificación:*

1. *Si $u \leq v$ entonces $I_{\mathfrak{p}}^u \supseteq I_{\mathfrak{p}}^v$,*
2. *$I_{\mathfrak{p}}^{-1} = G_{K_{\mathfrak{p}}}$,*
3. *$I_{\mathfrak{p}}^u = I_{\mathfrak{p}}$ si $u \in (-1, 0]$,*
4. *$P_{\mathfrak{p}} = \bigcup_{u>0} I_{\mathfrak{p}}^u$,*
5. *$\bigcap_u I_{\mathfrak{p}}^u = \{\mathrm{id}\}$,*
6. *$I_{\mathfrak{p}}^u \lhd G_{K_{\mathfrak{p}}}$ para todo u.*

Demostración. 1 y 2 se obtienen de los puntos 1 y 3 del Teorema 1.16 y del hecho de que la función de Herbrand dada en la definición 1.17 es biyectiva y creciente.

3 se obtiene de los puntos 2 y 4 del Teorema 1.16, del hecho de que para la función de Herbrand $\varphi(0) = 0$ y de que $I_{\mathfrak{p}}$ es el límite inverso de los grupos de

inercia de todas las extensiones Galois finitas de $K_{\mathfrak{p}}$.

4 se obtiene de los puntos 2 y 7 del Teorema 1.16, del hecho de que para la función de Herbrand $\varphi(0) = 0$ y de que $P_{\mathfrak{p}}$ es el límite inverso de los grupos de inercia moderado de todas las extensiones Galois finitas de $K_{\mathfrak{p}}$.

Para 5 basta ver que si $\sigma \in \bigcap_u I_{\mathfrak{p}}^u$, entonces $\nu_L(\sigma(x) - x) \geq w + 1$ para todo $w \geq -1$, $x \in R_L$ y $L/K_{\mathfrak{p}}$ extensión Galois finita. Luego $\sigma(x) - x = 0$ para todo $x \in \overline{K_{\mathfrak{p}}}$ y $\sigma = \mathrm{id}$.

Finalmente 6 se obtiene de 8 del Teorema 1.16. □

1.3. Idèles y grupos de clase

Definición **1.22.** *Sea K un cuerpo de números. Definimos el* ***grupo de idèles*** *como el grupo*

$$\mathbb{I}_K = \left\{ (a_\nu) \in \prod_\nu K_\nu^\times : a_\nu \in R_\nu^\times \text{ salvo una cantidad finita} \right\}$$

donde ν son todas las valuaciones de K (finitas o infinitas), y la operación de grupo es coordenada a coordenada.

El grupo $\mathbb{I}_K$ será un grupo topológico con la topología que tiene como base de abiertos los elementos de la forma $\prod_\nu U_\nu$ donde U_ν es abierto en $K_\nu^\times$ y $U_\nu = R_\nu^\times$ salvo finitos ν. Encajaremos a $K^\times$ en $\mathbb{I}_K$ por la diagonal, es decir $a \mapsto (a, a, ..)$. La factorización única en ideales fraccionales (ver Teorema 3.7 de [30]) asegura que $a \in R_\nu^\times$ salvo una cantidad finita de valuaciones ν. Por abuso de notación, escribiremos también $K^\times$ a la imagen de $K^\times$ por el mapa diagonal. Se puede demostrar (ver 4.2, pág. 166 de [31]) que $K^\times$ es discreto en $\mathbb{I}_K$.

El siguiente resultado será utilizado en el Teorema 6.14 y es el teorema que da sentido a la teoría de cuerpo de clases:

Teorema **1.23.** *(Ley de reciprocidad de Artin) Existe un homomorfismo $\Phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{ab}/K)$ tal que $\Phi_K(K^\times) = 1$, donde K^{ab} es la extensión abeliana maximal, construida como la unión de la extensiones abelianas finitas de K.*

Demostración. Ver Teorema 5.3, cáp. 5, pág. 174 de [31]. □

La teoría de cuerpo de clases, utiliza los idèles para entender las extensiones abelianas de K. En particular, nos va a interesar encontrar las extensiones de K de grado acotado que pueden ramificar en un conjunto finito de lugares S. La siguiente definición ayudará a simplificar la notación:

Definición **1.24.** *Sea K un cuerpo de números. Un* ***modulus*** *es una función $\mathfrak{N}$: $\{$lugares de $K\} \to \mathbb{Z}$ tal que*[5]

- $\mathfrak{N}(\nu_{\mathfrak{p}})$ *es cero salvo en finitos lugares finitos,*
- $\mathfrak{N}(\nu) = 0$ *o* 1 *si ν es un lugar real,*
- $\mathfrak{N}(\nu) = 0$ *si ν es un lugar complejo.*

Un modulus $\mathfrak{N}$ ***divide*** *a un modulus $\mathfrak{N}'$ si $\mathfrak{N}(\nu) \leq \mathfrak{N}'(\nu)$ para todo lugar ν. Un lugar ν divide a un modulus $\mathfrak{N}$, y lo denotaremos $\nu \mid \mathfrak{N}$, si $\mathfrak{N}(\nu) > 0$.*

Esta definición extiende la idea de ideales de $\mathcal{O}_K$ que dividen a ideales de $\mathcal{O}_K$, dando sentido a que lugares en infinito se dividan.

Definición **1.25.** *Sea K cuerpo de números, $\mathfrak{N}$ un modulus de K. Para cada lugar $\nu \mid \mathfrak{N}$, definimos*

$$W_{\mathfrak{N}}(\nu) = \begin{cases} \mathbb{R}_{>0} & \text{si } \nu \text{ real} \\ 1 + \mathfrak{M}_{\nu}^{\mathfrak{N}(\nu)} & \text{si } \nu \text{ finito} \end{cases}.$$

siendo $\mathfrak{M}_\nu$ el ideal maximal que definíamos previo a la definición 1.1, solo que ahora agregamos un subíndice ν, para aclarar el ideal maximal de qué valuación es.

Definimos también

$$\mathbb{I}_{\mathfrak{N}} = \left(\prod_{\nu \nmid \mathfrak{N}} K_\nu^\times \times \prod_{\nu \mid \mathfrak{N}} W_{\mathfrak{N}}(\nu) \right) \bigcap \mathbb{I}_K,$$

el subgrupo

$$W_{\mathfrak{N}} = \prod_{\substack{\nu \nmid \mathfrak{N} \\ \nu \text{ infinito}}} K_\nu^\times \times \prod_{\nu \mid \mathfrak{N}} W_{\mathfrak{N}}(\nu) \times \prod_{\substack{\nu \nmid \mathfrak{N} \\ \nu \text{ finito}}} R_\nu^\times$$

y

$$K_{\mathfrak{N}} = K^\times \cap \mathbb{I}_{\mathfrak{N}}$$

como la restricción del encaje de $K^\times$ a $\mathbb{I}_{\mathfrak{N}}$.

Llamaremos ***ray class group*** *al cociente*

$$C_{\mathfrak{N}}(K) = \mathbb{I}_{\mathfrak{N}} / (K_{\mathfrak{N}} W_{\mathfrak{N}}).$$

La proposición 4.6(a), pág. 168 de [31] junto con el Teorema 1.7, pág. 146 de [31], muestran que $C_{\mathfrak{N}}$ es un grupo finito. Llamaremos $h_{\mathfrak{N}} = \#C_{\mathfrak{N}}$. Más aún, tenemos una correspondencia entre los ray class group y los grupos de Galois de extensiones finitas:

[5] Los lugares son clases de equivalencias de las valuaciones de K. Dos valuaciones son equivalentes si inducen la misma topología.

Teorema **1.26.** *(Corolario de la ley de reciprocidad de Artin) Sea L/K una extensión abeliana finita, S un conjunto finito de lugares que ramifican en L. Entonces, existe un modulus $\mathfrak{N}$ que solo lo dividen lugares de S tal que el mapa*

$$\begin{aligned} \Psi_{L/K} : C_{\mathfrak{N}}(K) &\longrightarrow \mathrm{Gal}(L/K) \\ \nu &\longmapsto \left(\frac{\nu}{L/K}\right) \end{aligned}$$

es sobreyectivo.

Demostración. Ver [2]. □

El mapa $\Psi_{L/K}$ es llamado el **mapa de Artin**.

Nos interesarán también dos ray class group particulares.

Definición **1.27.** *Sea K cuerpo de números. Definimos el* ***grupo de clases*** *como $C(K) = C_{\mathfrak{N}}$ con $\mathfrak{N}(\nu) = 0$ para todo ν lugar de K. Denotaremos $h(K) = \#C(K)$ y lo llamaremos el* ***números de clases****. Definimos también el* ***grupo de clases narrow*** *como $C^+(K) = C_{\mathfrak{N}}$ con $\mathfrak{N}(\nu) = 0$ para todo ν lugar finito de K y $\mathfrak{N}(\nu) = 1$ si ν es real. Denotaremos $h^+(K) = \#C^+(K)$ y lo llamaremos el* ***números de clases narrow****.*

Es claro que $C(K)$ es un cociente de $C^+(K)$, así que $h(K) \mid h^+(K)$. La ley de reciprocidad de Artin (Teorema 1.23), hará corresponder a $C(K)$ con la extensión maximal abeliana no ramificada en ningún lugar de K y a $C^+(K)$ con la extensión maximal abeliana no ramificada en lugares finitos de K.

1.4. Teoría de Kummer

Para finalizar con el repaso, agregamos un teorema que usaremos en varios capítulos de este documento. El teorema en cuestión es debido a Ernst Kummer, que logra clasificar las extensiones cíclicas de un cuerpo que posee todas las raíces de las unidad.

Teorema **1.28.** *Sea n entero positivo, K cuerpo tal que $\mathrm{char}(K) \nmid n$ y K contiene todas las raíces n-ésimas de la unidad. Si L/K es una extensión cíclica de grado n (es decir, $\mathrm{Gal}(L/K)$ es cíclico de orden n), entonces $L = K(b^{1/n})$ para algún $b \in K$.*

Demostración. Ver lema 2, pág. 90 de [1]. □

Capítulo 2

Representaciones de Galois

Las representaciones juegan un rol fundamental en este documento como fue explicado en la introducción, puesto que nos permiten conectar las curvas elípticas y las formas modulares. En este capítulo definiremos y demostraremos todos los resultados que vamos a necesitar en el capítulo 5. Como es habitual, dejamos referencias para reforzar la lectura de las secciones de este capítulo:

Con respecto a representaciones sobre grupos, principalmente sobre grupos finitos, recomendamos [41] como una muy buena introducción al tema. En particular, los capítulos 1 y 2 de [41].

Dentro de todas las representaciones de Galois existentes, en este documento nos vamos a centrar en las representaciones continuas en las cuales $G = G_K$ con K un cuerpo de números, $k = \overline{\mathbb{F}_\ell}$ con ℓ primo y $\dim_{\overline{\mathbb{F}_\ell}}(V) = 2$. Un lector que quiera conocer más sobre otras representaciones de Galois, recomendamos un resumen en la sección 2.1 de [10] y la presentación [37], que está basada en [10], pero completa algunas demostraciones.

Para el resto de las secciones, son mínimos los resultados extra que precisaremos, por lo que se harán recomendaciones dentro de la sección cuando sea necesario.

2.1. Representaciones sobre grupos

Definición **2.1.** *Sea G un grupo, k un cuerpo y V un k-espacio vectorial finito. Una* ***representación*** *de G sobre V es un morfismo*

$$\rho : G \to \mathrm{GL}(V)$$

Definición **2.2.** *Decimos que dos representaciones ρ_1 , $\rho_2 : G \to \mathrm{GL}(V)$ son equivalentes y lo denotaremos $\rho_1 \sim \rho_2$, si existe $\tau \in \mathrm{GL}(V)$ tal que*

$$\rho_1(g) = \tau\rho_2(g)\tau^{-1}$$

para todo $g \in G$.

Esto último nos permite trabajar sobre $\mathrm{GL}_n(k)$ dado que dos representaciones son equivalentes si hay una matriz de cambio de base entre ellas.

Definición **2.3.** *Sea $\rho : G \to \mathrm{GL}(V)$ una representación. Sea W un subespacio vectorial de V estable bajo la acción de G por ρ. Podemos entonces considerar la representación $\rho^W : G \to \mathrm{GL}(W)$. Diremos que ρ^W es una* ***subrepresentación*** *de ρ.*

Es claro que V o $\{0\}$ son subespacios invariantes para cualquier representación, por lo que estos no serán particularmente importantes. Veamos otra forma de generar espacios invariantes:

Ejemplo **2.4.** *Si $H \lhd G$ es un subgrupo normal, entonces*

$$V^H = \{v \in V : \rho(h)v = v, \quad \forall h \in H\}$$

es un subespacio invariante de ρ. En efecto, que es subespacio es fácilmente verificable, y para ver que es invariante, hay que ver que dado $g \in G$ y $v \in V^H$, entonces $\rho(g)v \in V^H$, es decir, que $\rho(h)\rho(g)v = \rho(g)v$ para todo $h \in H$. Dado $h \in H$, como $H \lhd G$, existe $h' \in H$ tal que $g^{-1}hg = h'$, y entonces

$$\rho(h)\rho(g)v = \rho(hg)v = \rho(gh')v = \rho(g)\rho(h')v = \rho(g)v$$

Definición **2.5.** *Una representación $\rho : G \to \mathrm{GL}(V)$ se dice* ***irreducible*** *o* ***simple*** *si V no contiene subespacios propios estables por G.*

Es decir, que sus únicos subespacios invariantes son V o $\{0\}$.

Definición **2.6.** *Una representación es* ***semisimple*** *si es suma directa de representaciones simples. Una representación es* ***indescomponible*** *si no es suma directa de subrepresentaciones propias.*

Destacamos el hecho de que si ρ es una representación sobre un espacio vectorial V de dimensión 2, entonces que ρ sea semisimple pero no irreducible, implica que ρ diagonaliza simultáneamente en alguna base.

Ejemplo **2.7.** *Sea $\lambda \in \mathbb{Q}^\times$ y $\rho : \mathbb{Z} \to \mathrm{GL}_2(\mathbb{Q})$ dada por*

$$\rho(n) = \begin{pmatrix} \lambda^n & n\lambda^{n-1} \\ 0 & \lambda^n \end{pmatrix}.$$

Esta representación no es semisimple y si indescomponible. No es simple puesto que la primer columna de la matriz representa un subespacio invariante de dimensión 1, y no es semisimple porque si lo fuera tendría que diagonalizar en alguna

base para todo n, sin embargo $\rho(1)$ es la forma de Jordan canónica.

Este ejemplo muestra que no toda representación es semisimple. Dadas las opciones para el caso de representaciones sobre espacios vectoriales de dimensión 2, una representación es semisimple pero no irreducible si y solo si diagonaliza simultáneamente en alguna base para todos los elementos de G.

Definición **2.8.** *Sea $\rho : G \to \mathrm{GL}(V)$ una representación y consideremos una filtración $\{0\} = V_0 \subseteq V_1 \subseteq ... \subseteq V_l = V$ donde cada V_j son subrepresentaciones de ρ y V_j/V_{j-1} es simple.*

Definimos la ***semisimplificación*** *de V como*

$$V^{ss} = \bigoplus_{j=1}^{l} V_j/V_{j-1}.$$

Esto nos permite definir una representación

$$\rho^{ss} : G \to \mathrm{GL}(V^{ss})$$

El Lema 3.9 de [13] asegura la existencia de tal filtración y el Teorema 3.11 de [13] (Teorema de Jordan-Holder) asegura que la semisimplificación no depende de la filtración elegida.

Ejemplo **2.9.** *Consideremos otra vez la representación del ejemplo 2.7 y tomemos la filtración $\{0\} \subseteq W \subseteq \mathbb{Q}^2$ siendo W el espacio vectorial de dimensión 1 estable por ρ mencionado en el ejemplo 2.7. La acción de ρ sobre $\mathbb{Q}^2/W$ es simple porque es un $\mathbb{Q}$-espacio vectorial de dimensión 1. Si llamamos $B = \{w, v\}$ a la base de Jordan con $W = \langle w \rangle$, entonces $\{v + U\}$ es base de $\mathbb{Q}^2/W$ y por lo tanto $\{w, v + W\}$ es base de V^{ss}. Además, $\rho(n)(v + W) = \lambda^n v + W$ lo que implica que*

$$\rho^{ss}(n) = \begin{pmatrix} \lambda^n & 0 \\ 0 & \lambda^n \end{pmatrix}$$

Como se observa, la semisimplificación es un proceso que transforma una representación cualquiera en una representación semisimple.

Definición **2.10.** *Llamaremos* ***caracteres*** *a las representaciones de dimensión 1. Al ser de dimensión 1 podemos considerar que su imagen es directamente $\mathrm{GL}_1(k) \approx k^\times$.*

Nos encargaremos de un carácter en particular en la sección 2.3, que será muy importante en los capítulos posteriores.

Ejemplo **2.11.** *Si $\rho : G \to \mathrm{GL}(V)$ es una representación, entonces $\det \rho$ es un carácter.*

2.2. Representaciones de Galois

Sea K un cuerpo de números y consideremos ahora que $G = G_K$. Vamos a trabajar con representaciones continuas, por lo que es necesario construir una topología sobre G_K.

La topología en G_K, la haremos dando una base de entornos abiertos para el automorfismo identidad de $\overline{K}$. Los abiertos de la base de entornos, serán los conjuntos G_L con L/K una extensión Galois y finita. Llamaremos a esta topología la **topología de Krull**. Para interiorizar sobre la topología de Krull y conocer algunas propiedades interesantes, recomendamos ver la sección 5.4 de [50].

Definición **2.12.** *Una* ***representación de Galois*** *es una representación de G_K sobre un espacio vectorial V, continua con respecto a la topología de Krull en G_K.*

Como mencionábamos al comienzo del capítulo 2, en este documento nos vamos a centrar en las representaciones de Galois continuas en las cuales $G = G_K$ con K un cuerpo de números, $k = \overline{\mathbb{F}_\ell}$ con ℓ primo y $\dim_{\overline{\mathbb{F}_\ell}}(V) = 2$. Para $\mathrm{GL}(V)$, tomaremos la topología discreta. Diremos en este caso, que la representación tiene dimensión 2, porque es la dimensión del espacio vectorial donde la representación actúa.

Veamos como la continuidad nos permite reducir la información necesaria a la hora de determinar una representación de Galois. Para ello, empezaremos por el siguiente resultado:

Teorema **2.13.** *(Cebotarev) Sea L/K una extensión Galois finita y $\sigma \in \mathrm{Gal}(L/K)$. Denotemos $P_{L/K}(\sigma)$ el conjunto de los ideales primos $\mathfrak{p}$ de K no ramificados en L/K, que tienen un primo $\mathfrak{P} \mid \mathfrak{p}$ para el cual*

$$\sigma = \left(\frac{L/K}{\mathfrak{P}}\right).$$

En otras palabras, $P_{L/K}(\sigma)$ es el conjunto de los primos $\mathfrak{p}$, para el cual σ es un elemento de la clase de conjugación del automorfismo de Frobenius en $\mathfrak{p}$.

Entonces,

$$d(P_{L/K}(\sigma)) = \frac{\#[\sigma]}{\#\,\mathrm{Gal}(L/K)}$$

donde $[\sigma]$ es la clase de conjugación de σ en $\mathrm{Gal}(L/K)$ y d es la densidad de Dirichlet (ver definición 13.1, pág 542 de [33]).

Demostración. Ver Teorema 13.4, pág. 545 de [33]. □

En particular, la densidad de Dirichlet es positiva para cualquier σ, lo que implica que hay infinitos primos $\mathfrak{p}$ para los cuales σ es un levantado del automorfismo de Frobenius en $\mathfrak{p}$. Esto es lo que realmente utilizaremos para el siguiente resultado:

Teorema **2.14.** *Sea S un conjunto finito de primos de K y sea $D = \cup_{\mathfrak{p}\notin S}[\mathrm{Frob}_{\mathfrak{p}}]$ donde $[.]$ representa la clase de conjugación de $\mathrm{Frob}_{\mathfrak{p}}$. Entonces D es denso en G_K con la topología de Krull.*

Demostración. Para probar que es denso, hay que demostrar que para cada $\sigma \in G_K$ y para cada entorno de σ, existe un elemento de Frobenius. En efecto, los entornos de σ en la topología de Krull son de la forma σG_L con L/K extensión Galois finita. Notar que $\tau \in \sigma G_L$ si y solo si $\tau\mid_L = \sigma\mid_L$. Por lo tanto, basta con restringir σ a L y ver el grupo de Galois $\mathrm{Gal}(L/K)$. Por el Teorema 2.13, existe un levantado de Frobenius para un ideal primo fuera de S, que coincide con $\sigma\mid_L$. Esto prueba que D es denso. □

Teorema **2.15.** *Sea S un conjunto finito de ideales primos de K y sean ρ y ρ' dos representaciones de Galois.*

1. *Si $\rho(\mathrm{Frob}_{\mathfrak{p}}) = \rho'(\mathrm{Frob}_{\mathfrak{p}})$ para todos los Frobenius de todos los $\mathfrak{p}$ ideales primos fuera de S, entonces $\rho = \rho'$.*

2. *Si ρ, ρ' son dos representaciones semisimples de dimensión 2 tales que $\operatorname{tr}\rho(\mathrm{Frob}_{\mathfrak{p}}) = \operatorname{tr}\rho'(\mathrm{Frob}_{\mathfrak{p}})$ y $\det\rho(\mathrm{Frob}_{\mathfrak{p}}) = \det\rho'(\mathrm{Frob}_{\mathfrak{p}})$ para todo $\mathfrak{p}$ ideal primo fuera de S, entonces $\rho \sim \rho'$.*

Demostración. 1. Como coinciden en D que es denso por el Teorema 2.14 y ρ y ρ' son continuas, entonces son iguales.

2. La continuidad de ρ y ρ' permiten restringirse a la imagen de los mapas Frobenius por la parte anterior. El hecho de que solo alcance con mirar la traza y el determinante de las representaciones es un Teorema de Brauer-Nesbitt (ver Teorema 30.16, pág. 215 de [9]). □

Definición **2.16.** *Sea $\rho : G_K \to \mathrm{GL}_2(V)$ una representación de Galois. Decimos que una representación* ***factoriza por una extensión finita*** *si existe una extensión L/K finita tal que $\mathrm{Gal}(\overline{K}/L) \subseteq \ker(\rho)$.*

Teorema **2.17.** *Sea ρ una representación de Galois de dimensión 2, entonces ρ factoriza por una extensión finita y su imagen está contenida en $\mathrm{GL}_2(\mathbb{F}_{\ell^r})$ para algún $r > 0$. Mas aún, si la representación es de dimensión 1 (un carácter), entonces factoriza por una extensión finita y abeliana.*

Demostración. Como la topología en $\mathrm{GL}(V)$ es discreta, $\{\mathrm{id}\}$ es abierto y por tanto, como ρ es continua, $\ker\rho$ es abierto, y entonces existe L/K una extensión Galois y finita tal que $G_L \subseteq \ker\rho$. Por lo tanto ρ factoriza por $G_K/G_L = \mathrm{Gal}(L/K)$ que es un grupo finito. Finalmente, $\operatorname{Im}\rho$ es un subgrupo finito de $\mathrm{GL}(V) \approx \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$, lo que implica que está contenido en $\mathrm{GL}_2(\mathbb{F}_{\ell^r})$ para algún $r > 0$.

Para la segunda parte, tenemos que su imagen es finita y abeliana. Finita, aplicando el mismo argumento que en el párrafo anterior y abeliana porque está contenida en $k^\times$. De esta forma, si llamamos χ al carácter y $L = (\overline{K})^{\ker(\chi)}$, entonces $\mathrm{Gal}(L/K) \simeq \mathrm{Im}(\chi)$ y por ende la extensión L/K es abeliana. $\square$

Estudiemos ahora la ramificación de las representaciones de Galois. Consideremos primero el diagrama 2.1

$$\begin{tikzcd}
 & \overline{K_{\mathfrak{p}}} \arrow[dd, dash, "G_{K_{\mathfrak{p}}}"] \\
\overline{K} \arrow[ur, dash] \arrow[d, dash, "G_K"'] & \\
K \arrow[r, dash] & K_{\mathfrak{p}}
\end{tikzcd}$$

Figura 2.1: Diagrama de la completación topológica y algebraica de K.

En el diagrama 2.1, tomamos primero la completación de K con respecto al primo $\mathfrak{p}$ y luego elegimos una clausura algebraica. Consideremos el mapa $\mathrm{res} : G_{K_{\mathfrak{p}}} \to G_K$ dado por $\sigma \mapsto \sigma\mid_{\overline{K}}$. Este mapa esta bien definido puesto que $K \subseteq K_p \cap \overline{K}$ y nos permite pasar la representación ρ a una representación $\rho_{\mathfrak{p}} = \rho \circ \mathrm{res} : G_{K_{\mathfrak{p}}} \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$.

Definición **2.18.** *Sea ρ una representación de Galois y $\mathfrak{p}$ un primo finito de K que no divide a ℓ. Decimos que una representación es* ***no ramificada*** *en $\mathfrak{p}$ si el grupo de inercia $I_{\mathfrak{p}}$ actúa trivial para la representación $\rho_{\mathfrak{p}}$.*

Definición **2.19.** *Sea ρ una representación de Galois. Dado $\mathfrak{p}$ primo finito de K que no divide a ℓ, consideremos $I_{\mathfrak{p}}^u$ los grupos de ramificación como en la sección 1.2. Definimos el* ***conductor local de una representación*** *como*

$$n(\mathfrak{p}, \rho) = \int_{-1}^{\infty} \operatorname{codim} \rho^{I_{\mathfrak{p}}^u} du$$

donde $\operatorname{codim} \rho^{I_{\mathfrak{p}}^u} = \dim V - \dim \rho_{\mathfrak{p}}^{I_{\mathfrak{p}}^u} = 2 - \dim \rho^{I_{\mathfrak{p}}^u}$ *(en el caso de* $\dim V = 2$*).*

Teorema **2.20.** *Sea ρ una representación de Galois y $\mathfrak{p}$ primo finito de K. Entonces*

1. *$n(\mathfrak{p}, \rho)$ es un entero positivo*
2. *$n(\mathfrak{p}, \rho) = 0$ si y solo si ρ es no ramificado en $\mathfrak{p}$.*
3. *El conjunto $\{\mathfrak{p} \nmid \ell : n(\mathfrak{p}, \rho) \neq 0\}$ es finito.*

Demostración. 1. Veamos primero que $n(\mathfrak{p}, \rho)$ es finito. En efecto, por el Teorema 2.17 basta con mirar la acción de la inercia $I_{\mathfrak{p}}^u$ dentro de $\mathrm{Gal}(L/K)$, siendo L el cuerpo por el cual ρ factoriza. Por el Teorema 1.21, $\cap_u I_{\mathfrak{p}}^u = \{\mathrm{id}\}$ así que como $\mathrm{Gal}(L/K)$ es finito, existe $u_0 \geq -1$ tal que $I_{\mathfrak{p}}^u$ dentro de $\mathrm{Gal}(L/K)$ es el subgrupo trivial para todo $u \geq u_0$. De esta forma $n(\mathfrak{p}, \rho) = \int_{-1}^{u_0} \operatorname{codim} \rho^{I_{\mathfrak{p}}^u} du$ y por lo tanto es finito. Una prueba de que es entero se puede encontrar en el Teorema 1, página 99 de [42].

2. Dado que $\operatorname{codim} \rho^{I_{\mathfrak{p}}^u} \geq 0$ como función de u, entonces $n(\mathfrak{p}, \rho) = 0$ si y solo si $\operatorname{codim} \rho^{I_{\mathfrak{p}}^u} = 0$ como función de u. Esto implica que $\operatorname{codim} \rho^{I_{\mathfrak{p}}} = 0$ y por tanto $I_{\mathfrak{p}}$ actúa trivial. Recíprocamente, como los grupos de ramificación forman una filtración (ver Teorema 1.21 parte 1), si $I_{\mathfrak{p}}$ actúa trivial, entonces $I_{\mathfrak{p}}^u$ actúa trivialmente para todo $u \geq -1$, y por lo tanto $\operatorname{codim} \rho^{I_{\mathfrak{p}}^u} = 0$ como función de u.

3. Dado que L/K es una extensión finita, sólo una cantidad finita de primos ramifica, y entonces sólo una cantidad finita cumple que $n(\mathfrak{p}, \rho) \neq 0$ por la parte 2. □

Definición **2.21.** *Sea ρ una representación de Galois. Definimos el* ***conductor global*** *de ρ como el número*

$$N_\rho = \prod_{\mathfrak{p} \nmid \ell} \mathfrak{p}^{n(\mathfrak{p}, \rho)}$$

con $\mathfrak{p}$ primo finito.

Por el Teorema 2.20, sabemos que N_ρ es un ideal de $\mathcal{O}_K$.

Si bien los primos que dividen a ℓ no se tienen en cuenta en el conductor, es importante tener algunos resultados en relación a la acción de sus grupos de ramificación por la representación de Galois:

Teorema **2.22.** *Si ρ es una representación de Galois y $\mathfrak{l} \mid \ell$, entonces $V^{P_{\mathfrak{l}}} \neq \{0\}$*

Demostración. Como ρ tiene imagen finita (por el Teorema 2.17) y por el primer teorema de isomorfismo que dice que $\rho(P_{\mathfrak{l}}) \approx P_{\mathfrak{l}}/(\ker(\rho) \cap P_{\mathfrak{l}})$, tenemos que $\rho(P_{\mathfrak{l}})$ es un ℓ-grupo finito por el Teorema 1.9.

Sea $v \in V$ un vector no nulo y sea W el subgrupo generado por la órbita de v $\mathrm{orb}_{\rho|_{P_{\mathfrak{l}}}}(v) = \{\rho(g)v \in V : g \in P_{\mathfrak{l}}\}$. Como ρ factoriza por un cociente finito W es un subgrupo de $\mathbb{F}_{\ell^r}$ y por lo tanto es finito. Más aún, del hecho de que $\left|\mathrm{orb}_{\rho|_{P_{\mathfrak{l}}}}(v)\right| = [I_{\mathfrak{l}} : \mathrm{Stab}(v)]$ tenemos que $|W|$ es una potencia de ℓ.

Es claro que $W^{P_{\mathfrak{l}}} = \{w \in W : \rho(g)v = v, \forall g \in P_{\mathfrak{l}}\} \subseteq W \cap V^{P_{\mathfrak{l}}}$, es un subgrupo y es la unión de todas las órbitas de la acción de ρ que solo tienen un elemento. Por lo tanto, $W \setminus W^{P_{\mathfrak{l}}}$, es la unión de las órbitas de más de un elemento por la acción

de ρ. Supongamos que $W^{P_\mathfrak{l}}$ es trivial y sea v_0 generador de una de las órbitas de $W \setminus W^{P_\mathfrak{l}}$. Del hecho de que $|\mathrm{orb}_\rho(v_0)| = [P_\mathfrak{l} : \mathrm{Stab}(v_0)]$ tenemos que $|\mathrm{orb}_\rho(v_0)| = \ell^\alpha$ con $\alpha > 0$ y esto para todo v_0. Por lo tanto, $\ell \mid \left|W \setminus W^{P_\ell}\right|$ lo que implica que $|W| \equiv \left|W^{P_\ell}\right| \pmod{\ell}$ y como $|W|$ es una potencia de ℓ, entonces $\ell \mid \left|W^{P_\mathfrak{l}}\right|$. Luego como $W^{P_\mathfrak{l}}$ es un subespacio, es no vacío y por ende $\left|W^{P_\mathfrak{l}}\right| \geq \ell$. □

Teorema **2.23.** *Si ρ es una representación de Galois semisimple y $\mathfrak{l}$ un primo en K que divide a ℓ, entonces $\rho(P_\mathfrak{l}) = \{1\}$*

Demostración. Basta probarlo con ρ simple. Del Teorema 2.22, tenemos que $V^{P_\mathfrak{l}}$ es no trivial. Como ρ es simple, si tiene un vector invariante, entonces todos los vectores tienen que ser invariantes (de lo contrario se podría factorizar en la dirección del vector invariante). Esto lleva a que $V^{P_\mathfrak{l}} = V$ y por lo tanto $\rho(P_\mathfrak{l}) = \{1\}$. □

2.3. El carácter ciclotómico

Definición **2.24.** *Dada ξ una raíz ℓ-ésima primitiva de la unidad en $\overline{K}$, definimos el* ***carácter ciclotómico*** *$\chi_\ell : G_K \to \mathbb{F}_\ell^\times$ tal que*

$$\sigma(\xi) = \xi^{\chi_\ell(\sigma)}$$

Esto tiene sentido porque los automorfismos de Galois mandan las raíces del polinomio ciclotómico en sí mismas, y estas raíces forman un grupo abeliano cíclico de orden ℓ con ξ como generador.

Teorema **2.25.** *Sea K cuerpo de números, ℓ primo racional y $\mathfrak{p}$ primo en K.*

1. *El carácter ciclotómico no depende de la raíz primitiva elegida,*
2. *Es continuo con respecto a la topología de Krull,*
3. *Si $\mathfrak{p} \nmid \ell$, entonces $\chi_\ell(I_\mathfrak{p}) = \{1\}$ y $\chi_\ell(\mathrm{Frob}_\mathfrak{p}) = \#k$ siendo $k = \mathcal{O}_K/\mathfrak{p}$.*

Demostración. 1. Si ξ' es otra raíz primitiva, entonces existe r entero coprimo con ℓ tal que $\xi' = \xi^r$. Llamemos χ'_ℓ al carácter que cumple que $\sigma(\xi') = \xi'^{\chi'_\ell(\sigma)}$. Entonces

$$\xi'^{\chi'_\ell(\sigma)} = \sigma(\xi') = \sigma(\xi^r) = \sigma(\xi)^r = (\xi^{\chi_\ell(\sigma)})^r = (\xi^r)^{\chi_\ell(\sigma)} = \xi'^{\chi_\ell(\sigma)}$$

lo que demuestra que son el mismo carácter.

2. Como χ_ℓ es un morfismo de grupos entre grupos topológicos cuya imagen está en $\mathbb{F}_\ell^\times$, para chequear la continuidad basta con ver que $\chi_\ell^{-1}(\{1\})$ es abierto, dado que la topología en $\overline{\mathbb{F}_\ell}^\times$ es la topología discreta. No es difícil convencerse que $\chi_\ell^{-1}(\{1\}) = \mathrm{Gal}(\overline{K}/K(\xi))$ que es abierto porque $K(\xi)/K$ es una extensión Galois finita.

3. Completemos K con respecto a la valuación natural de $\mathfrak{p}$ y consideremos la extensión $K_{\mathfrak{p}}(\xi)$, que es el cuerpo de descomposición del polinomio $x^{\ell}-1$ en $K_{\mathfrak{p}}$. Denominemos ϕ al polinomio irreducible de ξ en $\mathbb{Q}_p$ con $\mathfrak{p} \mid p$. Entonces $\Delta(K_{\mathfrak{p}}(\xi)/K_{\mathfrak{p}}) \mid \Delta(\phi)$ (no necesariamente es igual porque ϕ puede no ser irreducible en $K_{\mathfrak{p}}$). Como $\mathfrak{p} \nmid \ell$, todas las raíces ℓ-ésimas de la unidad son diferentes módulo $\mathfrak{p}$ puesto que el polinomio ϕ es coprimo a su derivada módulo $\mathfrak{p}$. De esta forma, como

$$\Delta(\phi) = \prod_{i \neq j} (\xi^i - \xi^j)$$

con $0 < i, j < \ell$, entonces $\mathfrak{p} \nmid \Delta(\phi)$ y por lo tanto, $\mathfrak{p} \nmid \Delta(K_{\mathfrak{p}}(\xi)/K_{\mathfrak{p}})$, lo que implica que la extensión $K_{\mathfrak{p}}(\xi)/K_{\mathfrak{p}}$ es no ramificada en $\mathfrak{p}$. En conclusión, $K_{\mathfrak{p}}(\xi) \subseteq K_{\mathfrak{p}}^{nr}$ y por ende si $\sigma \in I_{\mathfrak{p}}$, σ fija todas las raíces de la unidad.

Para la segunda parte de 2, escribamos $q = |k|$. Sea s una preimagen del mapa de Frobenius. Por ser un automorfismo de $\overline{K}$, $s(\xi)$ es otra raíz ℓ-ésima de la unidad. Dado que s es una preimagen del mapa de Frobenius,

$$s(\xi) = \xi^q \mod \mathfrak{p}$$

Como $s(\xi)$ es una raíz ℓ-ésima de la unidad y son todas distintas módulo $\mathfrak{p}$, necesariamente $s(\xi) = \xi^q$ lo que da el resultado. □

2.4. Caracteres sobre $G_{\mathbb{Q}}$

En el capítulo 5 estudiaremos caracteres sobre $G_{\mathbb{Q}}$, por lo que demostraremos en esta sección un resultado que utilizaremos repetidas veces.

Teorema **2.26.** *Sea $\chi : G_{\mathbb{Q}} \to \overline{\mathbb{F}_{\ell}}^{\times}$ un carácter continuo con ℓ primo racional. Entonces, χ factoriza por $\mathrm{Gal}(\mathbb{Q}(\xi_{\ell N_{\chi}})/\mathbb{Q})$, siendo N_{χ} el conductor del carácter.*

Demostración. Usando el Teorema 2.17, tenemos que χ factoriza por una extensión abeliana $L/\mathbb{Q}$. Aplicando el Teorema de Kronecker-Weber que enuncia que toda extensión abeliana está contenida en una extensión ciclotómica (ver el Teorema 1.10, página 324 de [33] para una demostración), se puede considerar $\chi : \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \to \overline{\mathbb{F}_{\ell}}^{\times}$ con ξ_n una raíz n-ésima de la unidad, siendo n un entero positivo. Más aún podemos asumir que $N_{\chi} \mid n$.

Sea p un primo distinto de ℓ tal que $p \mid n$. Denotemos $t = \nu_p(N_{\chi})$, $r = \nu_p(n)$ y escribamos $n = p^r n_0$ con $\gcd(p, n_0) = 1$. Observar que $r \geq t \geq 0$. Como estamos considerando un carácter, y en virtud de la propiedad 1 de 1,21, existe un $u_0 \in [-1, +\infty)$ para el cual $\operatorname{codim} \rho^{I_p^u} = 1$ si $u \leq u_0$ y $\operatorname{codim} \rho^{I_p^u} = 0$ si $u > u_0$, por lo que, utilizando la fórmula de la definición 2.19 tenemos que $t = n(p, \rho) = u_0 + 1$.

Consideremos el diagrama de extensiones de 2.2. Usando el Teorema 1.23 (Ley de reciprocidad de Artin) para la extensión ciclotómica, obtenemos que $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}(\xi_{p^t n_0})) =$

$$\begin{tikzcd}
\mathbb{Q}(\xi_n) \arrow[d, dash] \\
\mathbb{Q}(\xi_{p^t n_0}) \arrow[d, dash] \\
\mathbb{Q}(\xi_{n_0}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

Figura 2.2: Diagrama de extensiones que explica que se puede elegir n óptimo para los caracteres de $G_{\mathbb{Q}}$.

$I_p^{u_0+1} = I_p^t$, y como $I_p^t \subseteq \ker(\chi)$ entonces se puede cocientar por I_p^t y ahora χ queda definida en $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})/I_p^t \simeq \mathrm{Gal}(\mathbb{Q}(\xi_{p^t n_0})/\mathbb{Q})$. De forma análoga se procede con todos los primos p que dividen a n.

Esto nos deja con $n = \ell^s N_\chi$ donde por definición del conductor (ver definición 2.21), $\gcd(\ell, N_\chi) = 1$. Supongamos que $s > 1$ y consideremos el diagrama 2.3.

$$\begin{tikzcd}
 & \mathbb{Q}(\xi_n) \arrow[d, dash, "\mathbb{Z}/\ell^{s-1}\mathbb{Z}"] \\
(\mathbb{Z}/\ell^s\mathbb{Z})^\times \arrow[r, dash] & \mathbb{Q}(\xi_\ell, \xi_{N_\chi}) \arrow[d, dash, "(\mathbb{Z}/\ell\mathbb{Z})^\times"] \\
 & \mathbb{Q}(\xi_{N_\chi}) \arrow[d, dash] \\
 & \mathbb{Q}
\end{tikzcd}$$

Figura 2.3: Diagrama de extensiones que explica que se puede tomar $n = \ell N_\chi$.

La extensión $\mathbb{Q}(\xi_n)/\mathbb{Q}(\xi_{N_\chi})$ tiene orden $\varphi(\ell^s) = \ell^{s-1}(\ell - 1)$. El ℓ-Sylow es por tanto un subgrupo de orden ℓ^s que por el Teorema 1.9 es P_ℓ dentro de esa extensión. El cociente es por lo tanto $(\mathbb{Z}/\ell\mathbb{Z})^\times$ que se corresponde a la extensión

$\mathbb{Q}(\xi_\ell, \xi_{N_\chi})/\mathbb{Q}(\xi_{N_\chi})$. Como los órdenes de los elementos de $\overline{\mathbb{F}_\ell}^\times$ son coprimos a ℓ, entonces $\chi(\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}(\xi_\ell, \xi_{N_\chi}))) = \{1\}$ y por ende actúa trivial. Esto permite factorizar el carácter por $\mathbb{Q}(\xi_\ell, \xi_{N_\chi}) = \mathbb{Q}(\xi_{\ell N_\chi})$. □

2.5. Caracteres de $I_{\mathfrak{l},t}$

Al igual que en la sección anterior, dejamos en esta sección algunos resultados y definiciones que utilizaremos en el capítulo 5.

Definimos

$$(\mathbb{Q}/\mathbb{Z})' = \Big\{\alpha \in \mathbb{Q}/\mathbb{Z} : \alpha = \frac{a}{d} : \gcd(d, \ell) = 1\Big\}.$$

Es decir, los elementos de $\mathbb{Q}/\mathbb{Z}$ cuyo orden aditivo es coprimo con ℓ.

Teorema **2.27.** *Denotemos* $\mathrm{Hom}(I_{\mathfrak{l},t}, \overline{\mathbb{F}_\ell}^\times)_C$ *al conjunto de los caracteres continuos de* $I_{\mathfrak{l},t}$ *a* $\overline{\mathbb{F}_\ell}^\times$. *Entonces*

$$\mathrm{Hom}(I_{\mathfrak{l},t}, \overline{\mathbb{F}_\ell}^\times)_C \simeq (\mathbb{Q}/\mathbb{Z})'.$$

Demostración. Por el Teorema 1.14, tenemos que

$$\mathrm{Hom}(I_{\mathfrak{l},t}, \overline{\mathbb{F}_\ell}^\times)_C \simeq \mathrm{Hom}(\varprojlim \mu_d, \overline{\mathbb{F}_\ell}^\times)_C.$$

El paso clave aquí, es demostrar que

$$\mathrm{Hom}(\varprojlim \mu_d, \overline{\mathbb{F}_\ell}^\times)_C \simeq \varinjlim \mathrm{Hom}(\mu_d, \overline{\mathbb{F}_\ell}^\times).$$

Para ello debemos ahondar más en la construcción de los límites directo e inverso involucrados. Primero, tenemos que $\varprojlim \mu_d$ está dado por la propiedad universal:

$$\begin{tikzcd}
\varprojlim \mu_d \arrow[rr, dashed, leftarrow] \arrow[dr, "\alpha_d"] \arrow[ddr, bend right, "\alpha_{d'}"'] & & X \arrow[dl, "f_d"] \arrow[ddl, bend left, "f_{d'}"] \\
& \mu_d & \\
& \mu_{d'} \arrow[u, "\alpha_{dd'}"] &
\end{tikzcd}$$

donde si $d \mid d'$ el mapa $\alpha_{dd'}$ manda $g_{d'} \mapsto g_d^{d'/d}$.

Por otro lado tenemos

$$\begin{tikzcd}
\varinjlim \mathrm{Hom}(\mu_d, \overline{\mathbb{F}_\ell}^\times) \arrow[rr, dashed, "f"] & & X \\
& \mathrm{Hom}(\mu_d, \overline{\mathbb{F}_\ell}^\times) \arrow[ul, "\beta_d"'] \arrow[ur, "f_d"] \arrow[d, "\beta_{dd'}"] & \\
& \mathrm{Hom}(\mu_{d'}, \overline{\mathbb{F}_\ell}^\times) \arrow[uul, bend left, "\beta_{d'}"] \arrow[uur, bend right, "f_{d'}"'] &
\end{tikzcd}$$

Figura 2.4: Diagrama del límite directo de $\mathrm{Hom}(\mu_d, \overline{\mathbb{F}_\ell}^\times)$.

donde si $d \mid d'$ el mapa $\beta_{dd'}$ manda $\chi \mapsto \chi\alpha_{dd'}$.

En el diagrama 2.4, tomemos $X = \mathrm{Hom}(\varprojlim \mu_d, \overline{\mathbb{F}_\ell}^\times)_C$. Para construir f, basta con definir los mapas f_d de forma que sean compatibles. Tomemos f_d que mapee $\chi \mapsto \chi\alpha_d$. Es compatible puesto que si $d \mid d'$, entonces $f_{d'}\beta_{dd'}(\chi) = \chi\alpha_{dd'}\alpha_{d'} = f_d(\chi)$.

Necesitamos ahora una inversa para f. Sea τ un carácter de $\mathrm{Hom}(I_{\mathfrak{l},t}, \overline{\mathbb{F}_\ell}^\times)_C$. Como τ es continuo, por el Teorema 2.17, existe $r > 0$ tal que $\mathrm{Im}(\tau) \subseteq \mathbb{F}_{\ell^r}^\times$. Sea d tal que $\ker(\alpha_d) \subseteq \ker(\tau)$. Tales d existen porque los $\ker(\alpha_d)$ son una base de entornos decreciente con intersección trivial por el Teorema 1.11 y $\ker(\tau)$ es abierto. Definimos $\tau_d : \mu_d \to \overline{\mathbb{F}_\ell}^\times$ como $\tau_d(g_d) = \tau(\alpha_d^{-1}(g_d))$. El mapa no depende de la preimagen elegida porque $\ker(\alpha_d) \subseteq \ker(\tau)$. Para ver que los $(\tau_d)_d$ definen un elemento en $\varinjlim \mathrm{Hom}(\mu_d, \overline{\mathbb{F}_\ell}^\times)$, hay que ver que $\beta_{dd'}(\tau_d) = \tau_{d'}$ para todo $d \mid d'$. En efecto

$$(\beta_{dd'}(\tau_d))(g_{d'}) = \tau_d\alpha_{dd'}(g_{d'}) = \tau(\alpha_d^{-1}\alpha_{dd'}(g_{d'})) = \tau(\alpha_{d'}^{-1}(g_{d'})) = \tau_{d'}(g_{d'}).$$

Definimos g como el mapa construido anteriormente, y debemos ver ahora que f y g son inversas una de otra. En efecto,

$$(\chi_d)_d \xrightarrow{f} (\chi_d\alpha_d)_d \xrightarrow{g} (\chi_d\alpha_d\alpha_d^{-1})_d = (\chi_d),$$

$$\tau \xrightarrow{g} (\tau_d)_d \xrightarrow{f} (\tau_d \alpha_d)_d = \tau.$$

Una vez tenemos que $\mathrm{Hom}(\varprojlim \mu_d, \overline{\mathbb{F}_\ell}^\times)_C \simeq \varinjlim \mathrm{Hom}(\mu_d, \overline{\mathbb{F}_\ell}^\times)$, tenemos que si g_d es el generador de μ_d, entonces los morfismos son de la forma $g_d \mapsto \xi_d^k$ con $k = 0, .., d-1$ y $\left\{\xi_d^k : k = 0, ..., d-1\right\} \simeq (1/d)\mathbb{Z}/\mathbb{Z}$. Por lo tanto

$$\mathrm{Hom}(I_{\mathfrak{l},t}, \overline{\mathbb{F}_\ell}^\times) \simeq \varinjlim (1/d)\mathbb{Z}/\mathbb{Z}$$

Ahora la unión de los $(1/d)\mathbb{Z}/\mathbb{Z}$ con d coprimo a ℓ es un sistema directo que da como resultado $(\mathbb{Q}/\mathbb{Z})'$ □

Debido al morfismo del Teorema 2.27, tenemos unos elementos especiales que son, del lado de $(\mathbb{Q}/\mathbb{Z})'$, los elementos de la forma $1/(\ell^n - 1)$ con $n \geq 1$.

Definición **2.28.** *Llamaremos* ***caracteres fundamentales de nivel*** *n al carácter θ_{ℓ^n-1} obtenido como la preimagen de $1/(\ell^n - 1)$ por el mapa del teorema, y a todas sus potencias $\theta_{\ell^n-1}^{\ell^k}$ con $k = 0, ..., n-1$.*

Los $\theta_{\ell^n-1}^{\ell^k}$ son también los encajes de $\mathbb{F}_{\ell^n}$ dentro de $\overline{\mathbb{F}_\ell}$ por lo que su producto es un carácter con imagen en $\mathbb{F}_\ell$, y como ese espacio de caracteres es generado por el carácter ciclotómico, tenemos que

$$\prod_{k=0}^{n-1} \theta_{\ell^n-1}^{\ell^k} = \chi_\ell \tag{2.1}$$

Definición **2.29.** *Sea $\rho : I_{\mathfrak{l},t} \to \mathrm{GL}(V)$ una representación de Galois. Aprovechando el isomorfismo del Teorema 1.14, decimos que la representación ρ tiene* ***nivel*** *n si ρ factoriza por $\mathbb{F}_{\ell^n}^\times$ y no por $\mathbb{F}_{\ell^m}^\times$ con $m \mid n$ y $m < n$.*

Teorema **2.30.** *Sea $\chi : I_{\mathfrak{l},t} \to \overline{\mathbb{F}_\ell}^\times$ un carácter de nivel n. Entonces $\mathrm{Im}(\chi) \subseteq \mathbb{F}_{\ell^n}^\times$*

Demostración. Si χ tiene nivel n es porque la propiedad universal del cociente, permite ver a $\chi : \mathbb{F}_{\ell^n}^\times \to \overline{\mathbb{F}_\ell}^\times$. Ahora, dado cualquier $\sigma \in I_{\mathfrak{l},t}$, lo identificamos con un elemento de $\mathbb{F}_{\ell^n}^\times$, entonces $\chi(\sigma)^{\ell^n-1} = 1$ lo que implica que $\chi(\sigma) \in \mathbb{F}_{\ell^n}^\times$ □

Esta página ha sido intencionalmente dejada en blanco.

Capítulo 3

Curvas elípticas

En este capítulo nos preocuparemos de definir y enunciar los teoremas que utilizaremos en los capítulos 5 y 6. Recomendamos [46] para un profundo estudio de curvas elípticas. Dentro de los conocimientos del lector, puede seleccionar dentro de ese libro en que profundizar. En este capítulo, haremos muchas referencias a resultados de [46].

3.1. Curvas elípticas

Definición **3.1.** *Una* ***curva elíptica*** *es un par (E, O), donde E es una curva no singular de género 1 y $O \in E$. Decimos que E está definida sobre un cuerpo K y lo denotamos E/K, si es definida sobre K como curva algebraica y $O \in E(K)$.*

Teorema **3.2.** *Sea E/K una curva elíptica, entonces*

- *Existen funciones $x, y \in K(E)$ tales que el mapa*

$$\Phi : E \to \mathbb{P}^2 : \Phi = [x : y : 1]$$

  da un isomorfismo de E/K a una curva suave de la forma

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{3.1}$$

  con $a_1, ..., a_6 \in K$, y tal que $\Phi(O) = [0 : 1 : 0]$. Recíprocamente, toda curva suave de la forma como C, es una curva elíptica definida sobre K con $O = [0, 1, 0]$

- *Dos curvas elípticas son isomorfas como curvas algebraicas si existe $u \in K^\times$, $r, s, t \in K$ tales que*

$$X = u^2X' + r; \qquad Y = u^3Y' + su^2X' + t$$

Demostración. Ver Prop 3.1, cap. 3 de [46]. □

A partir de ahora, para nosotros una curva elíptica será un objeto algebraico proyectivo que es dado por una ecuación de la forma de (3.1).

Teorema **3.3.** *(Bézout) Sean C y D curvas algebraicas proyectivas de grados m y n respectivamente definidas sobre $\overline{K}$ que no tienen componentes irreducibles en común. Entonces $C \cap D$ tiene mn puntos contados con multiplicidad*

Demostración. Ver Corolario 7.8, cap. 1 de [16]. □

Teorema **3.4.** *Sea E/K una curva elíptica, entonces $E(K)$ es un grupo abeliano.*

Demostración. Por el Teorema 3.2, basta con considerar E en $\mathbb{P}^2(\overline{K})$. Sean $P, Q \in E(\overline{K})$ diferentes y consideremos L la recta en $\mathbb{P}^2(\overline{K})$ que pasa por ellos. Como E y L son curvas, son irreducibles, así que por el Teorema 3.3, $E \cap L$ tiene tres puntos contados con multiplicidad. Llamemos $P * Q$ a este punto y apliquemos el procedimiento de vuelta pero ahora construyendo L' una recta proyectiva que pasa por $P*Q$ y O (si son diferentes). De vuelta por el Teorema 3.3, tenemos un tercer punto al que definiremos como $P+Q$. Si $P = Q$ o $P*Q = 0$, consideramos la curva tangente a E, lo cual está bien definida porque E es suave. Definimos $P+Q = (P*Q)*O$.

Veamos algunas propiedades de esta operación. Sean P, Q, R tres puntos cualesquiera:

- $\underline{P + O = P \text{ para todo } P}$: Si $P * O$ es el tercer punto de E que pasa por la recta formada por P y O, el resultado de $P + O$, es el otro punto que está en la recta que pasa por los puntos $P * O$ y O, pero esta recta es la misma que la anterior, así que $P + O = P$.

- $\underline{P + Q = Q + P}$: La recta que forman P y Q es la misma que forman Q y P.

- Todo punto P tiene opuesto: Veamos que $P * O = -P$. En efecto, $P + (P * O) = (P*(P*O))*O = O*O$. Para ver que eso es O, veamos que O es punto triple. En efecto, si homogeneizamos la ecuación (3.1) y ponemos $Z = 0$ nos queda $0 = X^3$, lo que muestra que O es un punto triple y por tanto $O*O = O$.

- $\underline{(P + Q) + R = P + (Q + R)}$: Ver proposición 3.4, cáp. 3 de [46].

- $\underline{E(K) \text{ es un subgrupo de } E}$: Si $P, Q \in E(K)$, entonces la recta L que pasa por ellos está definida en K, y como también lo está E, entonces $P*Q \in E(K)$ puesto que un polinomio de grado n definido sobre K, con $n-1$ raíces K, tiene todas sus raíces en K (por ejemplo porque el coeficiente de x^{n-1} es la suma de las raíces y puedo despejar). Luego aplica lo mismo con $(P*Q)*O = P+Q$.

□

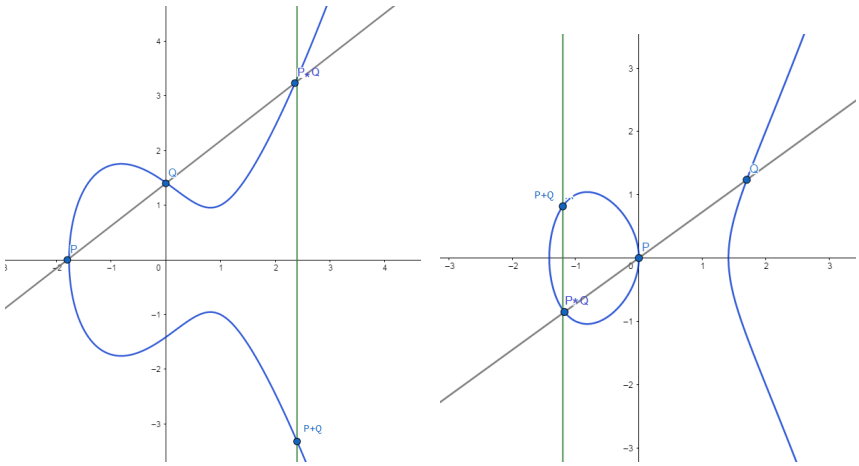


Figura 3.1: Ley de grupo en una curva elíptica

La figura 3.1 ilustra geométricamente la obtención del punto $P+Q$ en dos casos típicos de curvas elípticas $E/\mathbb{R}$.

Teorema **3.5.** *Si* $\mathrm{char}(K) \neq 2, 3$ *y* E/K *es una curva elíptica, entonces* E *es isomorfa a una curva elíptica de la forma*

$$y^2 = x^3 + ax + b \tag{3.2}$$

con $a, b \in K$

Demostración. La demostración de este resultado se puede encontrar al comienzo de la sección 1. cáp 3 de [46]. □

Una curva elíptica en la forma de la ecuación (3.2), la llamaremos **forma normal de Weierstrass**.

Definición **3.6.** *Sea* E/K *una curva elíptica en su forma normal de Weierstrass, llamaremos* ***discriminante*** *de* E *y lo denotaremos* $\Delta(E)$*, al número*

$$\Delta(E) = -16(4a^3 + 27b^2). \tag{3.3}$$

El discriminante cumple la propiedad de que es cero si y solo sí la curva es singular. La definición general para una curva elíptica en la forma de la ecuación (3.1) se puede encontrar al comienzo de la sección 1, cáp. 3, pagina 42 de [46]. La demostración de que es cero si y solo sí la curva es singular, se puede encontrar en la Proposición 1.4(a), cáp. 3 de [46]. En este documento solo la utilizaremos en el caso de una curva elíptica en su formal normal de Weierstrass.

3.2. Torsión y representación de curvas elípticas

El Teorema 3.4 mostró que $E(K)$ es un grupo abeliano, por lo tanto, la multiplicación por enteros actúa en los puntos de la curva elíptica. Denotaremos $[n]$ a este endomorfismo. Definimos además:

$$E(K)[n] = \{P \in E(K) : [n]P = O\}$$

$$E[n] = \left\{P \in E(\overline{K}) : [n]P = O\right\}$$

$$K(x(E[n])) = K(\{x(P) : P \in E[n]\})$$

$$K(E[n]) = K(\{x(P), y(P) : P \in E[n]\})$$

Los dos primeros son subgrupos y de hecho, $E(K)[n] = E[n] \cap E(K)$. Los dos últimos son cuerpos y de hecho, $K \subseteq K(x(E[n])) \subseteq K((E[n])$. Llamaremos **puntos de n-torsión** a los puntos de $E[n]$.

Teorema **3.7.** *Sea E/K una curva elíptica y sea $n \in \mathbb{Z}$ no nulo. Entonces:*

1. *Si* $\mathrm{char}(K) \nmid n$ *entonces*

$$E[n] = \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$

2. *Si* $\ell = \mathrm{char}(K)$ *entonces*

   a) $E[\ell^e] = \{0\}$ *para todo* $e = 1, 2, \ldots$ *ó*

   b) $E[\ell^e] = \frac{\mathbb{Z}}{\ell^e\mathbb{Z}}$ *para todo* $e = 1, 2, \ldots$

En el caso 2.(a) decimos que la curva es **supersingular** y en el caso 2.(b) que es **ordinaria**.

Demostración. Ver Corolario 6.4 página 86 de [46]. □

Ejemplo **3.8.** *Sea E/K una curva elíptica con* $\mathrm{char}(K) \neq 2, 3$. *Por el Teorema 3.5, podemos considerar en E la forma normal de Weierstrass $y^2 = f(x)$ con f de grado 3. Estudiemos los puntos de 2-torsión. Un punto $P = [x(P), y(P), 1] \in E[2]$ sí solo sí $y(P) = 0$ (ver Teorema 2.1, cáp. 2 de [47]), es decir, si $x(P)$ es raíz de f. En este caso entonces, $K(E[2]) = K(x(E[2]))$ que es el cuerpo de descomposición de f, y* $\mathrm{Gal}(K(E[2])/K)$ *es un subgrupo de S_3.*

Ejemplo **3.9.** *Como en el ejemplo 3.8, sea E/K una curva elíptica con* $\mathrm{char}(K) \neq 2, 3$ *y E en su forma normal de Weierstrass. Estudiemos ahora los puntos de 3-torsión. Un punto $P = [x(P), y(P), 1] \in E[3]$ si solo si $x(P)$ satisface ψ_3 un polinomio de grado 4 (ver Teorema 2.1, cáp 2 de [47]). Por lo tanto $K(x(E[3]))$ es el cuerpo de descomposición de ψ_3 y* $\mathrm{Gal}(K(x(E[3]))/K)$ *es un subgrupo de S_4. Como $y^2 = f(x)$, entonces $[K(E[3]) : K(x(E[3]))] \leq 2$, así que* $\mathrm{Gal}(K(E[3])/K)$ *es grupo de a lo sumo orden 48. Más aún, como veremos en el Teorema 3.11,* $\mathrm{Gal}(K(E[3])/K)$ *es un subgrupo de $GL_2(\mathbb{F}_3)$.*

Veamos que $K(\sqrt[3]{\Delta(E)}) \subseteq K(x(E[3]))$. Simples cálculos demuestran que en la forma normal de Weierstrass, $\Delta(E) = 2^4\,\Delta(f)$ y que $\Delta(\psi_3) = -3^3\,(\Delta(E))^2$. Sea g la resolvente cúbica[6] *de ψ_3, entonces $\Delta(g) = \Delta(\psi_3)$. Consideremos el diagramas de extensiones de la figura 3.2.*

$$\begin{tikzcd}
 & K(\psi_3) \arrow[d, dash, "\leq 4"] & \\
 & K(g) \arrow[dl, dash, "\leq 3"'] \arrow[dr, dash, "\leq 2"] & \\
K(\sqrt{\Delta(g)}) \arrow[dr, dash, "\leq 2"'] & & K(\theta) \arrow[dl, dash, "\leq 3"] \\
 & K &
\end{tikzcd}$$

Figura 3.2: Diagrama para $K(x(E[3]))$

En el diagrama anterior θ corresponde a una raíz de g. Tenemos que $\sqrt{\Delta(g)} = \sqrt{\Delta(\psi_3)} = 3\sqrt{-3}\,\Delta(E)$, por lo que $K(\sqrt{\Delta(g)}) = K(\sqrt{-3}) = K(\xi_3)$. El Teorema 1.28, implica que $K(g) = K(\xi_3, \alpha^{1/3})$ con $\alpha \in K^\times/(K^\times)^3$. Esto implica que podemos tomar $\theta = \alpha^{1/3}$, y que entonces $g(x) = \prod_{i=0}^{2}(x - \xi_3^i\theta)$. Entonces $\Delta(g) = \prod_{i\neq j}(\xi_3^i\theta - \xi_3^j\theta) = \theta^6 \prod_{i\neq j}(\xi_3^i - \xi_3^j) = \theta^6\Delta(x^3 - 1) = -3^3\,\theta^6 = -3^3\,\alpha^2$. Usando el hecho de que $\Delta(g) = \Delta(\psi_3) = -3^3\,(\Delta(E))^2$, obtenemos entonces que $\Delta(E) = \pm\,\alpha$, y por lo tanto, $K(\theta) = K(\sqrt[3]{\Delta(E)})$.

Del Teorema 3.7, vemos que si $m = \ell$ primo con $\mathrm{char}(K) \neq \ell$, entonces $E[\ell]$ es un $\mathbb{F}_\ell$-espacio vectorial de dimensión 2, lo cual nos permite entrar a teoría de representaciones de Galois de la siguiente manera:

Definición **3.10.** *Sea E/K una curva elíptica y ℓ un primo tal que $\ell \neq \mathrm{char}(K)$.*

[6] Ver al comienzo de la pág. 52 de [19] para una definición de la resolvente cúbica.

Definimos

$$\begin{aligned} \rho_{E,\ell} : G_K &\to \mathrm{GL}(E[\ell]) \\ \sigma &\mapsto (P \mapsto P^\sigma) \end{aligned}$$

donde P^σ es la acción del automorfismo sobre las coordenadas de P.

Como $[\ell]$ es un morfismo de curvas algebraicas con coeficientes en K, $[\ell]\sigma = \sigma[\ell]$ para todo $\sigma \in G_K$, lo que demuestra que la acción $\rho_{E,\ell}$ está bien definida, en el sentido de que $P^\sigma \in E[\ell]$ si $P \in E[\ell]$.

En general utilizaremos la notación matricial, cambiando $\mathrm{GL}(E[\ell])$ por $\mathrm{GL}_2(\mathbb{F}_\ell)$. Veamos algunas propiedades de $\rho_{E,\ell}$.

Teorema **3.11.** *Sea E/K una curva elíptica con* $\mathrm{char}(K) = 0$ *y ℓ un primo, entonces* $\ker(\rho_{E,\ell}) = \mathrm{Gal}(\overline{K}/K(E[\ell]))$. *En particular* $\mathrm{Gal}(K(E[\ell])/K)$ *es un subgrupo de* $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Demostración. $\sigma \in \ker(\rho_{E,\ell})$ si y solo si $P^\sigma = P$ para todo $P \in E[\ell]$, y esto si y solo si σ fija $K(E[\ell])$.

Para la última parte basta utilizar el primer teorema de isomorfismo en $\rho_{E,\ell}$. En efecto,

$$G_K/\ker(\rho_{E,\ell}) \simeq \mathrm{Gal}(K(E[\ell])/K) \simeq \mathrm{Im}(\rho_{E,\ell}) \leq \mathrm{GL}_2(\mathbb{F}_\ell)$$

donde usamos que $K(E[\ell])/K$ es una extensión Galois porque su grupo de Galois es precisamente el núcleo de $\rho_{E,\ell}$. □

Teorema **3.12.** *Sea E/K una curva elíptica y ℓ un primo, entonces* $\det(\rho_{E,\ell}) = \chi_\ell$.

Recordamos que χ_ℓ es el carácter ciclotómico definido en la sección 2.3.

Demostración. Para demostrar esto tendremos que usar algunos resultados del Weil Pairing que detallaremos a continuación.

El Weil Pairing es un mapa $e_N : E[N] \times E[N] \to \mu_N$ que cumple:

1. Es un mapa bilineal
2. Si $\{P, Q\}$ es base de $E[N]$ entonces $e_N(P, Q)$ es una raíz primitiva N-ésima de la unidad.
3. Si $\gamma \in \mathcal{M}_{2\times 2}(\mathbb{Z}/N\mathbb{Z})$ y

$$\begin{pmatrix} P' \\ Q' \end{pmatrix} = \gamma \begin{pmatrix} P \\ Q \end{pmatrix}$$

entonces

$$e_N(P', Q') = e_N(P, Q)^{\det(\gamma)}$$

4. Si $\sigma \in \mathrm{Gal}(\overline{K}/K)$ entonces

$$\sigma(e_N(P,Q)) = e_N(P^\sigma, Q^\sigma)$$

La definición de este mapa se puede encontrar en la sección 7.4 de [12] y la demostración de las propiedades en la proposición 7.4.1 en la misma sección de [12].

Con todo esto, sea $\{P,Q\}$ una base de $E[\ell]$ y sea $\sigma \in G_K$. Sea $\xi_\ell = e_\ell(P,Q)$ una raíz primitiva de la unidad. Ahora

$$\sigma(\xi_\ell) = \sigma(e_\ell(P,Q)) = e_\ell(P^\sigma, Q^\sigma)$$

por propiedad 4 y por otro lado

$$\begin{pmatrix} P^\sigma \\ Q^\sigma \end{pmatrix} = \rho_{E,\ell}(\sigma) \begin{pmatrix} P \\ Q \end{pmatrix}$$

lo que implica que

$$\xi_\ell^{\chi_\ell(\sigma)} = \sigma(\xi_\ell) = e_\ell(P,Q)^{\det(\rho_{E,\ell}(\sigma))} = \xi_\ell^{\det(\rho_{E,\ell}(\sigma))}$$

por propiedad 3. □

Ejemplo **3.13.** *Sea E/K una curva elíptica en su forma normal de Weierstrass con* $\mathrm{char}(K) = 0$. *Estudiemos las posibilidades para $\rho_{E,2}$. En su forma normal de Weierstrass, $E : y^2 = f(x)$ con f un polinomio de grado 3. Para empezar, el Teorema 3.11, muestra que $\rho_{E,2}$ factoriza por* $\mathrm{Gal}(K(E[2])/K) = \mathrm{Gal}(K(f)/K)$. *El ejemplo 3.8 muestra que* $\mathrm{Gal}(K(E[2])/K)$ *es un subgrupo de S_3. Por el Teorema 3.7, sabemos que $E[2]$ es isomorfo a $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ como grupo abeliano, así que $E[2]$ tiene tres puntos de orden 2 a los que llamaremos P_1, P_2 y P_3. Tomemos $\{P_1, P_2\}$ como base del módulo. Discutimos según tres casos:*

1. *<u>Dos puntos tienen coordenadas en K:</u> entonces los tres puntos tienen coordenadas en K dado que los $x(P_i)$ son raíces de f y por lo tanto la acción del grupo de Galois es trivial sobre los puntos, es decir*

$$\rho_{E,2}(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

para todo $\sigma \in G_K$

2. *<u>Solo un punto tiene coordenadas en K:</u> pongamos que $P_1 = (x_1, 0)$ tiene coordenadas en K, entonces $f(x) = (x - x_1)g(x)$ con g de grado 2 irreducible. Entonces* $\mathrm{Gal}(K(f)/K) = \{\mathrm{id}, \sigma\}$ *y $\sigma(P_2) = P_3 = P_1 + P_2$ y por lo tanto*

$$\rho_{E,2}(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

3. *Ningún punto tiene coordenadas en K: en este caso f es irreducible y* $\mathrm{Gal}(K(f)/K) = S_3$ *ó* A_3*. Será* A_3 *si* $\Delta(f)$ *es un cuadrado o* S_3 *si no.*

   Si es S_3*, el grupo de Galois tiene dos generadores,* $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$ *de orden 2 y* $\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ *de orden 3, que permuta los puntos como indican, así que*

$$\rho_{E,2}(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \rho_{E,2}(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

   Si es A_3*,* τ *genera el grupo de Galois, y*

$$\rho_{E,2}(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Para terminar esta sección haremos referencia a un resultado de Barry Mazur demostrado en 1978, que clasifica todas las torsiones posibles de curvas elípticas sobre $\mathbb{Q}$:

Teorema **3.14.** *(Clasificación de Mazur) Sea* $E/\mathbb{Q}$ *una curva elíptica. Entonces* $E_{tor}(\mathbb{Q})$ *es alguno de los siguientes grupos:*

- $\mathbb{Z}/N\mathbb{Z}$*, con* $1 \leq N \leq 10$ *o* $N = 12$*,*
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ *con* $N \leq 4$*.*

Demostración. Ver [27] y [28] para una demostración. □

3.3. Isogenias

Definición **3.15.** *Sean* E_1/K *y* E_2/K *dos curvas elípticas. Una* ***isogenia*** $\phi : E_1 \to E_2$ *es un morfismo de curvas algebraicas sobre* $\overline{K}$ *tal que* $\phi(O) = O$*.*

La proposición 6.8 de [16] prueba que si ϕ es una isogenia, entonces $\phi(E_1) = \{O\}$ o $\phi(E_1) = E_2$, y el Teorema 4.8 de [46] prueba que las isogenias son morfismos de grupos.

Ejemplo **3.16.** *Sea* E/K *una curva elíptica, entonces el mapa* $[n] : E \to E$ *definido en la sección 3.2 es una isogenia no constante si* $n \neq 0$*. Una demostración de esto se puede encontrar en el Ejemplo 4.1 y Proposición 4.2, cáp. 3 de [46].*

Teorema **3.17.** *Sean* E_1/K *y* E_2/K *dos curvas elípticas y* $\phi : E_1 \to E_2$ *una isogenia no constante, entonces existe una única isogenia* $\widehat{\phi} : E_2 \to E_1$ *tal que* $\widehat{\phi} \circ \phi = [n]$ *para algún* n*.*

Demostración. Ver el Teorema 6.1, cáp. 3 de [46]. □

Definición **3.18.** *Sean E_1/K y E_2/K dos curvas elípticas. Diremos que E_1 y E_2 son* ***isógenas*** *si existe una isogenia $\phi : E_1 \to E_2$ no constante.*

Ser isógenas es de hecho una relación de equivalencia. En efecto E es isógena a E puesto que [1] es una isogenia no constante entre E y E. La transitiva se cumple porque la composición de isogenias es isogenia y la propiedad reflexiva se cumple debido al Teorema 3.17.

Teorema **3.19.** *Sea E/K una curva elíptica y H un subgrupo finito de E. Entonces existen únicos E' curva elíptica y $\phi : E \to E'$ isogenia no constante tal que* $\ker \phi = H$.

Demostración. Ver Proposición 4.12, cáp. 3 [46]. □

Debido a su unicidad (salvo isomorfismo) llamaremos E/H a la curva elíptica E' del Teorema 3.19.

3.4. Curvas elípticas sobre cuerpos locales

Consideremos ahora que (K, ν) es un cuerpo local no arquimediano de característica cero sobre una valuación discreta. Como en la sección 1.1, sea R su anillo local, $\mathfrak{M}$ el ideal maximal y k su cuerpo residual de característica ℓ. Sea E/K una curva elíptica. Por el Teorema 3.2, sabemos que E tiene la forma

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

con $a_1, ..., a_6 \in K$. Llamaremos **cambio de variable admisible**, al cambio de variable de la forma $(x, y) \to (u^{-2}x, u^{-3}y)$ con $u \in K^\times$.

Tomando un cambio de variable admisible en E, transformamos a_i en u^ia_i. Eligiendo u tal que $\min_i \left\{\nu(u^ia_i)\right\} \geq 0$, nos aseguramos que $u^ia_i \in R$ para cada i. Esto nos permite reducir módulo $\mathfrak{M}$. Además, si los coeficientes tienen todos valuación positiva, también lo tendrá el discriminante asociado a esa curva elíptica.

Si Δ' es el discriminante con coeficientes u^ia_i y Δ el discriminante de la curva con coeficientes a_i, entonces, $\Delta' = u^{-12}\Delta$, por lo que la valuación de $\Delta(E)$ es modificable por múltiplos de 12.

Definición **3.20.** *Una curva elíptica E está en su* ***ecuación minimal*** *si todos sus coeficientes $a_i \in R$ y $\nu(\Delta(E))$ es el mínimo posible. Llamaremos* ***discriminante minimal****, y lo denotaremos $\Delta_\nu^{min}(E)$, al discriminante de una curva elíptica en su ecuación minimal.*

Observar que $\nu(\Delta_\nu^{min}(E))$ está bien definido y que $\Delta_\nu^{min}(E)$ está definido a menos de elementos invertibles en R.

Teorema **3.21.** *Sea E una curva elíptica con los coeficientes como en la ecuación* (3.1)*. Entonces*

1. *Si $a_i \in R$ para cada i y $\nu(\Delta(E)) < 12$, entonces la ecuación es minimal.*
2. *Si $a_i \in R$ para cada i y $\nu(c_4) < 4$, entonces la ecuación es minimal.*
3. *Si $a_i \in R$ para cada i y $\nu(c_6) < 6$, entonces la ecuación es minimal.*
4. *Si $\mathrm{char}(K) \neq 2, 3$ y E es una ecuación minimal, entonces $\nu(\Delta(E)) < 12$ o $\nu(c_4) < 4$*

Demostración. 1. Como $\nu(\Delta(E))$ puede ser modificado por múltiplos de 12, si $a_i \in R$ para cada i y $\nu(\Delta(E)) < 12$, entonces la ecuación es minimal. De igual manera se procede para demostrar 2 y 3, con c_4 y c_6 (ver al comienzo de la sección 1, cáp. 3, pagina 42 de [46] para una definición de ellos). Finalmente para 4, ver Remark 1.1, pág. 186, cáp. 7 de [46]. □

Para entender el fenómeno del cambio de variable admisible veamos el siguiente ejemplo:

Ejemplo **3.22.** *Consideremos $E/\mathbb{Q}$ en su forma normal de Weierstrass dada por*

$$E : y^2 = x^3 + \frac{1}{p^4}x + \frac{1}{p^6}$$

con $p \neq 2, 31$.

En la forma que se presenta, $\Delta(E) = -\frac{2^4\,31}{p^{12}}$ (usando la ecuación (3.3)*) y los coeficientes de E no se pueden reducir módulo p puesto que todos tienen valuación negativa en p. Sin embargo, si tomamos el cambio de variable admisible con $u = p^2$, la curva queda*

$$E : y^2 = x^3 + p^4x + p^6,$$

y su discriminante es $\Delta(E) = -2^4p^{12}\,31$.

Ahora los coeficientes están en R y se pueden reducir, y su reducción es $\widetilde{E} : y^2 = x^3$ que es singular. Esto se debe a que los coeficientes son muy divisibles entre p.

Sin embargo, si ahora tomamos el cambio de variable admisible $u = p$, la curva queda

$$E : y^2 = x^3 + x + 1$$

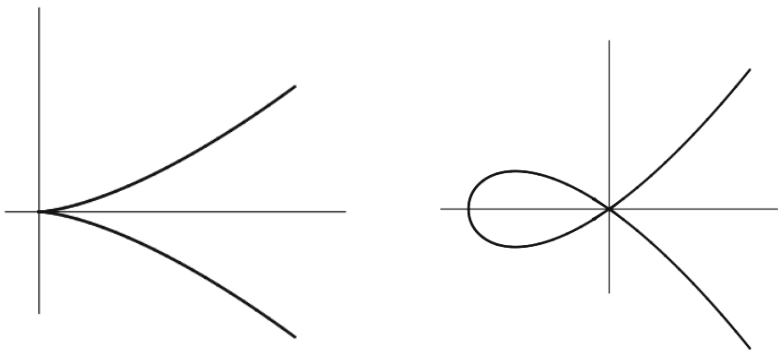
que tiene todos sus coeficientes en R y su discriminante es $\Delta(E) = -2^4\,31$ que sí es una curva elíptica en $k = \mathbb{F}_p$.

Como en el ejemplo 3.22, llamemos $\widetilde{E}/k$ a la curva que se obtiene al reducir la ecuación minimal de E. Dado que $\Delta(\widetilde{E}) = \widetilde{\Delta_\nu^{min}(E)}$, si $\nu(\Delta_\nu^{min}(E)) > 0$, la curva reducida es singular, y por ende no es una curva elíptica. Encontramos tres opciones posibles al reducir:

1. Buena reducción: Si $\widetilde{E}$ es una curva elíptica en k.
2. Mala reducción: Si $\widetilde{E}$ no es una curva elíptica en k. En este caso tenemos dos opciones:
   a) Reducción aditiva (o inestable): Si $\widetilde{E}$ tiene una cúspide.
   b) Reducción multiplicativa (o semiestable): Si $\widetilde{E}$ tiene un nodo. En este caso tenemos dos opciones:
      1) Multiplicativa split: si las pendientes de las tangentes del nodo están en k.
      2) Multiplicativa non-split: si las pendientes de las tangentes del nodo no están en k.

Si E/K tiene reducción multiplicativa non-split, cambiando K por una extensión L se puede lograr que E/L tenga reducción multiplicativa split. En el párrafo previo al corolario 5.4, cáp. 5 de [45] se explica que se puede tomar L/K una extensión cuadrática no ramificada en $\mathfrak{p}$.

La figura 3.3 ilustra los dos casos de mala reducción mencionados.



(a) Curva con una cúspide en $(0,0)$. (b) Curva con un nodo en $(0,0)$.

Figura 3.3: Curvas con singularidades.

El siguiente teorema relaciona los puntos de torsión de E con los puntos de la curva elíptica reducida:

Teorema **3.23.** *Sea E/K una curva elíptica de buena reducción, K cuerpo local en las hipótesis del comienzo de la sección y n un entero coprimo a* $\mathrm{char}(k)$. *Entonces el mapa reducción $E(K)[n] \xrightarrow{\sim} \widetilde{E}(k)$ es inyectivo.*

Demostración. Ver Proposición 3.1(b), cáp. 7 de [46]. □

Definición **3.24.** *Sea E/K una curva elíptica. El* ***conductor local*** *que denotaremos $f_\nu(E)$ es un número entero no negativo que da información sobre el tipo de reducción de E.*

La definición formal se puede encontrar en la sección 10, cáp. 4 de [45]. A los efectos de este documento, nos alcanza con el siguiente teorema:

Teorema **3.25.** *Sea E/K una curva elíptica con K cuerpo local en las hipótesis del comienzo de la sección. Si E tiene buena reducción o reducción multiplicativa, o si $\ell \geq 5$ entonces*

$$f_\nu(E) = \begin{cases} 0 & \text{si } E \text{ tiene buena reducción} \\ 1 & \text{si } E \text{ tiene reducción multiplicativa} \\ 2 & \text{si } E \text{ tiene reducción aditiva} \end{cases} \tag{3.4}$$

Demostración. Ver Teorema 10.2, cáp. 4 de [45]. □

Para terminar esta sección, consideremos el siguiente resultado que es debido a John Tate:

Teorema **3.26.** *Sea $K/\mathbb{Q}_p$ una extensión finita y E/K una curva elíptica con reducción multiplicativa split. Entonces existe $q \in \mathfrak{M}$ y $\phi : \overline{K}^\times/q^{\mathbb{Z}} \to E(\overline{K})$ un isomorfismo de grupos que es compatible con la acción del grupo de Galois G_K, siendo $q^{\mathbb{Z}}$ el subgrupo multiplicativo generado por q. En particular, si L/K es una extensión algebraica, $\phi : L^\times/q^{\mathbb{Z}} \to E(L)$ es un isomorfismo de grupos.*

Demostración. Ver Teoremas 3.1 y 5.3, cáp. 5 de [45]. □

Aclarar que la acción de G_K en $\overline{K}^\times$ es $\sigma.x = \sigma(x)$, que queda bien definida en $\overline{K}^\times/q^{\mathbb{Z}}$ porque $q \in R \subseteq K$. La acción de G_K en $E(\overline{K})$ es P^σ, que es actuar sobre las coordenadas de P.

El número q en el Teorema 3.26 se lo denomina el **período de Tate** y está relacionado con el discriminante de E a través de la ecuación

$$\Delta(E) = q \prod_{n \geq 1} (1 - q^n)^{24} \tag{3.5}$$

que converge en $\mathfrak{M}$.

Si la curva E/K tiene reducción multiplicativa non-split, considerando la extensión cuadrática L/K que transforma E/L en una reducción multiplicativa split,

podemos aplicar el Teorema 3.26. Esto hace que la acción de Galois no sea totalmente compatible en los dos lados, sino que aparece un carácter $\delta : G_K \to \mathrm{Gal}(L/K) \simeq \{\pm 1\}$ de orden 2 tal que

$$\phi(x)^\sigma = \phi(\delta(\sigma)\sigma.x)$$

para todo $x \in \overline{K}^\times/q^{\mathbb{Z}}$. Para una explicación más detallada, ver el lema 5.2, cáp. 5 de [45].

3.5. Curvas elípticas sobre cuerpos de números

Consideramos ahora el caso en el que K es un cuerpo de números. Por cada primo finito $\mathfrak{p}$, podemos considerar su localización y calcular su conductor local. Esto nos motiva a la siguiente definición:

Definición **3.27.** *Sea E/K una curva elíptica, el* ***conductor global*** *que denotaremos $N(E)$ es el ideal*

$$N(E) = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}(E)}$$

donde la productoria es tomada sobre los primos finitos de K y $f_{\mathfrak{p}}(E)$ es el conductor local en la valuación natural de $\mathfrak{p}$

Si bien la productoria se hace sobre infinitos términos, solo finitos son no triviales. En efecto, por el Teorema 3.25, $f_{\mathfrak{p}}(E) = 0$ si y solo sí E tiene buena reducción módulo $\mathfrak{p}$ y esto sí y solo sí $\nu_{\mathfrak{p}}(\Delta^{min}_{\nu_{\mathfrak{p}}}(E)) = 0$. Ahora, dada una curva elíptica E con su ecuación como la de 3.1, son finitos los primos $\mathfrak{p}$ para los cuales esa ecuación ya no está en su versión minimal, puesto que son finitos los primos $\mathfrak{p}$ que dividen a $\Delta(E)$. Para los otros primos primos, $\Delta^{min}_{\nu_{\mathfrak{p}}}(E) = \Delta(E)$ y $\nu_{\mathfrak{p}}(\Delta^{min}_{\nu_{\mathfrak{p}}}(E)) = 0$.

Definición **3.28.** *Sea E/K una curva elíptica sobre K un cuerpo de números. Decimos que E es* ***semiestable*** *si E tiene buena reducción o reducción multiplicativa para todos los primos finitos $\mathfrak{p}$.*

El Teorema 3.25, muestra que una curva es semiestable si y solo si $N(E)$ es libre de cuadrados.

El siguiente teorema nos relaciona propiedades de la curva elíptica con el conductor de su representación de Galois asociada:

Teorema **3.29.** *Sea E/K una curva elíptica con K cuerpo de números, sea $\mathfrak{p}$ primo finito en K y ℓ primo en $\mathbb{Q}$ tal que $\mathfrak{p} \nmid \ell$.*

1. *Si E tiene buena reducción en $\mathfrak{p}$, entonces $\rho_{E,\ell}$ es no ramificada en $\mathfrak{p}$.*

2. *Si E tiene reducción multiplicativa en $\mathfrak{p}$, entonces son equivalentes:*

a) $n(\mathfrak{p}, \rho_{E,\ell}) = 0$

b) $\ell \mid \nu_{\mathfrak{p}}(\Delta_{\nu_{\mathfrak{p}}}^{min}(E))$

c) *$K(E[\ell])/K$ es no ramificado en $\mathfrak{p}$*

En caso contrario, $n(\mathfrak{p}, \rho_{E,\ell}) = 1$.

Demostración. 1. Si E tiene buena reducción, por el Teorema 3.23, $E(K)[\ell] \hookrightarrow \widetilde{E}(k)$ es inyectivo. Sea $\sigma \in I_{\mathfrak{p}}$ y $P \in E[\ell]$, entonces $\widetilde{P^\sigma - P} = \widetilde{P^\sigma} - \widetilde{P} = \widetilde{O}$ puesto que $\sigma \in I_{\mathfrak{p}}$. Luego $P^\sigma = P$ y por ende $I_{\mathfrak{p}}$ actúa trivial.

2. Si ahora E tiene reducción multiplicativa, la idea es usar el período de Tate de la completación $K_{\mathfrak{p}}$ de K. Si E tiene reducción multiplicativa non-split, consideramos $L/K_{\mathfrak{p}}$ la extensión cuadrática no ramificada en $\mathfrak{p}$ que hace a E split. Para considerar ambos casos, trabajemos en L donde $L/K_{\mathfrak{p}}$ será una extensión de grado 1 ó 2 dependiendo el caso.

Tenemos entonces $\phi : \overline{K_{\mathfrak{p}}}^{\times}/q^{\mathbb{Z}} \to E(\overline{K_{\mathfrak{p}}})$ un isomorfismo de grupos compatible con la acción de Galois por el Teorema 3.26. En particular $E[\ell] \simeq \langle \xi_\ell, q^{1/\ell} \rangle / q^{\mathbb{Z}}$.

La propiedad funtorial de ϕ implica que si $F = L(E[\ell])$, entonces $E(F)[\ell] = E[\ell] \simeq \langle \xi_\ell, q^{1/\ell} \rangle / q^{\mathbb{Z}} = \left(F^\times/q^{\mathbb{Z}}\right)_\ell$, siendo $\left(F^\times/q^{\mathbb{Z}}\right)_\ell$ la ℓ-torsión del grupo $F^\times/q^{\mathbb{Z}}$. Por lo tanto $L(\xi_\ell, q^{1/\ell}) \subseteq F$. Recíprocamente, si $\alpha \in \left(F^\times/q^{\mathbb{Z}}\right)_\ell$, entonces $\phi(\alpha) \in E(F)[\ell] = E[\ell]$ lo que implica que $\alpha \in L(\xi_\ell, q^{1/\ell})$ y por lo tanto $F = L(\xi_\ell, q^{1/\ell})$.

De esta forma, $I_{\mathfrak{p}}$ actúa trivial, si y solo sí F/L es no ramificada, sí y solo sí $\mathrm{Im}(\nu_F) = \mathrm{Im}(\nu_L) = \mathrm{Im}(\nu_{\mathfrak{p}})$ (donde en la última igualdad usamos que $L/K_{\mathfrak{p}}$ es no ramificada), sí y solo sí $\nu_F(q^{1/\ell}) \in \mathbb{Z}$ y esto último sí y solo sí $\ell \mid \nu_{\mathfrak{p}}(q)$. A través de la ecuación (3.5) tenemos que $\nu_{\mathfrak{p}}(q) = \nu_{\mathfrak{p}}(\Delta_{\nu_{\mathfrak{p}}}^{min}(E))$, lo que da el resultado.

Ahora, si ninguna de las equivalencias se cumple tenemos que $n(\mathfrak{p}, \rho_{E,\ell}) = 1$. Para demostrar esto, debemos mencionar que la definición del conductor local de la curva elíptica, $f_{\mathfrak{p}}(E)$, dado en la definición 3.24, se hace a través de la representación de Galois ℓ-ádica de la curva elíptica, y como la representación módulo ℓ se obtiene de una reducción de la representación ℓ-ádica, tenemos que $n(\mathfrak{p}, \rho_{E,\ell}) \leq f_{\mathfrak{p}}(E)$. Finalmente, por el Teorema 3.25, $n(\mathfrak{p}, \rho_{E,\ell}) \leq 1$ en el caso de reducción multiplicativa. □

En la sección 3.4 vimos que la ecuación minimal de la curva elíptica depende de la valuación por la que se reducía. La proposición 8.2, cáp. 8 de [46], da una condición necesaria y suficiente para que una curva elíptica sobre un cuerpo de números K tenga un modelo minimal global, es decir, un modelo minimal que sirve para todas las valuaciones finitas de K. A los efectos de este documento sin embargo, nos alcanza con enunciar el siguiente resultado, que es un corolario de la proposición 8.2, cáp. 8 de [46]:

Teorema **3.30.** *Si K es un cuerpo de números con número de clase 1, entonces toda curva elíptica tiene un modelo minimal global.*

Demostración. Ver Corolario 8.3, cáp. 8 de [46]. □

Llamaremos simplemente $\Delta^{min}(E)$ al discriminante del modelo minimal global de E, y quitaremos el prefijo que dependía de la valuación, puesto que ahora $\Delta^{min}_{\nu_{\mathfrak{p}}}(E) = \Delta^{min}(E)$ para todos los primos $\mathfrak{p}$.

Observar que si E tiene modelo minimal global entonces los primos que dividen al conductor global y al discriminante son los mismos. Esto ocurre simplemente porque en el conductor global aparecen los primos de mala reducción y los de mala reducción son justamente los que dividen a $\Delta^{min}(E)$.

Para terminar esta sección, consideremos dos resultados que nos serán útiles en las secciones 5.3 y 6.3 respectivamente.

Teorema **3.31.** *Sea ℓ primo, $E/\mathbb{Q}$ una curva elíptica semiestable y $\rho_{E,\ell}$ reducible. Entonces E o una curva isógena poseen un punto de ℓ-torsión.*

Demostración. Si es reducible, $\rho_{E,\ell} = \begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$ con H (la primer columna) un subgrupo de orden ℓ $G_{\mathbb{Q}}$-invariante.

El ingrediente principal aquí es dado por Serre en el lema 6, pág. 307 de [40]. En ese lema, demuestra que si $E/\mathbb{Q}$ es semiestable, entonces φ_1 y φ_2 no ramifican fuera de ℓ y solo uno de ellos ramifica ℓ. Como $\mathbb{Q}$ no admite extensiones de grado mayor a 1 no ramificadas, uno de ellos debe ser 1, y el otro χ_ℓ por el Teorema 3.12.

Si $\varphi_1 = 1$, entonces E tiene un punto de orden ℓ. Si $\varphi_2 = 1$, entonces la primer columna es un subgrupo H que es G_K-invariante de orden ℓ, entonces $E' = E/H$ tiene un punto de orden ℓ puesto que la representación va a ser de la forma

$$\rho_{E',\ell} = \begin{pmatrix} 1 & * \\ 0 & \chi_\ell \end{pmatrix}.$$

□

Teorema **3.32.** *(Cotas de Hasse) Sea E/K una curva elíptica, $\mathfrak{q}$ ideal primo de $\mathcal{O}_K$ y $\widetilde{E}$ la reducción de E módulo $\mathfrak{q}$. Entonces*

$$\left| \#\widetilde{E}(\mathbb{F}_{\mathfrak{q}}) - N(\mathfrak{q}) - 1 \right| \leq 2\sqrt{N(\mathfrak{q})}.$$

Demostración. Ver Teorema 1.1 de [46]. □

Esta página ha sido intencionalmente dejada en blanco.

Capítulo 4

Formas Modulares

En este capítulo daremos un breve resumen de formas modulares clásicas, lo necesario para comprender las formas modulares módulo ℓ, que son las que nos interesan en la Conjetura de Serre. Para un lector que ya conoce sobre formas modulares clásicas, en la primer sección nos enfocaremos en las formas modulares para $\Gamma_1(N)$, pero ya comenzaremos con el espacio dividido por los caracteres de $\mathbb{Z}/N\mathbb{Z}$. Esta separación hace que ya no sea necesario el operador diamante, puesto que el mismo preserva estos subespacios. Solo los operadores de Hecke T_n nos interesarán aquí.

Para un lector que no conoce sobre formas modulares clásicas le recomendamos [36]. En [36] se evitan algunas demostraciones pesadas puesto que la idea es dar un resumen sobre el tema. Si el lector busca una lectura más profunda acerca de formas modulares clásicas, le recomendamos [12].

4.1. Formas modulares clásicas

Sea $\mathrm{SL}_2(\mathbb{Z}) = \{\gamma \in \mathcal{M}_{2\times 2}(\mathbb{Z}) : \det(\gamma) = 1\}$. Es conocido que $\mathrm{SL}_2(\mathbb{Z})$ es un grupo no abeliano con el producto de matrices. Esto se puede ver por el hecho de que el determinante es un morfismo con el producto y que dada una matriz $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, su inverso es $\frac{1}{\det(A)} \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, y entonces el inverso de una matriz de $\mathrm{SL}_2(\mathbb{Z})$ es una matriz de $\mathrm{SL}_2(\mathbb{Z})$.

Definición **4.1.** *Llamamos* ***subgrupo de congruencia de nivel N*** *al conjunto*

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

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

Es fácil ver que $\Gamma_0(N)$ es un subgrupo de $\mathrm{SL}_2(\mathbb{Z})$. Más aún $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N\prod_{p|N}(1 + 1/p)$ (ver página 14 de [12]). En particular, el índice es finito. Notar

que $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$

Recordamos que un **carácter de Dirichlet** es un morfismo de grupos $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. El mismo puede ser extendido a $\chi : \mathbb{Z} \to \mathbb{C}$ como

$$\chi(n) = \begin{cases} \chi(n + N\mathbb{Z}) & \text{si } \gcd(n, N) = 1 \\ 0 & \text{si no} \end{cases}$$

Por abuso de notación, llamaremos χ también a este carácter. La función χ es totalmente multiplicativa[7].

Llamaremos $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ al semiplano superior complejo.

Por comodidad en la notación, definimos el siguiente operador:

Definición **4.2.** *Sea $\epsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ un carácter de Dirichlet, k un entero y $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, definimos el operador $[\gamma]_{k,\epsilon_0} : \{F : \mathcal{H} \to \mathbb{C}\} \to \{F : \mathcal{H} \to \mathbb{C}\}$ dado por:*

$$(F\,[\gamma]_{k,\epsilon_0})(z) = \epsilon_0(d)(cz + d)^{-k} F\left(\frac{az + b}{cz + d}\right) \tag{4.1}$$

cuando $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Observar que si $z \in \mathcal{H}$, entonces $\frac{az+b}{cz+d}$ sigue estando en $\mathcal{H}$ porque $\det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ es positivo. Por lo tanto $[\gamma]_{k,\epsilon_0}$ está bien definido. Es simple verificar que $[\gamma\gamma']_{k,\epsilon_0} = [\gamma]_{k,\epsilon_0}\,[\gamma']_{k,\epsilon_0}$ para cualesquiera sean $\gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$.

Definición **4.3.** *Sea $\epsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ un carácter de Dirichlet, k y $N \geq 1$ enteros. Una* ***forma débilmente modular de peso*** *k* ***y nivel*** *N* ***asociada a*** *ϵ_0 es una función $F : \mathcal{H} \to \mathbb{C}$ tal que*

1. *F es holomorfa en $\mathcal{H}$,*
2. *$F\,[\gamma]_{k,\epsilon_0} = F$ para toda $\gamma \in \Gamma_0(N)$.*

Si aplicamos el punto 2 a una forma débilmente modular con la matriz $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$, obtenemos que $F(z) = F(z + 1)$ para todo $z \in \mathcal{H}$, y por lo tanto F es 1-periódica y admite una expansión de Fourier dada por $F(z) = \sum_{n=-\infty}^{\infty} a_n(F) q^n$ donde $q = e^{2\pi i z}$. Podemos ver entonces a F como una función con variable q en $B_1(0) \setminus \{0\}$.

Definición **4.4.** *Diremos que una forma débilmente modular F es* ***holomorfa en infinito*** *si la expansión de Fourier anterior admite una extensión holomorfa a $B_1(0)$. En ese caso definimos $F(\infty) = a_0(F)$.*

[7] Una función $f : \mathbb{Z} \to \mathbb{C}$ se dice totalmente multiplicativa si $f(mn) = f(m)f(n)$ para todo $m, n \in \mathbb{Z}$

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

Finalmente, estamos en condiciones de definir:

Definición **4.5.** *Sea $\epsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ un carácter de Dirichlet, k y $N \geq 1$ enteros. Decimos que $F : \mathcal{H} \to \mathbb{C}$ es una* ***forma modular de peso*** *k* ***y nivel*** *N* ***asociada a*** *ϵ_0 si*

1. *F es una forma débilmente modular de peso k y nivel N asociada a ϵ_0,*
2. *$F\,[\alpha]_{k,\epsilon_0}$ es holomorfa en infinito $\forall \alpha \in \mathrm{SL}_2(\mathbb{Z})$.*

A la condición del último punto de la definición 4.5 se le suele denominar **holomorfa en las cúspides** por razones que se exponen en la sección 1.1 de [36].

Llamaremos $\mathcal{M}_k(N, \epsilon_0)$ al espacio de las formas modulares de peso k, nivel N asociada a ϵ_0. Es fácil ver que son $\mathbb{C}$-espacio vectoriales. Más aún, su dimensión es finita y en casi todos los casos se conoce la dimensión. Para ver una demostración de esto, se recomienda leer el capítulo 3 de [12]. Los resultados de las dimensiones son mostrados en el Teorema 3.5.1 (para k par) y Teorema 3.6.1 (para k impar), ambos en el capítulo 3 de [12]. La figura 3.3 de la página 107 de [12] muestra el valor de la dimensión para $\Gamma_0(N)$.

Dentro de $\mathcal{M}_k(N, \epsilon_0)$, nos va interesar el siguiente subespacio:

Definición **4.6.** *Sea $\epsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ un carácter de Dirichlet, k y $N \geq 1$ enteros. Decimos que $F : \mathcal{H} \to \mathbb{C}$ es una* ***forma cuspidal de peso*** *k* ***y nivel*** *N* ***asociada a*** *ϵ_0 si*

1. *F es una forma modular de peso k y nivel N asociada a ϵ_0,*
2. *$F\,[\alpha]_{k,\epsilon_0}(\infty) = 0$, $\forall \alpha \in \mathrm{SL}_2(\mathbb{Z})$.*

Llamaremos $\mathcal{S}_k(N, \epsilon_0)$ al espacio de las formas cuspidales de peso k y nivel N asociada a ϵ_0. Es fácil ver que es un $\mathbb{C}$-subespacio vectorial de $\mathcal{M}_k(N, \epsilon_0)$.

Al igual que con $\mathcal{M}_k(N, \epsilon_0)$, se conocen las dimensiones de casi todos los subespacios $\mathcal{S}_k(N, \epsilon_0)$. Los valores se pueden encontrar en las mismas referencias citadas antes.

Nos interesa ahora considerar operadores sobre el espacio de formas modulares que pueden restringirse al subespacio de formas cuspidales. Estos operadores se conocen como los **operadores de Hecke**. Su definición general puede encontrarse en la sección 1.2 de [36].

Dentro de todos los operadores de Hecke posibles que se pueden definir nos interesarán los operadores $T_n : \mathcal{S}_k(N, \epsilon_0) \to \mathcal{S}_k(N, \epsilon_0)$. Sus definiciones no son relevantes a efectos de este documento, pero lo que sí utilizaremos en algunas demostraciones es que su construcción se hace de la siguiente forma:

- Se define T_p para cada $p \nmid N$ como en la definición 1.10 de [36].
- Se define T_{p^r} de forma inductiva en función de T_p y los anteriores (ver posterior al Teorema 1.12 de [36]).
- Se prueba que si p, q son primos distintos entonces T_{p^r} y T_{q^s} conmutan para todo $r, s \geq 0$ y se define $T_n = \prod_{i=1}^{m} T_{p_i^{e_i}}$ siendo $n = \prod_{i=1}^{m} p_i^{e_i}$.

Resumimos en el siguiente teorema los resultados que nos interesan aquí.

Teorema **4.7.** *Sean m y n dos enteros positivos. Entonces:*

1. $T_m T_n = T_n T_m$.
2. *Si* $\gcd(m, n) = 1 \Rightarrow T_m T_n = T_{mn}$.
3. *Si $F \in \mathcal{M}_k(N, \epsilon_0)$ tiene una expansión de Fourier de la forma $F(z) = \sum_{j=0}^{\infty} a_j(F) q^j$ con $q = e^{2\pi i z}$, entonces*

$$a_j(T_n F) = \sum_{d \mid \gcd(j,n)} d^{k-1} \epsilon_0(d) a_{jn/d^2}(F).$$

En particular, si $\gcd(j, n) = 1$ *entonces* $a_j(T_n F) = a_{jn}(F)$.

Demostración. Para los primeros dos puntos, ver el Teorema 1.13 de [36]. Para el punto 3, ver la proposición 5.3.1 del capitulo 5 de [12]. □

Recordamos que un operador $T : V \to V$ es **normal** si conmuta con su operador adjunto. Para poder definir adjuntos en los operadores de Hecke que venimos estudiando, es necesario definir un producto interno en las formas cuspidales. Este producto se conoce como el **producto interno de Petersson**. Si bien no es de el interés de este trabajo formalizar este producto interno, un buen resumen del mismo se puede encontrar en la subsección 1.2.2 de [36]. En particular, se define el producto interno de Petersson en la definición 1.16 de [36].

Por simplicidad, llamemos $T^0(N) = \{T_n : \gcd(n, N) = 1\}$. Tenemos el siguiente teorema:

Teorema **4.8.** *Los operadores de $T^0(N)$ de $\mathcal{S}_k(N, \epsilon_0)$ son normales.*

Demostración. Si $n = p$ primo, entonces la demostración se encuentra en el Teorema 1.18 de [36]. Luego, si tenemos $n \in \mathbb{N}$ coprimo con N, el operador T_n se puede descomponer en sus factores primos debido a su construcción (ver previo al Teorema 4.7) y como cada uno de ellos es normal, su composición es normal, demostrando que los elementos de $T^0(N)$ son normales. □

Utilizando el teorema espectral para operadores normales, tenemos entonces que cada operador de $T^0(N)$ tiene una base ortogonal de vectores propios. Más aún, por el Teorema 4.7, los operadores de $T^0(N)$ conmutan y por lo tanto se diagonalizan simultáneamente, lo que implica que podemos encontrar una base ortogonal de vectores propios para todos los elementos de $T^0(N)$. Utilizaremos la terminología **"forma propia"** en lugar de vector propio a partir de ahora.

Por último, subdividiremos a $\mathcal{S}_k(N, \epsilon_0)$ en una suma directa de dos subespacios, a los que llamaremos formas cuspidales viejas (que denotaremos $\mathcal{S}_k^{old}(N, \epsilon_0)$) y formas cuspidales nuevas (que denotaremos $\mathcal{S}_k^{new}(N, \epsilon_0)$).

Si $M \mid N$, y $\epsilon_0 : (\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{C}$ es un carácter de Dirichlet, entonces ϵ_0 puede ser inducido a un carácter de Dirichlet en $(\mathbb{Z}/N\mathbb{Z})^\times$, simplemente componiendo ϵ_0 con la proyección natural de $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/M\mathbb{Z})^\times$. Por abuso de notación, llamemos ϵ_0 también a este carácter inducido. Entonces, si $M \mid N$, tenemos que $\Gamma_0(N) \subseteq \Gamma_0(M)$ y no es difícil ver tampoco que $\mathcal{S}_k(M, \epsilon_0) \subseteq \mathcal{S}_k(N, \epsilon_0)$.

Esto muestra que hay ciertas formas cuspidales que no son propiamente de nivel N, si no que vienen de un nivel más chico. Es un problema análogo, al que ocurre con los caracteres primitivos.

Existe otra forma de inducir formas cuspidales de un nivel menor que no profundizaremos. Definimos el **subespacio de formas viejas de nivel** N como el subespacio generado por todas las formas cuspidales que provienen de un nivel M que divide a N con $M < N$. Una definición más precisa puede encontrarse en la definición 1.19 en el capítulo 1 de [36].

Definimos el **subespacio de formas nuevas de peso** k **y nivel** N **asociada a** ϵ_0 que denotaremos $\mathcal{S}_k^{new}(N, \epsilon_0)$, como el complemento ortogonal del subespacio anterior con respecto al producto interno de Petersson, es decir,

$$\mathcal{S}_k^{new}(N, \epsilon_0) = (\mathcal{S}_k^{new}(N, \epsilon_0))^\perp.$$

Los subespacios $\mathcal{S}_k^{old}(N, \epsilon_0)$ y $\mathcal{S}_k^{new}(N, \epsilon_0)$ son invariantes por la acción de T_n. Una demostración de esto puede encontrarse en la Proposición 5.6.2 de [12]. Usando esto y el Teorema 4.8, concluimos que los subespacios "old" y "new" tienen una base ortogonal de formas propias de $T^0(N)$. Más aún, si nos restringimos al espacio de formas cuspidales nuevas, encontramos una base ortogonal de formas propias de todos los operadores T_n, es decir, podemos quitar la condición de que $\gcd(n, N) = 1$ como muestra el Teorema 4.10.

Definición **4.9.** *Una forma propia cuspidal nueva se dice* ***normalizada*** *si en su expansión de Fourier* $F(z) = \sum_{n=0}^{\infty} a_n(F) q^n$, *entonces* $a_1(F) = 1$.

El teorema 1.23 de [36] muestra que tal normalización se puede hacer puesto que $a_1(F) \neq 0$ si $F \in \mathcal{S}_k^{new}(N, \epsilon_0)$ no trivial.

Teorema **4.10.** *Si $F \in \mathcal{S}_k^{new}(N, \epsilon_0)$ es una forma propia normalizada de todos los operadores de Hecke $T^0(N)$, entonces $T_n F = a_n(F)F$, $\forall n \in \mathbb{Z}^+$.*

Demostración. Ver Teorema 1.25 de [36] para una demostración. □

Teorema **4.11.** *Si $F \in \mathcal{S}_k^{new}(N, \epsilon_0)$ es una forma propia normalizada de todos los operadores de $T^0(N)$, entonces los $a_n(F)$ son enteros algebraicos para todo $n \geq 0$ y $\mathbb{Q}(\{a_n(F) : n \in \mathbb{Z}^+\})$ es un cuerpo de números.*

Demostración. Ver párrafo posterior a la definición 3.15 de [36]. □

Si $F \in \mathcal{S}_k^{new}(N, \epsilon_0)$ es una forma propia normalizada de todos los operadores de $T^0(N)$, denotaremos K_F al cuerpo de números del Teorema 4.11.

4.2. Formas modulares módulo ℓ

El objetivo es ahora definir formas modulares en $\overline{\mathbb{F}_\ell}$ con ℓ primo impar. La idea es básicamente, reducir los coeficientes de Fourier de una forma modular clásica. La condición de primo impar la agregamos en este documento puesto que no precisaremos el caso de $\ell = 2$, que agrega la condición extra de que k sea par (ver al comienzo de la sección 3 de [43]).

Sea entonces ℓ primo impar, $N \geq 1$ coprimo a ℓ, k entero mayor o igual a 2 y $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}_\ell}^\times$ un carácter de Dirichlet tal que $\epsilon(-1) = (-1)^k$.

La imagen de ϵ es finita porque el dominio es finito, así que existe $r > 0$ tal que $\mathrm{Im}(\epsilon) \subseteq \mathbb{F}_{\ell^r}^\times$. En particular, $(\epsilon(x))^{\ell^r - 1} - 1 = 0$ para todo $x \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Fijemos $x_0 \in (\mathbb{Z}/N\mathbb{Z})^\times$ y consideremos ahora las raíces del polinomio $x^{\ell^r-1} - 1$ en $\overline{\mathbb{Z}}$. En particular, están en $\overline{\mathbb{Z}}_\ell$ y por ende podemos reducir módulo ℓ. Como ℓ es coprimo a $\ell^r - 1$, las raíces del polinomio ciclotómico anterior son todas distintas módulo ℓ, así que sólo una de las raíces coincide módulo ℓ con $\epsilon(x_0)$. Llamemos z a la raíz de $x^{\ell^r-1} - 1$ que coincide con $\epsilon(x_0)$ al reducir y definamos $\epsilon_0(x_0) = z$. Haciendo esto para cada elemento de $(\mathbb{Z}/N\mathbb{Z})^\times$ y utilizando el encaje fijado de $\overline{\mathbb{Z}} \hookrightarrow \mathbb{C}$ al comienzo del capítulo 1, tenemos entonces un levantamiento de ϵ, es decir, un carácter de Dirichlet $\epsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ tal que $\widetilde{\epsilon_0(x)} = \epsilon(x)$ para todo $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, siendo $\widetilde{\cdot} : \overline{\mathbb{Z}}_\ell \to \overline{\mathbb{F}_\ell}$ el mapa reducción.

Hecho esto, estamos en condiciones de definir formas cuspidales para $\mathbb{F}_\ell$.

Definición **4.12.** *Una* ***forma cuspidal*** *de tipo (N, k, ϵ) con coeficientes en $\overline{\mathbb{F}_\ell}$ es una serie formal*

$$f(z) = \sum_{n \geq 1} a_n(f) q^n$$

tal que existe una forma cuspidal clásica F de $\mathcal{S}_k(N, \epsilon_0)$

$$F(z) = \sum_{n \geq 1} a_n(F) q^n$$

con $a_n(F) \in \overline{\mathbb{Z}}$ que cumple que $\widetilde{a_n(F)} = a_n(f)$ para todo $n \geq 1$.

Notar que podemos llegar a encontrar tales formas cuspidales clásicas, como muestra el Teorema 4.11.

De forma análoga al caso de formas modulares clásicas expuestos en la sección anterior, definiremos operadores de Hecke para $\mathcal{S}_k(N, \epsilon)$ en $\overline{\mathbb{F}_\ell}$. Como implica la construcción de los T_n en la sección anterior y el Teorema 4.8, solo es relevante definir los T_p cuando p es primo, ya que a partir de ellos podemos construir todos los operadores de Hecke y alcanza con conocer la acción de estos para tener una base ortonormal de formas propias. Si $f(z) = \sum_{j \geq 1} a_j(f) q^j$, definimos

$$T_p f = \begin{cases} \sum_{j \geq 1} a_{pj}(f) q^j + \epsilon(p) p^{k-1} \sum_{j \geq 1} a_j(f) q^{pj} & \text{si } \ p \nmid \ell N \\ \sum_{j \geq 1} a_{pj}(f) q^j & \text{si } \ p \mid \ell N \end{cases} \tag{4.2}$$

Veamos que la definición de T_p cuando $p \nmid \ell N$ coincide con el Teorema 4.7 cuando $n = p$ primo. En efecto, $\gcd(j, p) = 1$ ó p. Si $\gcd(j, p) = 1$, $a_j(T_p F) = a_{jp}(F)$ que se corresponde a los términos de la primer sumatoria en la ecuación (4.2). Si $\gcd(j, p) = p$ entonces $a_j(T_p F) = a_{jp}(F) + p^{k-1} \epsilon_0(p) a_{j/p}(F)$ y entonces el primer término es parte de la primer sumatoria en la ecuación (4.2), mientras que el segundo término solo aparece en múltiplos de p y es el segundo término en la ecuación (4.2) con el cambio de variable $j \mapsto pj$.

Si observamos, el caso $p \mid \ell N$ es coherente con el caso anterior, ya que el segundo término desaparece debido a que $\epsilon(p) p^{k-1} \equiv 0 \pmod{\ell}$ si $k \geq 2$.

Debido a esta compatibilidad con el caso de formas modulares clásicas, tenemos que si f es una forma propia normalizada de los operadores de Hecke anteriores, entonces $T_p(f) = a_p(f) f$ para todo p primo, por el Teorema 4.10.

4.3. Representaciones de formas modulares

Veamos que podemos asociar una representación de Galois a una forma modular. Esto sin embargo es muy complicado de hacer en toda su generalidad, y solo lo haremos sin demostrar todos los teoremas, en el caso más sencillo que es cuando $k = 2$.

Sea f una forma propia nueva normalizada de $\mathcal{S}_2(N, \epsilon)$ en $\overline{\mathbb{F}_\ell}$. Por definición, existe F una forma propia nueva normalizada clásica de $\mathcal{S}_2(N, \epsilon_0)$ tal que f se obtiene reduciendo los coeficientes $a_j(F) \pmod{\ell}$. A partir de F podemos construir

una variedad abeliana A_F sobre $\mathbb{Q}$. Una explicación de esto se puede encontrar en la sección 3.4 de [36], aunque la prueba de que A_F es definida sobre $\mathbb{Q}$ se puede encontrar en el Teorema 5.23 de [35]. Como las variedades abelianas son variedades algebraicas proyectivas con una estructura de grupo en sus puntos, el objetivo es utilizar su ℓ^n-torsión para construir la representación de Galois.

Si $K_F = \mathbb{Q}$, entonces A_F es una curva elíptica, y la representación de Galois de F se construye como en el caso de curvas elípticas (ver definición 3.10) utilizando la ℓ-torsión. En el caso general, A_F es una variedad abeliana de dimensión $2[K_F : \mathbb{Q}]$, por lo que un procedimiento similar a la definición 3.10 daría como resultado una representación de dimensión $2[K_F : \mathbb{Q}]$. Veamos sin demostrar los detalles, como se logra construir una representación de dimensión 2.

Sea $A_F[\ell^n]$ el conjunto de los puntos de ℓ^n-torsión de A_F. No es difícil ver que en cualquier variedad abeliana, el mapa $[\ell] : A_F[\ell^n] \to A_F[\ell^{n-1}]$ está bien definido, y permite generar un sistema inverso. Definimos

$$\mathrm{Ta}_\ell(A_F) = \varprojlim A_F[\ell^n]$$

que es conocido como el **módulo de Tate** de una variedad abeliana.

Teorema **4.13.** *Sea F una forma propia nueva normalizada de $\mathcal{S}_2(N, \epsilon_0)$ y $V_\ell(A_F) = \mathrm{Ta}_\ell(A_F) \otimes \mathbb{Q}$. Entonces $V_\ell(A_F)$ es un módulo libre de rango 2 sobre $K_F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.*

Demostración. Ver lema 9.5.3 de [12]. □

Con $V_\ell(A_F)$ un módulo de rango 2 sobre $K_F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \prod_{\mathfrak{l}|\ell} K_{F,\mathfrak{l}}$, siendo $\mathfrak{l}$ primos en $\mathcal{O}_{K_F}$ y $K_{F,\mathfrak{l}}$ la localización de K con respecto al primo $\mathfrak{l}$, sí podemos obtener una representación de dimensión 2 $\rho_{F,\mathfrak{l}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{F,\mathfrak{l}})$ como es explicado en la página 383 de [12].

Nuestro objetivo ahora es reducir los coeficientes de las matrices de $\mathrm{GL}_2(K_{F,\mathfrak{l}})$. Sin embargo, los coeficientes no necesariamente están en el anillo. Es necesario para eso el siguiente teorema:

Teorema **4.14.** *Sean d entero positivo, ℓ primo, K un cuerpo de números, L una extensión finita de $\mathbb{Q}_\ell$, R_L el anillo de enteros de L y $\rho : G_K \to \mathrm{GL}_d(L)$ una representación ℓ-ádica continua. Entonces existe $\rho' : G_K \to \mathrm{GL}_d(R_L)$ tal que $\rho \sim \rho'$.*

Demostración. Escribamos $V = L^d$ y $\Lambda = R_L^d$. Por la proposición 7.46 de [30], tenemos que R_L es compacto y por lo tanto Λ es compacto. Por otro lado, R_L es un dominio de factorización única (porque es un dominio local donde su único ideal maximal es principal generado por el uniformizador), lo que implica que Λ es un retículo de V puesto que tiene rango al menos d como R_L-módulo.

El Teorema 5.4.15 de [50] muestra que G_K es compacto, y como Λ también es compacto y ρ es continua, entonces $\rho(G_K \times \Lambda) = \Lambda'$ es compacto. Como L^d es un espacio métrico, que Λ' sea compacto, implica que es acotado, y entonces $\nu(w) \geq -r$ para todo $w \in \Lambda'$, donde[8] $\nu(w) = \text{mín}\,\{\nu(w_i) : i = 1, ..., d\}$ con $w = (w_1, ..., w_d)$ y $r \geq 0$. Como Λ es el retículo de los vectores con valuación no negativa, $\Lambda' \subseteq \pi^{-r}\Lambda$, siendo π el uniformizador de R_L.

A su vez, $\Lambda' = \bigcup_{g \in G_K} \rho(g)\Lambda$, así que $\Lambda \subseteq \Lambda'$ y entonces Λ' tiene rango al menos d. Usando nuevamente que R_L es un dominio de factorización única, obtenemos que Λ' tiene rango d y es por lo tanto un retículo en V.

Por su definición, es claro que Λ' es un retículo estable bajo G_K. Esto implica que la acción de G_K en Λ' genera matrices en $GL_d(R_L)$ y como Λ' es un retículo, su base es base de V, así que para cada elemento de G_K, en la base de Λ' obtenemos $\rho'(g) \in \mathrm{GL}_d(R_L)$. Las representaciones ρ y ρ' son conjugadas porque son obtenidas por un cambio de base entre una base de V y la base del retículo Λ'. □

Utilizando el Teorema 4.14 para $K = \mathbb{Q}$, $L = K_{F,\mathfrak{l}}$ y $\rho = \rho_{F,\mathfrak{l}}$, podemos entonces reducir una representación conjugada a $\rho_{F,\mathfrak{l}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{F,\mathfrak{l}})$ con coeficientes en su anillo de enteros para obtener una representación módulo ℓ. Llamaremos $\rho_F : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ a la semisimplificación de la representación módulo ℓ. Esta representación obtenida queda definida a menos de conjugación, incluso si cambiamos el primo $\mathfrak{l}$ que divide a ℓ en K_F. Destacamos su propiedad más importante en el siguiente teorema:

Teorema **4.15.** *Sea ρ_F la representación de Galois asociada a F forma propia nueva normalizada de $\mathcal{S}_2(N, \epsilon_0)$. Entonces la representación es no ramificada para primos $p \nmid \ell N$ y en estos primos donde no ramifica,* $\mathrm{tr}(\rho_F(\mathrm{Frob}_p)) = a_p(F) \pmod{\ell}$ *y* $\det(\rho_F(\mathrm{Frob}_p)) = \epsilon(p)\chi_\ell(p)$.

Demostración. Ver Teorema 9.5.4 de [12]. □

Esto muestra que la representación que cumple el Teorema 4.15 es única (salvo conjugación) por el Teorema 2.15, puesto que el conjunto de primos que dividen a ℓN son una cantidad finita y ρ_F es semisimple.

Ahora sí, estamos en condiciones de definir las representaciones de Galois para formas modulares módulo ℓ.

Definición **4.16.** *Sea f una forma propia nueva normalizada de $\mathcal{S}_2(N, \epsilon)$ en $\overline{\mathbb{F}_\ell}$. Definimos la* ***representación de Galois asociada a*** *f que denotaremos ρ_f como $\rho_f = \rho_F$ siendo F un levantamiento de f por el mapa reducción módulo ℓ.*

[8] en la valuación para los vectores de L^d se toma mínimo porque permite medir el denominador más grande en las coordenadas de w.

Esta definición no depende del levantamiento elegido, puesto que si F' es otro levantamiento de f, entonces $a_p(F) \equiv a_p(F')$ (mód ℓ) para todo primo $p \nmid \ell N$ y por lo tanto por el Teorema 4.15,

$$\mathrm{tr}(\rho_F(\mathrm{Frob}_p)) \equiv a_p(F) \pmod{\ell} \equiv a_p(F') \pmod{\ell} \equiv \mathrm{tr}(\rho_{F'}(\mathrm{Frob}_p))$$

y

$$\det(\rho_F(\mathrm{Frob}_p)) = \chi_\ell(p) = \det(\rho_{F'}(\mathrm{Frob}_p))$$

Luego $\rho_F = \rho_{F'}$ por el Teorema 2.15.

Si el peso no es 2, también se puede asociar una representación pero la construcción es más complicada. Resumimos en el siguiente teorema la existencia de la representación de Galois para cualquier peso:

Teorema **4.17.** *(Deligne, Serre, 1974). Sea $f(z) = \sum_{n\geq 1} a_n(f)q^n$ una forma propia nueva normalizada de $\mathcal{S}_k(N,\epsilon)$ en $\overline{\mathbb{F}_\ell}$. Entonces existe una representación de Galois*

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$$

tal que en los primos $p \nmid \ell N$, la representación ρ_f no ramifica, y en estos primos donde no ramifica, $\mathrm{tr}(\rho_f(\mathrm{Frob}_p)) = a_p(f)$ *y* $\det(\rho_f(\mathrm{Frob}_p)) = \epsilon\chi_\ell^{k-1}(p)$.

Demostración. Ver Teorema 6.7 de [11]. □

Capítulo 5

Conjetura de Serre

La Conjetura de Serre fue expuesta por Jean Pierre Serre en 1987 en el artículo [43]. He aquí su enunciado:

> (Conjetura de Serre) Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ una representación de Galois impar e irreducible. Entonces ρ es equivalente a ρ_f, con ρ_f una representación que proviene de una forma propia nueva normalizada f de $\mathcal{S}_k(N, \epsilon)$ para cierto nivel N, peso k y carácter ϵ que depende de la representación ρ.

A lo largo de este capítulo, nos dedicaremos a precisar cómo conocer el nivel, peso y carácter de la forma cuspidal que menciona la conjetura. El nivel y carácter lo haremos en la sección 5.1 que es más sencillo que el peso, al que le dedicaremos toda la sección 5.2.

Además de exponer su conjetura, en [43], Serre da siete aplicaciones de la misma. En este documento mostraremos dos de ellas. La primera es el Último Teorema de Fermat. El enunciado de este teorema y las ideas de su demostración utilizando la Conjetura de Serre ya fueron presentadas en la introducción. Aquí seremos más precisos con los argumentos. La segunda aplicación nos servirá de puntapié para el capítulo 6, puesto que en este capítulo, en la sección 5.4, usaremos la Conjetura de Serre para estudiar las curvas elípticas de conductor primo sobre $\mathbb{Q}$ y en el capítulo siguiente haremos lo mismo pero para curvas elípticas sobre cuerpos cuadráticos reales.

Como mencionábamos en la introducción, la Conjetura de Serre fue demostrada en 2009 por los trabajos de Chandrashekhar Khare y Jean-Pierre Wintenberger (ver [20], [21] y [22]).

En este capítulo no dejaremos referencias de lectura recomendadas, puesto que el sentido de los capítulos anteriores de este documento era justamente exponer los resultados necesarios para utilizarlos aquí.

5.1. Definición de N y ϵ

Sea ℓ primo racional y $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ una representación de Galois como en la definición 2.12. Consideremos el carácter $\det(\rho)$. Por el teorema 2.26, $\det(\rho)$ factoriza por una extensión ciclotómica $\mathbb{Q}(\xi_n)$ donde $n = \ell N_{\det\rho}$ y $\gcd(\ell, N_{\det\rho}) = 1$. Tomaremos $N = N_{\det\rho}$. Como $\mathrm{Gal}(\mathbb{Q}(\xi_n/\mathbb{Q})) \simeq (\mathbb{Z}/\ell N\mathbb{Z})^\times \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$ (esto último por el Teorema Chino de los restos), podemos descomponer a $\det\rho$ en dos caracteres $\varphi : (\mathbb{Z}/\ell\mathbb{Z})^\times \to \overline{\mathbb{F}_\ell}^\times$ y $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}_\ell}^\times$ tales que

$$\det\rho = \epsilon\varphi. \tag{5.1}$$

Como $(\mathbb{Z}/\ell\mathbb{Z})^\times$ es cíclico de orden $\ell-1$, entonces $\varphi(x) = x^h$ con $h \in \mathbb{Z}/(\ell-1)\mathbb{Z}$, y por lo tanto $\varphi = \chi_\ell^h$ siendo $\chi_\ell : G_{\mathbb{Q}} \to \overline{\mathbb{F}_\ell}$ el carácter ciclotómico definido en la sección 2.3.

Definición **5.1.** *Escribamos $c \in \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ a la conjugación compleja. Como c tiene orden 2, entonces $\det\rho(c) = \pm 1$. Diremos que la representación ρ es* ***impar*** *si $\det\rho(c) = -1$.*

A partir de ahora nos ocuparemos de representaciones impares. Observar que si $\ell = 2$ todas las representaciones son impares puesto que $-1 \equiv 1 \mod 2$.

Si $\ell \neq 2$, entonces $\rho(c)$ es conjugada a $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Esto último es porque $\rho(c)$ es conjugada a su forma canónica de Jordan, que si no fuera diagonal no tendría orden 2 porque $\ell \neq 2$ y si es diagonal, sus elementos en la diagonal tienen que ser elementos de orden 2 en $\overline{\mathbb{F}_\ell}$. Luego cada uno es 1 o -1, pero como la representación es impar, tiene que ser uno de cada signo.

5.2. Definición de k

La definición de k va a depender según la acción de $I_{\ell,t}$. Consideremos ρ_ℓ definido igual que en el párrafo siguiente al diagrama 2.1.

Consideremos ρ_ℓ^{ss} la semisimplificación de ρ_ℓ. Como es semisimple, por el teorema 2.23, podemos factorizar $\rho_\ell^{ss}|_{I_\ell}$ a $\rho_\ell^{ss} : I_{\ell,t} \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$. La semisimplificación tiene dos caracteres $\varphi, \varphi' : I_t \to \overline{\mathbb{F}_\ell}^\times$ tales que

$$\rho_\ell^{ss} = \begin{pmatrix} \varphi & 0 \\ 0 & \varphi' \end{pmatrix}.$$

Teorema **5.2.** *φ y φ' tienen nivel 1 ó 2. Si tienen nivel 2, entonces $\varphi' \neq \varphi$, $\varphi' = \varphi^\ell$ y $\varphi = \varphi'^\ell$.*

Demostración. Por el teorema 1.12, tenemos que cualquier preimagen del mapa de Frobenius s actuando en $I_{\ell,t}$ por conjugación es lo mismo que componer ℓ veces. Entonces

$$\rho_\ell^{ss}(s\sigma s^{-1}) = \rho_\ell^{ss}(\sigma^\ell) = \rho_\ell^{ss}(\sigma)^\ell,$$

lo que implica que

$$\begin{pmatrix} \varphi & 0 \\ 0 & \varphi' \end{pmatrix} \sim \begin{pmatrix} \varphi & 0 \\ 0 & \varphi' \end{pmatrix}^\ell$$

donde con $\sim$ nos referimos a que son conjugadas como matrices.

Las opciones son $\varphi = \varphi^\ell$ y $\varphi' = \varphi'^\ell$ lo que implican que ambos tienen nivel 1, ó $\varphi = \varphi'^\ell$ y $\varphi' = \varphi^\ell$ que sustituyendo una ecuación implica que ambas tienen nivel 2 si son distintas. □

Separamos nuestra discusión según las dos opciones del teorema 5.2.

5.2.1. Cuando φ y φ' tienen nivel 2

Si tienen nivel 2, entonces ρ_ℓ como representación de $G_{\mathbb{Q}_\ell}$ es irreducible. En efecto, si no lo fuera tendría un subespacio W de dimensión 1 y una subrepresentación ρ'_ℓ de dimensión 1. Si aplicamos el Teorema de Jordan-Holder usando a W como parte de la filtración y restringimos a I_t y a ρ_ℓ^{ss}, obtenemos que ρ'_ℓ es una de φ o φ'. Pero entonces ρ'_ℓ es de nivel 1 pero tanto φ como φ' tienen nivel 2.

Dado el teorema 2.27, y la definición de caracteres fundamentales de nivel 2, tenemos que

$$\varphi = \theta_{\ell^2-1}^{a+\ell b}$$

con $0 \leq a, b \leq \ell - 1$. Para simplificar la notación, escribamos $\theta = \theta_{\ell^2-1}$. Observar que $a \neq b$, puesto que si $a = b$, entonces $\varphi = (\theta\theta^\ell)^a = \chi_\ell^a$ por ecuación (2.1), pero esto no puede ser porque χ_ℓ tiene tiene nivel 1.

Cambiando los roles de φ y φ' si es necesario (a través de un cambio de base en la representación), podemos asumir que $0 \leq a < b \leq \ell - 1$. La representación tiene entonces esta forma:

$$\rho_\ell^{ss} = \begin{pmatrix} \theta^{a+\ell b} & 0 \\ 0 & \theta^{b+\ell a} \end{pmatrix}$$

Para este caso, definimos

$$\boxed{k = 1 + \ell a + b.}$$

5.2.2. Cuando φ y φ' tienen nivel 1 y P_ℓ actúa trivial

Como el espacio de caracteres de nivel 1 está generado por el carácter ciclotómico que tiene orden $\ell - 1$, tenemos que $\varphi = \chi_\ell^a$ y que $\varphi' = \chi_\ell^b$ y cambiando roles si es necesario podemos asumir que $0 \leq a \leq b \leq \ell - 2$. Como P_ℓ actúa trivial, es semisimple, y por lo tanto la representación tiene esta forma:

$$\rho_\ell = \begin{pmatrix} \chi_\ell^a & 0 \\ 0 & \chi_\ell^b \end{pmatrix}$$

La definición de k en este caso es

$$\boxed{k = \begin{cases} 1 + \ell a + b & \text{si } (a,b) \neq (0,0) \\ \ell & \text{si } (a,b) = (0,0) \end{cases}}$$

5.2.3. Cuando P_ℓ no actúa trivialmente

Veamos que en este caso $\dim(V^{P_\ell}) = 1$. En efecto, 0 no puede ser por el Teorema 2.22 y 2 tampoco porque P_ℓ no actúa trivialmente. Como P_ℓ es normal en $G_\mathbb{Q}$ por el Teorema 1.10, el subespacio V^{P_ℓ} es estable bajo la acción de $G_\mathbb{Q}$ (ver ejemplo 2.4) y por ende, también lo es V/V^{P_ℓ}, lo que implica que ρ actúa como

$$\rho = \begin{pmatrix} \theta_2 & * \\ 0 & \theta_1 \end{pmatrix}$$

Si consideramos la semisimplificación y nos restringimos a $I_{\ell,t}$, nos queda

$$\rho_\ell^{ss} = \begin{pmatrix} \theta_2 & 0 \\ 0 & \theta_1 \end{pmatrix}.$$

Por el Teorema 2.23, obtenemos que $\theta_i(P_\ell) = 1$ con $i = 1, 2$, y por ende los caracteres θ_1, θ_2 quedan bien definidos en $I_{\ell,t}$. Sea $\sigma \in I_\ell$ y s una preimagen del automorfismo de Frobenius. El teorema 1.12, nos da entonces que $\theta_i(\sigma) = \theta_i(s\sigma s^{-1}) = \theta_i(\sigma)^\ell$ en $I_{\ell,t}$ para $i = 1, 2$, lo que demuestra que los caracteres θ_1, θ_2 tienen nivel 1 por teorema 2.30 y por lo tanto, son una potencia del carácter ciclotómico, es decir, $\theta_i \mid_{I_t} = \chi_\ell^{\alpha_i}$ con $\alpha_i \in \mathbb{Z}/(\ell - 1)\mathbb{Z}$ con $i = 1, 2$. De esta forma $\theta_i \chi_\ell^{-\alpha_i}$ es un carácter trivial en I_ℓ al que llamaremos ϵ_i y de esta forma concluimos que

$$\rho_\ell = \begin{pmatrix} \chi_\ell^{\alpha_2}\epsilon_2 & * \\ 0 & \chi_\ell^{\alpha_1}\epsilon_1 \end{pmatrix}$$

donde entonces, $\epsilon_i(I_\ell) = 1$ con $i = 1, 2$.

Normalicemos $0 \leq \alpha_1 \leq \ell - 2$ y $1 \leq \alpha_2 \leq \ell - 1$ y definamos $a = \text{mín}\{\alpha_1, \alpha_2\}$ y $b = \text{máx}\{\alpha_1, \alpha_2\}$. Separamos en dos casos:

1. **Si** $\alpha_2 \neq \alpha_1 + 1$ tomamos

$$\boxed{k = 1 + \ell a + b.}$$

2. **Si** $\alpha_2 = \alpha_1 + 1$ la definición de k va a depender de la ramificación salvaje. Para entender la distinción definamos primero $K = (\overline{K})^{\ker(\rho_\ell|_{I_\ell})}$. Entonces $\mathrm{Gal}(K/\mathbb{Q}_\ell^{nr}) \simeq \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell^{nr})/\mathrm{Gal}(\overline{\mathbb{Q}_\ell}/K) = I_\ell/\ker(\rho_\ell\mid_{I_\ell}) \simeq \rho_\ell(I_\ell)$. Como $\rho_\ell(P_\ell)$ es un subgrupo de $\rho_\ell(I_\ell)$, definimos $K_t = K^{\rho_\ell(P_\ell)}$. Como $\rho_\ell(P_\ell)$ es un ℓ-Sylow dentro de $\rho_\ell(I_\ell)$, K_t es la extensión moderada más grande dentro de K, lo que implica que $K_t = K \cap \mathbb{Q}_\ell^t$. Como $P_\ell \lhd I_\ell$ por el teorema 1.10, entonces $\rho_\ell(P_\ell) \lhd \rho_\ell(I_\ell)$ y de forma análoga tenemos que $\mathrm{Gal}(K_t/\mathbb{Q}_\ell^{nr}) \simeq \rho_\ell(I_\ell)/\rho_\ell(P_\ell)$. El diagrama de extensiones queda como se muestra en la figura 5.1 :

$$\begin{tikzcd}
 & \overline{\mathbb{Q}_\ell} \arrow[d, dash, "\ker(\rho_\ell\mid_{I_\ell})"] \\
 & K \arrow[d, dash, "\rho_\ell(P_\ell)"] \\
\rho_\ell(I_\ell) & K_t \arrow[d, dash, "\rho_\ell(I_\ell)/\rho_\ell(P_\ell)"] \\
 & \mathbb{Q}_\ell^{nr}
\end{tikzcd}$$

Figura 5.1: Diagrama de extensiones para el caso en el que la acción de P_ℓ es no trivial.

Del hecho de que $\epsilon_i(I_\ell) = 1$ para $i = 1, 2$, del teorema 2.25 y de que $\alpha_2 = \alpha_1 + 1$, tenemos que

$$\rho_\ell(I_\ell) = \left\{ \begin{pmatrix} x^{\alpha_1+1} & * \\ 0 & x^{\alpha_1} \end{pmatrix} : x \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\}$$

$$\rho_\ell(P_\ell) = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} : x \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\}$$

Consideremos el mapa $\rho_\ell(I_\ell) \to (\mathbb{Z}/\ell\mathbb{Z})^\times$ que manda $\begin{pmatrix} x^{\alpha_1+1} & * \\ 0 & x^{\alpha_1} \end{pmatrix} \mapsto x^{\alpha_1+1}/x^{\alpha_1}$, es decir, que divide los elementos de la diagonal. Es fácil chequear que es un homomorfismo sobreyectivo de grupos cuyo núcleo es $\rho_\ell(P_\ell)$. Por lo tanto, $\mathrm{Gal}(K_t/\mathbb{Q}_\ell^{nr}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times$.

Como $\rho_\ell(I_\ell)$ es un grupo finito, la extensión $K/\mathbb{Q}_\ell^{nr}$ es finita y por lo tanto $K_t/\mathbb{Q}_\ell^{nr}$ es una extensión finita. Como observamos antes, K_t es un subcuerpo de $\mathbb{Q}_\ell^t$, así que usando el teorema 1.11, tenemos que $K_t \subseteq K_d$ para algún

d. Más aún, como tenemos que $\mathrm{Gal}(K_t/\mathbb{Q}_\ell^{nr}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times$, concluimos que $K_t = \mathbb{Q}_\ell^{nr}(\xi_\ell)$ por el teorema 1.28.

Por otro lado, los elementos de $\rho_\ell(P_\ell)$ tienen orden ℓ (puesto que $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)^\ell = \left(\begin{smallmatrix} 1 & \ell* \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ porque la característica es ℓ) y como el grupo es finito, entonces

$$\rho_\ell(P_\ell) = \prod_J (\mathbb{Z}/\ell\mathbb{Z})$$

donde J es un conjunto finito (pongamos $m = |J|$). En particular es abeliano.

Esto último nos permite considerar una acción $\rho_\ell(I_\ell)/\rho_\ell(P_\ell) \curvearrowright \rho_\ell(P_\ell)$ dada por $(g\rho_\ell(P_\ell)).u = gug^{-1}$. Esta bien definida puesto que si $h \in \rho_\ell(P_\ell)$ entonces $(gh\rho_\ell(P_\ell)).u = g(huh)^{-1}g^{-1} = gug^{-1}$ donde en esta última igualdad usamos el hecho de que $hu = uh$. Si somos más precisos, que $g \in \rho_\ell(I_\ell)$ implica que $g = \begin{pmatrix} x^{\alpha_1+1} & c \\ 0 & x^{\alpha_1} \end{pmatrix}$ y que $u \in \rho_\ell(P_\ell)$ implica que $u = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}$ donde $c, d \in \overline{\mathbb{F}_\ell}$. Entonces

$$gug^{-1} = \begin{pmatrix} 1 & dx \\ 0 & 1 \end{pmatrix} \tag{5.2}$$

Del hecho de que $\rho_\ell(P_\ell)$ es isomorfo al grupo $\prod_J(\mathbb{Z}/\ell\mathbb{Z})$ aditivo, y que $\rho_\ell(I_\ell)/\rho_\ell(P_\ell) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times$, la ecuación (5.2) se transforma en siguiente acción de $(\mathbb{Z}/\ell\mathbb{Z})^\times \curvearrowright \prod_J(\mathbb{Z}/\ell\mathbb{Z})$ dada por

$$x.(g_1, ..., g_m) = (g_1^x, ..., g_m^x)$$

Usando el teorema 1.28, obtenemos que

$$K = K_t(x_1^{1/\ell}, ..., x_m^{1/\ell})$$

con $x_i \in (\mathbb{Q}_\ell^{nr})^\times/(\mathbb{Q}_\ell^{nr})^{\times\ell}$ para cada $i = 1, ..., m$. Si bien en principio los elementos son de K_t, se pueden tomar en $(\mathbb{Q}_\ell^{nr})^\times$, puesto que podemos multiplicar todos sus conjugados por el grupo $\mathrm{Gal}(K_t/\mathbb{Q}_\ell^{nr})$.

Como observamos en la sección 1.1 posterior a la definición 1.4, tenemos que $\mathrm{Im}(v_{\mathbb{Q}_\ell}) = \mathrm{Im}(v_{\mathbb{Q}_\ell^{nr}}) = \mathbb{Z}$. Escribiremos v_ℓ a la valuación ℓ-ádica. Separamos este caso en dos casos más:

a) Decimos que la representación es **poco ramificada** si

$$v_\ell(x_i) \equiv 0 \mod \ell$$

para todo $i = 1, ..., m$.

Hipótesis del caso	**Forma de la representación**	**Valor de k**	**Condiciones de a y b**
φ, φ' nivel 2	$\rho_\ell^{ss}\mid_{I_{\ell,t}}=\begin{pmatrix}\theta^{a+\ell b} & 0\\ 0 & \theta^{b+\ell a}\end{pmatrix}$	$k=1+\ell a+b$	$0\leq a<b\leq \ell-1$
φ, φ' nivel 1, P_ℓ actúa trivialmente	$\rho_\ell^{ss}\mid_{I_{\ell,t}}=\begin{pmatrix}\chi_\ell^{a} & 0\\ 0 & \chi_\ell^{b}\end{pmatrix}$	$k=\begin{cases}1+\ell a+b & (a,b)\neq(0,0)\\ \ell & (a,b)=(0,0)\end{cases}$	$0\leq a\leq b\leq \ell-2$
P_ℓ actúa no trivial	$\rho_\ell=\begin{pmatrix}\chi_\ell^{\alpha_2}\epsilon_2 & *\\ 0 & \chi_\ell^{\alpha_1}\epsilon_1\end{pmatrix}$	$k=\begin{cases}1+\ell a+b & \text{si } \alpha_2\neq\alpha_1+1 \text{ o } \alpha_2=\alpha_1+1 \text{ poco ramificada}\\ \ell(a+1)+b & \text{si } \alpha_2=\alpha_1+1 \text{ muy ramificada } \ell\neq 2\\ 4 & \text{si } \alpha_2=\alpha_1+1 \text{ muy ramificada } \ell=2\end{cases}$	$0\leq\alpha_1\leq\ell-2$ $1\leq\alpha_2\leq\ell-1$ $a=\text{mín}\{\alpha_1,\alpha_2\}$ $b=\text{máx}\{\alpha_1,\alpha_2\}$

Tabla 5.1: Resumen de los valores de k según la representación.

b) Decimos que la representación es **muy ramificada** si no es poco ramificada.

Antes de definir los valores de k para cada caso, hagamos algunas observaciones.

Si estamos en el caso de representación poco ramificada, podemos tomar los x_i en $\mathbb{Z}_\ell^\times$. En efecto, como los x_i se toman módulo $(\mathbb{Q}_\ell^{nr})^{\times\ell}$, si $v_\ell(x_i)=\ell a$, entonces $v_\ell(x_i(\ell^{-a})^\ell)=0$ y $x_i(\ell^{-a})^\ell$ es otro representante de x_i módulo $(\mathbb{Q}_\ell^{nr})^{\times\ell}$.

Si la representación es poco ramificada definimos

$$\boxed{k=1+\ell a+b=2+\alpha_1(\ell+1)}$$

Si la representación es muy ramificada definimos

$$\boxed{k=\begin{cases}\ell(a+1)+b=(\alpha_1+1)(\ell+1) & \text{si } \ell\neq 2\\ 4 & \text{si } \ell=2\end{cases}}$$

La diferencia con el caso poco ramificado es que sumamos $\ell-1$ si $\ell\neq 2$ y un término 2 si $\ell=2$.

Resumimos en la tabla 5.1 los valores de k según el caso:

5.2.4. Algunas propiedades de k

Teorema **5.3.** *Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ una representación impar. Entonces*

$$\det(\rho)\mid_{I_\ell} = \chi_\ell^{k-1}.$$

Demostración. Hay que chequear cada caso de las definiciones de k dada. Veamos el primer caso de la tabla 5.1 a modo de ejemplo.

En este caso, por la ecuación (2.1), tenemos que $\theta^{\ell+1} = \chi_\ell$. Entonces

$$\det(\rho)\mid_{I_\ell} = \theta^{a+\ell b}\theta^{b+\ell a} = \theta^{(\ell+1)(a+b)} = \chi_\ell^{a+b}.$$

Ahora $k-1 = \ell a + b \equiv a + b \pmod{\ell - 1}$.

El resto de los casos se hacen de la misma forma. □

Teorema **5.4.** *Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ una representación de Galois impar. Entonces $k = 2$ si y solo si $\det\rho\mid_{I_\ell} = \chi_\ell$ y ρ es finita en ℓ.*

Demostración. Ver proposición 4 de [43]. □

Teorema **5.5.** *Sea $E/\mathbb{Q}$ una curva elíptica, ℓ primo y $\rho_{E,\ell}$ la representación de Galois asociada a la curva elíptica.*

1. *Si E tiene buena reducción en ℓ entonces $k = 2$*
2. *Si E tiene reducción multiplicativa en ℓ, entonces*

$$k = \begin{cases} 2 & si \;\; \ell \mid \nu_\ell(\Delta^{min}(E)), \\ \ell + 1 & si \; \ell \nmid \nu_\ell(\Delta^{min}(E)) \; y \; \ell \neq 2 \\ 4 & si \; \ell \nmid \nu_\ell(\Delta^{min}(E)) \; y \; \ell = 2 \end{cases}$$

Demostración. 1. Si E tiene buena reducción en ℓ, ρ es finita en ℓ, así que por los teoremas 5.4 y 3.12, concluimos que $k = 2$.

2. En reducción multiplicativa, como en el teorema 3.29, tenemos que

$$E[\ell] \simeq \left\langle \xi_\ell, q^{1/\ell} \right\rangle / q^{\mathbb{Z}}$$

con acción de Galois compatible.

Como $\sigma(\xi_\ell) = \xi_\ell^{\chi_\ell(\sigma)}$ y $\sigma(q^{1/\ell}) = \xi_\ell^* q^{1/\ell}$, donde desconocemos el exponente que corresponde pero tampoco es importante, tenemos que

$$\rho_{E,\ell} \simeq \begin{pmatrix} \chi_\ell & * \\ 0 & 1 \end{pmatrix}.$$

Notar que la forma de $\rho_{E,\ell}$ se corresponde con el último caso de la tabla 5.1, con $\epsilon_1 = \epsilon_2 = 1$ y $\alpha_2 = \alpha_1 + 1 = 1$, por lo que debemos distinguir según si la representación es poco ramificada o muy ramificada. Para ellos vemos quienes son en este caso los cuerpos K y K_t del diagrama 5.1. En efecto, $K = \mathrm{Fix}(\ker(\rho\,|_{I_\ell})) = \mathbb{Q}_\ell^{nr}(E[\ell]) = \mathbb{Q}_\ell^{nr}(\xi_\ell, q^{1/\ell})$. Lo estudiado en la sección 5.2.3, muestra que $K_t = \mathbb{Q}_\ell^{nr}(\xi_\ell)$, y entonces el hecho de que la extensión sea poco ramificada o no depende de $\nu_\ell(q)$, que por la ecuación (3.5), es igual a $\nu_\ell(\Delta^{min}(E))$.

Si es poco ramificado, entonces $\ell \mid \nu_\ell(\Delta^{min}(E))$ y como $(a, b) = (1, 0)$ de la tabla 5.1, entonces $k = 2$ en este caso. Si es muy ramificado, entonces $\ell \nmid \nu_\ell(\Delta^{min}(E))$ y como $(a, b) = (1, 0)$, entonces $k = \ell + 1$ si $\ell \neq 2$ y $k = 4$ si $\ell = 2$, dando el resultado. □

5.3. Aplicación: Último Teorema de Fermat

La Conjetura de Serre, ofrece una solución alternativa y rápida al "Último Teorema de Fermat" como explicamos en la introducción. En esta sección, volvemos a explicar el argumento pero siendo más precisos en los detalles, y utilizando los teoremas que fuimos mencionando y/o deduciendo a lo largo del documento.

Recordemos que

Teorema **5.6.** *(Último Teorema de Fermat, Wiles, 1995) Si $n > 2$ entero, y existen enteros a, b, c tales que*

$$a^n + b^n = c^n, \tag{5.3}$$

entonces $abc = 0$.

El caso $n = 3$ fue demostrado por Leonard Euler en 1753 y el caso $n = 4$ lo hizo el propio Pierre de Fermat aproximadamente en el año 1670. Una demostración elemental del caso $n = 4$ se puede encontrar en el teorema 2C, cáp. 1, sec. 2 de [38] y una demostración del caso $n = 3$ en el teorema 4A, cáp. 1, sec. 4 del mismo libro.

Por lo tanto si $n \geq 5$, tenemos tres opciones: o $3 \mid n$, o $4 \mid n$, o existe un primo $\ell \geq 5$ tal que $\ell \mid n$. En los primeros dos casos, $n = \alpha n'$ siendo $\alpha = 3, 4$, así que si existiese una solución $(a, b, c) \in \mathbb{Z}^3$ con todos no nulos para n, entonces $(a^{n'}, b^{n'}, c^{n'})$ es solución entera con todos no nulos para 3 o 4, que ya sabemos que no existe. En el tercer caso, $n = n'\ell$, y el mismo argumento que antes, nos lleva a tener una solución entera con todos no nulos para ℓ. Con esta observación, alcanza con probar el teorema 5.6 para cuando n es primo mayor o igual a 5.

Supongamos que tenemos (a, b, c) una solución de enteros no nulos para algún primo ℓ mayor o igual a 5. Por ser (5.3) una ecuación homogénea, se pueden tomar (a, b, c) coprimos. Es claro que uno de ellos debe ser par (pongamos b) y como son coprimos, los otros dos deben ser impares. Para simplificar la notación, denotemos

$(A, B, C) = (a^\ell, b^\ell, c^\ell)$.

Consideremos la curva elíptica

$$E : y^2 = x(x + A)(x - B).$$

Entonces E es una curva elíptica definida sobre $\mathbb{Q}$ en la cual,

1. $\Delta^{min}(E) = 2^{-8}A^2B^2C^2$,
2. $N(E) = \mathrm{rad}(ABC)$, es decir,
3. E tiene reducción multiplicativa en todos los primos que dividen al discriminante.

Tener en cuenta que 2 ya esta considerado en ABC porque $2 \mid b$ y por ende $2^{10} \mid B^2$ puesto que $\ell \geq 5$.

Teorema **5.7.** *Si $\ell \geq 5$ primo, entonces $\rho_{E,\ell}$ es irreducible.*

Demostración. Por la forma de la ecuación que determina E, tenemos que $E[2] \subseteq E(\mathbb{Q})$. Si $\rho_{E,\ell}$ fuera reducible, por el teorema 3.31, E o una curva isógena posee un punto de ℓ-torsión, lo que implica $|E_{tor}(\mathbb{Q})| \geq 4\ell \geq 20$, lo cual es absurdo por la clasificación de Mazur (teorema 3.14). □

Apliquemos ahora la Conjetura de Serre. Por el teorema 5.7, $\rho_{E,\ell}$ es irreducible. Por el teorema 3.12, $\det \rho_{E,\ell} = \chi_\ell$; en particular, $\epsilon = 1$, $\rho_{E,\ell}$ es impar y $k \equiv 2 \pmod{\ell - 1}$.

Por el teorema 3.29, el conductor $N_{\rho_{E,\ell}}$ es el producto de los primos $p \neq \ell$ de mala reducción tal que $\ell \nmid \nu_p(\Delta^{min}(E))$. Si $p \neq 2$ y $p \mid abc$ (pongamos $r = \nu_p(abc)$), entonces $\nu_p(\Delta^{min}(E)) = 2\ell r$. Si $p = 2$, $\nu_2(\Delta(E)) = 2\ell r - 8$. Entonces $N_{\rho_{E,p}} = 2$.

Con respecto al peso, como $\ell \mid \nu_\ell(\Delta^{min}(E)) = 2\ell r$, entonces $k = 2$.

La Conjetura de Serre establece que $\rho_{E,p}$ debe ser conjugada a una representación ρ_f con f una forma propia nueva normalizada de $\mathcal{S}_2(2, 1)$. Tal forma cuspidal no existe, lo que da el resultado.

Un hecho fundamental para que esta demostración funcione para cada primo ℓ, es que la forma cuspidal f que buscamos no depende de ℓ, puesto que el peso y el nivel en donde debemos buscar es siempre 2. Si hubiese dependido de ℓ, este argumento hubiese servido sólo para los primos en los que podamos computar la dimensión del espacio de formas propias cuspidales y obtengamos que es trivial, que serían una cantidad finita. El hecho de poder bajar el nivel y el peso a un número que no depende de ℓ es una especie de resultado de "Level-Lowering" intrínseco en los teoremas 3.29 y 5.5.

5.4. Aplicación: Curvas elípticas con conductor primo sobre $\mathbb{Q}$

El objetivo es clasificar las curvas elípticas definidas sobre $\mathbb{Q}$ con conductor primo. Sea $E/\mathbb{Q}$ una curva elíptica tal que $N(E) = P$ con P primo. Por el teorema 3.30, podemos tomar E en su modelo minimal global. Entonces por el comentario hecho posterior al teorema 3.30, sabemos que los primos que dividen al discriminante son los mismos que los que dividen al conductor, y por lo tanto, $\Delta^{min}(E) = \pm P^m$ con $m \geq 1$. La idea es utilizar la Conjetura de Serre para reducir la posibilidad de primos que pueden dividir a m. Para ello, empezamos con el siguiente teorema:

Teorema **5.8.** *Sea $E/\mathbb{Q}$ una curva elíptica semiestable, ℓ primo y $\left|\Delta^{min}(E)\right|$ una potencia ℓ-ésima. Entonces E tiene un subgrupo $\mathbb{Q}$-racional de orden ℓ y $\ell \leq 7$.*

Demostración. Si $\ell > 7$, por el Teorema de Mazur (teorema 3.14), $\rho_{E,\ell}$ es irreducible, aplicando el mismo argumento que en el teorema 5.7. Como $\Delta^{min}(E)$ es una potencia ℓ-ésima, entonces $\ell \mid \nu_p(\Delta^{min}(E))$ para todo primo p y entonces por el teorema 3.29, $N_{\rho_{E,\ell}} = 1$ y por el teorema 5.5, $k = 2$.

Por el teorema 3.12, $\det \rho_{E,\ell} = \chi_\ell$, así que en particular $\epsilon = 1$. Aplicando la Conjetura de Serre, $\rho_{E,\ell}$ es conjugada a una representación ρ_f con f una forma propia nueva normalizada de $\mathcal{S}_2(1,1)$. Esto nos lleva a una contradicción puesto que no existen formas cuspidales de peso 2 y nivel 1. Por lo tanto $\ell \leq 7$.

Una vez más, el hecho de que $\Delta^{min}(E)$ es una potencia ℓ-ésima y el teorema 3.29 nos lleva ahora a que $\mathbb{Q}(E[\ell])/\mathbb{Q}$ es no ramificada fuera de ℓ. Si suponemos que E no tiene un subgrupo $\mathbb{Q}$-racional de orden ℓ, entonces E no tiene isogenias racionales de orden ℓ (puesto que si tuviera, el núcleo de la isogenia sería un subgrupo $\mathbb{Q}$-racional) y por lo expuesto en la página 261 de [40], entonces $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Escribamos $d = \Delta_{\mathbb{Q}(E[\ell])/\mathbb{Q}}$ y $n = [\mathbb{Q}(E[\ell]) : \mathbb{Q}]$. Entonces $|d|^{1/n} = \ell^\alpha$ con α conocido como es explicado en la proposición 9.2 de [6]. En todos los casos de α para $\ell \leq 7$, $|d|^{1/n}$ viola cotas inferiores de Odlyzko, que son mejoras a las cotas de Minkowski (ver teorema 1 de [34]). $\square$

Teorema **5.9.** *Sea $E/\mathbb{Q}$ una curva elíptica con conductor $N(E) = P$ primo y sea $\Delta^{min}(E) = \pm P^m$. Entonces $m = 1$ salvo finitas clases de isogenia listadas en la tabla 5.2.*

Demostración. Por el comentario posterior a la definición 3.28, E es semiestable. Supongamos que $m > 1$. Entonces, existe ℓ primo tal que $\ell \mid m$. Entonces por el teorema 5.8, $\ell \leq 7$ y hay un subgrupo $\mathbb{Q}$-racional de orden ℓ.

Si $\ell = 2$, hay un subgrupo $\mathbb{Q}$-racional de orden 2. En el teorema 2 de [44] se prueba que entonces E es isógena a una curva de Setzer-Neumann si $P \neq 17$ y hay dos opciones si $P = 17$.

Para $\ell = 3, 5, 7$, [32] demuestra que las únicas opciones son $(P, \ell) \in \{(11, 5), (19, 3), (37, 3)\}$. $\square$

Para finalizar este capítulo, describimos en la tabla 5.2 las curvas mencionadas en el teorema 5.9 para cuando el discriminante de la curva no es primo. En la tabla también se indican el conductor y el discriminante de las mismas.

Ec. de la curva / LMFDB label	**Conductor**	**Discriminante minimal**
$y^2 + xy = x^3 + \frac{u-1}{4}x^2 + 4x + u$ $(p = u^2 + 64)$	p	$-p^2$
11.a2	11	-11^5
17.a2	17	17^2
17.a3	17	-17^4
19.a2	19	-19^3
37.b2	37	37^3

Tabla 5.2: Curvas elípticas de conductor primo cuyo discriminante no es primo

Capítulo 6

Curvas elípticas en cuerpos cuadráticos

Inspirados en la sección 5.4, buscamos clasificar las curvas elípticas de conductor potencia de primo para algunos cuerpos cuadráticos reales.

Como antecedentes similares, tenemos: para curvas elípticas sobre $\mathbb{Q}$ de conductor primo, el artículo [29] de Jean-François Mestre y Joseph Oesterlé, quienes demostraron el resultado de la sección 5.4 sin utilizar la conjetura de Serre. Para extensiones de $\mathbb{Q}$, en [8], John Cremona y Ariel Pacetti clasifican las curvas elípticas de conductor primo sobre cuerpos cuadráticos imaginarios de número de clases 1.

Lo que haremos será replicar las ideas expuestas en [8]. Se presentarán, por supuesto, algunas diferencias con respecto a su estudio. La ventaja principal, es que, como veremos en la sección 6.1.3, se cuenta con teoremas de modularidad y Level-Lowering para cuerpos cuadráticos reales. La desventaja, va a radicar en que para determinar las curvas elípticas posibles, se debe buscar entre las unidades del anillo de enteros del cuerpo, pero en cuerpos cuadráticos imaginarios, las unidades son finitas, mientras que en cuerpos cuadráticos reales, son infinitas.

En este capítulo, dedicaremos la sección 6.1 a enunciar los resultados ya conocidos (clásicos o modernos) que utilizaremos para la investigación. En el resto de las secciones, iremos obteniendo resultados para completar el problema. Para realizar algunos cálculos, se utilizó la herramienta MAGMA (ver [3]), por lo que los programas escritos serán puestos en un apéndice de este documento y serán citados conforme se explican los argumentos.

6.1. Resultados conocidos

6.1.1. Sobre las unidades en cuerpos cuadráticos reales

Sea K un cuerpo cuadrático real, entonces $K = \mathbb{Q}(\sqrt{d})$ con d entero positivo y libre de cuadrados. Veamos un teorema clásico que utilizaremos con frecuencia:

Teorema **6.1.** *Sea K un cuerpo cuadrático real. Entonces*

$$\mathcal{O}_K^\times \simeq \{\pm 1\} \times \left\{\epsilon_f^k : k \in \mathbb{Z}\right\}$$

Demostración. Como K es cuadrático real, tiene $r = 2$ encajes reales y $s = 0$ encajes complejos. Luego aplicar el teorema de las unidades de Dirichlet (Teorema 5.1 de [30]) para obtener que el rango es 1 y que la torsión es $\{\pm 1\}$ porque el resto de las raíces de la unidad no son reales. □

Tenemos cuatro posibles generadores para la parte libre del grupo de unidades. Sin embargo, solo uno de ellos es mayor a 1.

Definición **6.2.** *Sea K un cuerpo cuadrático real. Llamamos* ***unidad fundamental de*** *K y la denotaremos ϵ_f, al único elemento de $\mathcal{O}_K^\times$ que genera la parte libre y es mayor a 1.*

6.1.2. Formas modulares de Hilbert

Veamos como generalizar las formas modulares clásicas de la sección 4.1 si ahora tenemos K un cuerpo cuadrático real. El fin de esta generalización, es conseguir un teorema de modularidad que nos permita entender mejor las representaciones de curvas elípticas sobre K.

Daremos aquí una breve explicación de la generalización. Para más detalles, se recomienda leer el capítulo "Hilbert Modular Forms and Their Applications" de [5]. Para una explicación resumida, pero que abarca algunos aspectos en los que aquí no profundizaremos, ver sección 3.6 de [7]

Para empezar, generalicemos la definición 4.1:

Definición **6.3.** *Sea $\mathcal{N}$ un ideal de $\mathcal{O}_K$. Llamamos* ***subgrupo de congruencia de nivel*** *$\mathcal{N}$ al conjunto*

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

donde la congruencia módulo $\mathcal{N}$ es en cada entrada de la matriz.

Al igual que en la sección 4.1, el índice de $\Gamma_0(\mathcal{N})$ en $\mathrm{SL}_2(\mathcal{O}_K)$ es finito y $\Gamma_0(1) = \mathrm{SL}_2(\mathcal{O}_K)$.

Como K es un cuerpo cuadrático real, tiene dos encajes distintos $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{R}$. Como hay dos encajes, consideramos la acción de las matrices de $\mathrm{SL}_2(\mathcal{O}_K)$ sobre $\mathcal{H}^2$ según los dos encajes posibles.

Definición **6.4.** *En concreto, como en la definición 4.2, dada* $\gamma \in \mathrm{SL}_2(\mathcal{O}_K)$ *y* $k = (k_1, k_2)$ *un par de enteros definimos el operador* $[\gamma]_k : \mathbb{C}^{\mathcal{H}^2} \to \mathbb{C}^{\mathcal{H}^2}$ *como:*

$$(F\,[\gamma]_k)(z, z') = (\sigma_1(c)z + \sigma_1(d))^{-k_1}(\sigma_2(c)z' + \sigma_2(d))^{-k_2} \\ F\left(\frac{\sigma_1(a)z + \sigma_1(b)}{\sigma_1(c)z + \sigma_1(d)}, \frac{\sigma_2(a)z' + \sigma_2(b)}{\sigma_2(c)z' + \sigma_2(d)}\right)$$

cuando $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

No es difícil ver que esto generaliza la ecuación (4.1), puesto que si $K = \mathbb{Q}$, solo tendríamos un encaje y $\mathcal{O}_K = \mathbb{Z}$.

Definición **6.5.** *Sea* K *un cuerpo cuadrática real,* $k = (k_1, k_2)$ *un par de enteros y* $\mathcal{N} \lhd \mathcal{O}_K$. *Una* ***forma modular de Hilbert de peso*** (k_1, k_2) ***y nivel*** $\mathcal{N}$ *es una función* $F : \mathcal{H}^2 \to \mathbb{C}$ *tal que:*

1. F *es biholomorfa en* $\mathcal{H}^2$,
2. $F\,[\gamma]_k = F$ *para toda* $\gamma \in \Gamma_0(\mathcal{N})$,

Si comparamos con la definición 4.5, no estamos imponiendo que F sea holomorfa en las cúspides. Esto se debe a que las formas modulares de Hilbert son automáticamente holomorfas en las cúspides por el principio de Götzky-Koecher (ver Teorema 1.20 de [5]). Al igual que en la sección 4.1, debido a la definición de $\Gamma_0(\mathfrak{N})$ tenemos que F es 1-periódica y podemos considerar una expansión de Fourier en dos variables para F.

Definición **6.6.** *Si* $k_1 = k_2 = k$ *diremos* ***peso paralelo*** k.

A partir de ahora, solo trabajaremos con formas modulares de peso paralelo k. Denotaremos $\mathcal{M}_k(\mathcal{N})$ al espacio de las formas modulares de peso paralelo k y nivel $\mathcal{N}$. Una vez más, cada $\mathcal{M}_k(\mathcal{N})$ es $\mathbb{C}$-espacio vectorial de dimensión finita (ver Teorema 1.33 de [5]) y en casi todos los casos se conoce la dimensión.

Definición **6.7.** *Sea* K *un cuerpo cuadrática real,* k *un entero y* $\mathcal{N} \lhd \mathcal{O}_K$ *enteros. Decimos que* $F : \mathcal{H} \to \mathbb{C}$ *es una* ***forma cuspidal de peso paralelo*** k ***y nivel*** $\mathcal{N}$ *si*

1. F *es una forma modular de peso paralelo* k *y nivel* $\mathcal{N}$,
2. $F\,[\alpha]_k\,(\infty, \infty) = 0$, $\forall \alpha \in \mathrm{SL}_2(\mathcal{O}_K)$.

Denotaremos $\mathcal{S}_k(\mathcal{N})$ *al espacio de formas cuspidales de peso paralelo* k *y nivel* $\mathcal{N}$.

Definición **6.8.** *Una forma cuspidal se dice* ***normalizada*** *si en su expansión de Fourier* $a_1(F) = 1$.

Los espacios de formas modulares y cuspidales se pueden computar usando MAGMA (ver [3]).

Continuando con las analogías con respecto a la sección 4.1, vemos que podemos asociar también operadores de Hecke a las formas modulares de Hilbert (ver página 32 de [7]) cuyas propiedades son iguales a las expuestas en el Teorema 4.7. Estos operadores, junto a una noción de producto interno de Petersson (ver definición 1.30 de [5]) nos permite definir el concepto de forma propia cuspidal nueva como en la sección 4.1, y al igual que antes existe una representación de Galois:

Teorema **6.9.** *Sea K un cuerpo cuadrático real, F una forma de Hilbert propia nueva normalizada de $\mathcal{S}_k(\mathcal{N})$ y ℓ primo racional. Entonces existe una representación de Galois*

$$\rho_F : G_K \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$$

tal que en los primos $\mathfrak{p} \nmid \ell\mathfrak{N}$, la representación ρ_F no ramifica, y en estos primos donde no ramifica, $\mathrm{tr}(\rho_F(\mathrm{Frob}_\mathfrak{p})) = a_\mathfrak{p}(F)$ *y* $\det(\rho_F(\mathrm{Frob}_\mathfrak{p})) = N(\mathfrak{p})$ *siendo $N(\mathfrak{p})$ la norma del primo $\mathfrak{p}$.*

Demostración. Ver [48] y [17]. Este último para el caso de peso paralelo 1. □

6.1.3. Teoremas de modularidad y Level-Lowering

Como vimos en la introducción, contar con teoremas de este tipo es fundamental para resolver problemas. Un teorema de modularidad, nos permite asociar representaciones de Galois de curvas elípticas a representaciones de formas de Hilbert propias nuevas normalizadas, y un teorema de Level-Lowering, nos da el dato sobre el espacio de que peso y nivel debemos buscar. Afortunadamente, tales teoremas existen en el caso de cuerpos cuadráticos reales:

Teorema **6.10.** *(Modularidad) Todas las curvas elípticas sobre cuerpos cuadráticos reales son modulares*

Demostración. Ver Teorema 1 de [14]. □

Teorema **6.11.** *(Level-Lowering) Sea K totalmente real, E/K una curva elíptica de conductor $\mathcal{N}$, ℓ un primo racional. Denotemos $\Delta_\mathfrak{q}$ el discriminante del modelo minimal de E en $\mathfrak{q}$ y sean*

$$\mathcal{M}_\ell = \prod_{\substack{\mathfrak{q}||\mathcal{N} \\ \ell | v_\mathfrak{q}(\Delta_\mathfrak{q})}} \mathfrak{q}, \qquad \mathcal{N}_\ell = \frac{\mathcal{N}}{\mathcal{M}_\ell}$$

donde $||$ significa que $\mathfrak{q}$ divide exactamente a $\mathfrak{N}$.

Agreguemos además que,

1. *$\ell \geq 5$ y $e(\mathfrak{q} \mid \ell) < \ell - 1$ para todo $\mathfrak{q} \mid \ell$,*
2. *$\mathbb{Q}(\xi_\ell)^+ = \mathbb{Q}(\xi_\ell + \overline{\xi_\ell}) \nsubseteq K$,*
3. *E es modular,*
4. *$\overline{\rho}_{E,\ell}$ es irreducible,*
5. *E es semiestable para los $\mathfrak{q} \mid \ell$,*
6. *$\ell \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$ para todo $\mathfrak{q} \mid \ell$.*

Entonces existe una forma modular de Hilbert propia nueva y normalizada F, de peso paralelo 2 y de nivel $\mathcal{N}_\ell$ tal que $\rho_{E,\ell} \sim \rho_F$

Demostración. Ver Teorema 7 de [15]. □

6.2. Estrategia

La estrategia puede dividirse en cuatro etapas:

1. Lo primero que haremos será usar los Teoremas 6.10 y 6.11 para trabajar sobre algunos cuerpos cuadráticos reales que nos permitan decir (en la mayoría de los casos) que las representaciones de curvas elípticas son reducibles (Teorema 6.12).
2. Luego, buscaremos un análogo al Teorema 3.31, para deducir que las curvas elípticas cuya representación es reducible, tiene un punto de ℓ-torsión para algún ℓ que divide a $\nu_{\mathfrak{p}}(\Delta^{min}(E))$ (Teorema 6.14).
3. Vamos a reducir las posibilidades de los valores de ℓ usando cotas de Hasse.
4. Teniendo pocos valores para ℓ y conociendo la forma de las curvas elípticas cuando tienen un punto de ℓ-torsión para valores pequeños de ℓ, vamos a buscar los posibles coeficientes a_i de las curvas elípticas.

Esta es en principio la estrategia. Sin embargo, en cada paso, iremos teniendo casos bordes que deben ser tratados diferente y usando algún resultado extra. En este documento sin embargo, no completaremos todos los detalles, y se seguirá trabajando en un futuro con el problema.

6.3. Resultados generales

Sea $K = \mathbb{Q}(\sqrt{d})$ cuerpo cuadrático real. Utilizando MAGMA [3], encontramos que para $d \leq 1000$, solo $d = 2, 3, 5, 13, 17, 21$ cumplen que $\mathcal{S}_2(1) = \{0\}$ (ver 'PROGRAMA 1' en apéndice). En lo que queda del documento, K será un cuerpo cuadrático real para alguno de esos valores de d.

Usando MAGMA, se puede ver también que todos los cuerpos anteriores tienen número de clase 1, y que el número de clase narrow es igual 1 para casi todos los cuerpos a excepción de $d = 3$ y $d = 21$, en el cual el número de clase narrow es 2. Esto implica por el Teorema 3.30, que todas las curvas elípticas tienen modelo minimal global y tiene sentido referirse al discriminante minimal $\Delta^{min}(E)$.

Sea E/K una curva elíptica con conductor potencia de primo $N(E) = \mathfrak{p}^n$, siendo $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ y $n > 0$. Por el comentario posterior al Teorema 3.30, sabemos que $(\Delta^{min}(E)) = \mathfrak{p}^m$ con $m > 0$. A lo largo de lo que queda de capítulo, reservaremos d, n, m y $\mathfrak{p}$ al uso que les hemos dado hasta ahora.

Teorema **6.12.** *Sea K algunos de los cuerpos considerados, E/K una curva elíptica con conductor primo $\mathfrak{p}$ y $m > 1$. Sea $\ell \geq 5$ primo racional tal que $\ell \mid m$. Entonces $\rho_{E,\ell}$ es reducible excepto si $d = \ell = 5$.*

Demostración. Supongamos que $\rho_{E,\ell}$ es irreducible. La idea es utilizar el Teorema 6.11.

De las hipótesis de ese teorema, las partes 6 y 5 son porque el conductor de E es primo. 4, es la suposición, 3 es el Teorema 6.10 y 1 es porque el cuerpo es cuadrático y $\ell \geq 5$.

La condición 2 debemos mirarla con más detalle. La extensión $\mathbb{Q}(\xi_\ell)^+/\mathbb{Q}$ tiene grado $\frac{\ell-1}{2}$, por lo que si $\ell \geq 7$, no está contenida en K que es de grado 2. Si $\ell = 5$, $\mathbb{Q}(\xi_\ell)^+ = \mathbb{Q}(\sqrt{5})$ que no está contenido en K si $d \neq 5$. Estando ahora sí en las hipótesis, por el Teorema 6.11, la representación $\rho_{E,\ell}$ se asocia a una forma cuspidal de Hilbert de peso paralelo 2 y nivel 1. Dado que para los cuerpos K con los que decidimos trabajar, $\mathcal{S}_2(1)$ es trivial, llegamos a una contradicción. $\square$

El Teorema 6.12, nos deja el primer caso borde que corresponde a $(d, \ell) = (5, 5)$, el cual no estudiaremos en este documento.

En la misma línea del Teorema 6.12, tenemos:

Teorema **6.13.** *Sea K algunos de los cuerpos considerados, E/K una curva elíptica con conductor $\mathfrak{p}^n$ tal que $2 \mid m$. Entonces $\rho_{E,2}$ es reducible.*

Demostración. Supongamos que $\rho_{E,2}$ es irreducible. Por el ejemplo 3.13, tenemos que $\mathrm{Gal}(K(E[2])/K) \approx S_3$ o A_3. Como el número de clase es 1, tenemos que $\Delta(E) = u\pi^{2r}$ con $u \in \mathcal{O}_K^\times$ y π generador de $\mathfrak{p}$.

Supongamos que es S_3. Dado que la característica de K es cero, podemos llevar E a su forma normal de Weierstrass, obteniendo que la curva es de la forma $y^2 = f(x)$ con f de grado 3. En este lugar, tenemos que $\phi_2 = f$ y por ende $\Delta(\phi_2) = \Delta(f) = 2^{-4}\Delta(E) = 2^{-4}u\pi^{2r}$. Como el grupo de Galois es S_3, el ejemplo 3.13 muestra que u no es un cuadrado y por ende $K(\sqrt{\Delta(E)}) = K(\sqrt{u})$ es un subcuerpo de $K(E[2])$. Por el Teorema 3.29, los primos que pueden ramificar en la

extensión $K(E[2])/K$ son 2 y $\mathfrak{p}$. Ahora, como $2 \mid v_{\mathfrak{p}}(\Delta_{\mathfrak{p}})$, entonces $\mathfrak{p}$ no ramifica, y por lo tanto, solo el 2 puede ramificar. Esto nos lleva a buscar cuerpos L tales que:

- $\mathrm{Gal}(L/K) = S_3$,
- $\mathcal{O}_L$ no ramifica afuera de 2,
- $K(\sqrt{u}) \subseteq L$

Más aún, por el Teorema 6.1, $K(\sqrt{u})$ es alguno de $K(\sqrt{\epsilon_f})$, $K(\sqrt{-\epsilon_f})$ o $K(\sqrt{-1})$, siendo ϵ_f la unidad fundamental, y $\mathrm{Gal}(L/K(\sqrt{u})) = C_3$. Utilizando 'PROGRAMA 2' copiado en el apéndice, encontramos que no hay ningún cuerpo L en las condiciones anteriores.

Si ahora el grupo de Galois es A_3, las ideas de la parte anterior sirven y lo que buscamos es una extensión L tal que

- $\mathrm{Gal}(L/K) = A_3$,
- $\mathcal{O}_L$ no ramifica afuera de 2.

Tampoco encontramos cuerpos en este caso. □

Faltaría un análogo a los Teoremas 6.12 y 6.13 para $\ell = 3$ que no estudiaremos en este documento.

El siguiente teorema es un análogo al Teorema 3.31 presentado en el capítulo 3.

Teorema **6.14.** *Sea K algunos de los cuerpos considerados, $\ell \geq 3$ un primo racional tal que $\ell \mid m$ y E/K una curva elíptica semiestable para la cual $\rho_{E,\ell}$ es reducible. Entonces E o una curva isógena tiene un punto de ℓ-torsión, excepto que la representación sea alguna de las siguientes:*

1. $\rho_{E,\ell} \simeq \begin{pmatrix} \chi_3 & * \\ 0 & \chi_\ell \chi_3 \end{pmatrix}$ *en $d = 3, 21$ con ℓ que no ramifica.*
2. $\rho_{E,\ell} \simeq \begin{pmatrix} \chi_\ell \chi_3 & * \\ 0 & \chi_3 \end{pmatrix}$ *en $d = 3, 21$ con ℓ que no ramifica.*
3. $\rho_{E,3} \simeq \begin{pmatrix} \psi\chi_3 & * \\ 0 & \psi \end{pmatrix}$ *en $d = 13$, con $\psi : G_K \to \mathbb{F}_3^\times$ que factoriza por el cuerpo $K\left(\sqrt{\frac{\sqrt{13}-1}{2}}\right)$.*
4. $\rho_{E,3} \simeq \begin{pmatrix} \psi\chi_3 & * \\ 0 & \psi \end{pmatrix}$ *en $d = 13$ con $\psi : G_K \to \mathbb{F}_3^\times$ que factoriza por el cuerpo $K\left(\sqrt{\frac{-\sqrt{13}-1}{2}}\right)$.*

5. $\rho_{E,3} \simeq \begin{pmatrix} \psi\chi_3 & * \\ 0 & \psi \end{pmatrix}$ *en* $d = 21$ *con* ψ *que factoriza por el cuerpo* $L = K\left(\sqrt{\frac{3-\sqrt{21}}{2}}\right)$.

6. $\rho_{E,3} \simeq \begin{pmatrix} \psi\chi_3 & * \\ 0 & \psi \end{pmatrix}$ *en* $d = 21$ *con* ψ *que factoriza por el cuerpo* $L = K\left(\sqrt{\frac{3+\sqrt{21}}{2}}\right)$.

7. $\rho_{E,7} \simeq \begin{pmatrix} \chi_7^2 & * \\ 0 & \chi_7^{-1} \end{pmatrix}$ *en* $d = 21$.

Demostración. Observar que como el cuerpo es real, si la representación es irreducible, entonces es absolutamente irreducible (es decir, que es irreducible incluso en $\overline{\mathbb{F}_\ell}$). En efecto, como el cuerpo es real, existe $c \in G_K$ una conjugación compleja. Como $\det \rho_{E,\ell} = \chi_\ell$, la conjugación compleja actúa como -1, lo que implica que sus valores propios son 1 y -1, así que entonces los vectores propios están en $\mathbb{F}_\ell$ porque los valores propios lo están. Como $\ell > 2$, tenemos que $1 \neq -1$ y entonces estos subespacios parten la representación en 2 a través de la acción de conjugación compleja. Si estos dos subespacios son invariantes por el resto de los elementos, entonces la representación será reducible, si no, será irreducible. Esto ocurre incluso en cuerpos de números con al menos un encaje real en $\mathbb{C}$, que es lo que nos permite asegurar tener una conjugación compleja en G_K.

Como $\rho_{E,\ell}$ es reducible, en alguna base adecuada tenemos que

$$\rho_{E,\ell} \simeq \begin{pmatrix} \theta_2 & * \\ 0 & \theta_1 \end{pmatrix}$$

con $\theta_i : G_K \to \mathbb{F}_\ell^\times$ tales que $\theta_1\theta_2 = \chi_\ell$, porque es la representación de una curva elíptica.

Debido al Teorema 3.29 y al hecho de que $\ell \mid m$, sabemos que $\rho_{E,\ell}$ solo puede ramificar en lugares finitos arriba de ℓ y los lugares de infinito, y esto se traslada a los caracteres θ_1 y θ_2. A su vez, el lema 1 de [23], indica que si E es semiestable y ℓ no ramifica en K, entonces los caracteres no pueden ramificar en el mismo primo arriba de ℓ. Si uno de los caracteres es 1, entonces E o una curva isógena tiene un punto de orden ℓ, basados en el mismo argumento que en el Teorema 3.31. Discutamos según las posibilidades de ℓ en K.

Si <u>ℓ es inerte</u>, entonces solo uno de los caracteres puede ramificar en ℓ, y por lo tanto el otro solo puede ramificar en los lugares de infinito. Para cuerpos donde el número de clases narrow es 1, esto implica que el carácter que no ramifica en ℓ debe ser trivial. Para cuerpos donde el número de clases narrow es 2, esto significa que uno o ambos caracteres factorizan por la extensión abeliana maximal K^+ donde

K no ramifica en ningún lugar finito (ver Teorema 1.26). Por lo tanto, E tiene un punto de ℓ-torsión en K^+. En los cuerpos que estamos considerando esto solo puede pasar si $d = 3$ o 21. En ambos casos, $K^+ = K(\sqrt{-3})$ y el carácter es χ_3. Si ninguno de los caracteres es trivial, tenemos en principio las siguientes combinaciones:

(a) θ_1 ramifica en ℓ y $\theta_2 = \chi_3$,

(b) θ_2 ramifica en ℓ y $\theta_1 = \chi_3$,

(c) $\theta_1 = \theta_2 = \chi_3$. Esto último sin embargo no puede ocurrir puesto que $\theta_1\theta_2 = \chi_3^2 = 1 \neq \chi_\ell$ para $\ell > 2$.

Si ℓ descompone, entonces $\ell = \mathfrak{l}_1\mathfrak{l}_2$. Si ambos primos ramifican en el mismo carácter, entonces el otro carácter solo puede ramificar en lugares de infinito. El mismo argumento que el planteado antes, nos lleva a que si uno de ellos no es trivial, entonces $d = 3$ o 21 y $\theta_1 = \chi_3$ ó $\theta_2 = \chi_3$.

Consideremos el caso en el que θ_i solo ramifica en $\mathfrak{l}_i$ con $i = 1, 2$. Sea $u \in^\times$ y llamemos u_ν al elemento de $\mathbb{I}_K$ que vale 1 en todas las coordenadas que no son la valuación ν y u en ν. Para simplificar la notación, llamemos $u = (u, u, ...)$ el encaje por la diagonal de la unidad u. El Teorema 1.23 nos permite considerar $\widetilde{\theta}_i = \theta_i \circ \Phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{ab}/K) \to \overline{\mathbb{F}_\ell}$, así como $\widetilde{\chi}_\ell = \chi_\ell \circ \Phi_K$. Se cumple que

$$\widetilde{\chi}_\ell(u_{\mathfrak{l}_i}) = u \pmod{\mathfrak{l}_i} \tag{6.1}$$

para $i = 1, 2$. Una vez más el Teorema 1.26, nos asegura que $\widetilde{\theta}_1(u) = 1$ para todo $u \in \mathcal{O}_K^\times$. Del hecho de que θ_1 solo puede ramificar en $\mathfrak{l}_1$, ∞_1 y en ∞_2 siendo estos dos últimos los lugares del infinito, tenemos que

$$1 = \widetilde{\theta}_1(u) = \widetilde{\theta}_1(u_{\mathfrak{l}_1})\widetilde{\theta}_1(u_{\infty_1})\widetilde{\theta}_1(u_{\infty_2}). \tag{6.2}$$

Por otro lado, como θ_2 no ramifica en $\mathfrak{l}_1$ y $\widetilde{\chi}_\ell = \widetilde{\theta}_1\widetilde{\theta}_2$, entonces $\widetilde{\chi}_\ell(u_{\mathfrak{l}_1}) = \widetilde{\theta}_1(u_{\mathfrak{l}_1})$. Además, $\widetilde{\theta}_1(u_{\infty_i}) = \pm 1$ porque corresponden a los lugares en infinito para $i = 1, 2$, así que sustituyendo en la ecuación (6.2), obtenemos

$$\widetilde{\chi}_\ell(u_{\mathfrak{l}_1}) = \widetilde{\theta}_1(u_{\infty_1})\widetilde{\theta}_1(u_{\infty_2}) \tag{6.3}$$

Evaluando la ecuación (6.3) en $u = \epsilon_f^2$ y utilizando la ecuación (6.1) y el hecho de que $\widetilde{\theta}_1(u_{\infty_i})$ son caracteres de orden 2 para $i = 1, 2$, obtenemos que

$$\widetilde{\chi}_\ell((\epsilon_f^2)_{\mathfrak{l}_1}) = \epsilon_f^2 \pmod{\mathfrak{l}_1} = 1 = \widetilde{\theta}_1((\epsilon_f^2)_{\infty_1})\widetilde{\theta}_1((\epsilon_f^2)_{\infty_2})$$

, lo que implica que $\mathfrak{l}_1 \mid (\epsilon_f^2 - 1)$. Esto da finitos valores posibles para ℓ en cada uno de los cuerpos que consideramos. Teniendo en cuenta el hecho de que ℓ tiene que descomponer y ser mayor a 2 por nuestra hipótesis, solo encontramos el caso $(d, \ell) = (13, 3)$. Por lo tanto, $\theta_1 : G_K \to \mathbb{F}_3^\times$ y solo ramifica en 3, lo que nos lleva a buscar extensiones L/K de grado 2 que solo ramifiquen en uno de los primos $\mathfrak{l}_i$ arriba de 3. El PROGRAMA 3 (ver apéndice) da los cuerpos $K\left(\sqrt{\frac{\pm\sqrt{13}-1}{2}}\right)$, que

corresponden básicamente a tomar raíz cuadrada de dos generadores de los ideales $\mathfrak{l}_1$ y $\mathfrak{l}_2$. Este caso se suma a la lista de excepciones.

Si <u>ℓ ramifica:</u> Aplicando el mismo argumento que en el Teorema 2.5 de [8], obtenemos que θ_1/θ_2 es no ramificado sobre primos finitos. Discutimos según dos casos:

1. Si $\underline{\theta_1/\theta_2 = 1}$, entonces $\theta_1^2 = \chi_\ell$. Sea L el cuerpo por el cual factoriza θ_1, como $\theta_1 : G_K \to \mathbb{F}_\ell^\times$ por ser la representación de una curva elíptica, entonces $[L : K] \mid \ell - 1$ y como ya sabíamos, L/K solo ramifica en ℓ o en lugares del infinito. A su vez, si $\theta_1(\sigma) = 1$ entonces $\chi_\ell(\sigma) = 1$, lo que implica que $\mathrm{Gal}(\overline{K}/L) \subseteq \mathrm{Gal}(\overline{K}/K(\xi_\ell))$ y entonces $K(\xi_\ell) \subseteq L$. Por otro lado, $|\chi_\ell| = [K(\xi_\ell) : K]$ que será $\frac{\ell-1}{2}$ sí $K \subseteq \mathbb{Q}(\xi_\ell)$ y será $\ell - 1$ en caso contrario. En nuestros cuerpos, será $\frac{\ell-1}{2}$ si $d = 5, 13, 17$. Por lo tanto, en $d = 5, 13, 17$ podría aparecer un carácter en una extensión cuadrática de $K(\xi_\ell)$ que no ramifique en primos finitos que no dividen a ℓ. El programa que hace esto es el PROGRAMA 3 (ver apéndice) y no encontró ningún cuerpo L. Por lo tanto, $L = K(\xi_\ell)$ y entonces $\theta_1 = \chi_\ell^k$ con $k < |\chi_\ell|$, que será $\ell - 1$ o $\frac{\ell-1}{2}$ según el valor de d como fue explicado antes. La ecuación $\theta_1^2 = \chi_\ell$ implica que $2k \equiv 1 \pmod{|\chi_\ell|}$ que no da soluciones para ninguno de los casos.

2. Si $\underline{\theta_1/\theta_2 \neq 1}$. Este caso solo puede ocurrir si el número de clases narrow es mayor a 1, y al igual que como era explicado en el caso de ℓ inerte, entonces $d = 3$ o 21 y $\theta_1/\theta_2 = \chi_3$. Despejando en el determinante de la representación obtenemos que $\theta_1^2 = \chi_\ell \chi_3$.

   Si $d = 3$, entonces $\ell = 3$ y tanto θ_1, θ_2 como χ_3 factorizan por $K(\sqrt{-3})$. De la ecuación $\theta_1\theta_2 = \chi_3$, obtenemos que uno de ellos debe ser trivial.

   Si $d = 21$, entonces $\ell = 3$ ó 7, y podemos escribir $K = \mathbb{Q}(\sqrt{\ell\,\ell'})$. Observar que cualquiera de los dos sea ℓ, tenemos que $\chi_3 = \chi_\ell^{\frac{\ell-1}{2}}$, y entonces $\theta_1^2 = \chi_\ell^{\frac{\ell+1}{2}}$. Como los primos son de la forma $3 \pmod 4$, tenemos que $\left(\theta_1/\chi_\ell^{\frac{\ell+1}{4}}\right)^2 = 1$, por lo que encontrar θ_1 es equivalente a encontrar un carácter de orden 2, que sea igual a $\theta_1/\chi_\ell^{\frac{\ell+1}{4}}$. Como en los casos anteriores, esto lo haremos buscando una extensión L/K de grado 2 que solo ramifique en ℓ y en infinito. La segunda parte del PROGRAMA 3 (ver apéndice) hace esto y obtenemos cuatro extensiones posibles:

   Para $(d, \ell) = (21, 3)$: $K\left(\sqrt{\frac{3-\sqrt{21}}{2}}\right)$, $K\left(\sqrt{\frac{3+\sqrt{21}}{2}}\right)$ y $K(\sqrt{-3})$.

   Para $(d, \ell) = (21, 7)$: $K(\sqrt{-7})$.

En el último caso de $(d, \ell) = (21, 3)$ y en el único caso de $(d, \ell) = (21, 7)$, el carácter es $\chi_\ell^{\frac{\ell+1}{2}}$, y por tanto $(\theta_1, \theta_2) = (\chi_\ell^{\frac{3\ell-1}{4}}, \chi_\ell^{\frac{\ell+1}{4}})$. Si $\ell = 3$ esto es $(\theta_1, \theta_2) = (1, \chi_3)$, y por tanto hay un punto de 3-torsión. Si $\ell = 7$, entonces $(\theta_1, \theta_2) = (\chi_7^5, \chi_7^2)$. □

En lo que continúa, buscaremos curvas elípticas con puntos de ℓ-torsión en K, por lo que excluiremos en este documento, el estudio de curvas elípticas sin puntos de torsión en K con representación reducible, que corresponde a los casos señalados en el Teorema 6.14. Los casos bordes que aparecieron, no se estudiarán en este documento.

Veamos el punto 3 de nuestra estrategia, reduciendo los valores posibles para ℓ. Para ellos daremos dos teoremas. El primero (Teorema 6.16) es aplicable para cualquier curva elíptica con un punto de ℓ-torsión. El segundo (Teorema 6.17) agrega una hipótesis más sobre el primo que divide al conductor.

Empezaremos sin embargo, con un teorema análogo al Teorema 3.14 para cuerpos cuadráticos:

Teorema **6.15.** *Sea K un cuerpo cuadrático y E/K una curva elíptica. Entonces $E_{tor}(K)$ es alguno de los siguientes grupos:*

- $\mathbb{Z}/N\mathbb{Z}$, *con* $1 \leq N \leq 16$ *o* $N = 18$,
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ *con* $N \leq 6$,
- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3N\mathbb{Z}$ *con* $N \leq 2$,
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Demostración. Ver teorema de [18]. □

Teorema **6.16.** *Sea K algunos de los cuerpos considerados, ℓ primo y E/K una curva elíptica con un punto de ℓ-torsión. Entonces $\ell \leq 13$.*

Demostración. Si P es el punto de ℓ-torsión, debe ser un elemento de alguna de las torsiones posibles del Teorema 6.15. No es difícil ver que entonces $\ell \leq 13$. □

Teorema **6.17.** *Sea K algunos de los cuerpos considerados, ℓ primo impar, E/K una curva elíptica con un punto de ℓ-torsión y conductor $N(E) = \mathfrak{p}^n$ con $\mathfrak{p}$ ideal primo de $\mathcal{O}_K$. Si $\mathfrak{p} \nmid 2$, entonces*

- $\ell \leq 5$ *si* $d = 2, 3, 17$,
- $\ell \leq 7$ *si* $d = 5, 13, 21$.

Demostración. Sea $\mathfrak{q}$ ideal primo arriba de 2. Como $\mathfrak{p} \nmid 2$, E tiene buena reducción en $\mathfrak{q}$, y entonces por el Teorema 3.23, $E(K)[\ell] \hookrightarrow \widetilde{E}(\mathbb{F}_\mathfrak{q})$. Por el Teorema 3.32,

$$\#\widetilde{E}(\mathbb{F}_\mathfrak{q}) \leq N(\mathfrak{q}) + 1 + 2\sqrt{N(\mathfrak{q})}.$$

En $d = 2, 3$, el número 2 ramifica, entonces $N(\mathfrak{q}) = 2$. En $d = 17$, el número 2 descompone así que $N(\mathfrak{q}) = 2$ y en $d = 5, 13, 21$, el número 2 es primo, así que $N(\mathfrak{q}) = 4$ por lo que

$$\ell \leq \#E(\mathbb{F}_\mathfrak{q}) \leq \begin{cases} 6 & \text{si } d = 2, 3, 17, \\ 9 & \text{si } d = 5, 13, 21. \end{cases} \tag{6.4}$$

Luego, simplemente usar que ℓ es primo para obtener el resultado. □

6.4. Curvas elípticas con 2-torsión

En esta sección nos encargaremos de las curvas elípticas de conductor potencia de primo impar con un punto de 2-torsión sobre K, en los cuerpos cuadráticos reales considerados. Sea E/K una curva elíptica en las hipótesis mencionadas antes. Por el Teorema 3.30, sabemos que E tiene un modelo minimal global

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{6.5}$$

Si tomamos el cambio de variable $y \mapsto y - \frac{a_1x - a_3}{2}$, llevamos el modelo anterior a la forma

$$E : y^2 = x^3 + \left(a_2 + (a_1/2)^2\right) x^2 + (a_4 + a_1a_3/2)\, x + \left(a_6 + (a_3/2)^2\right) \tag{6.6}$$

que es entera en los primos impares puesto que allí 2 es invertible. Debemos sin embargo, hacer este modelo entero en los primos arriba de 2. Para ello, si $\mathfrak{q} = (\tau) \mid 2$, vamos a escalar por τ^{2r} para un r adecuado. La elección de r dependerá de sí la reducción en $\mathfrak{q}$ de E es supersingular u ordinaria.

Teorema **6.18.** *Sea K cuerpo cuadrático con número de clase 1, E/K una curva elíptica de conductor potencia primo impar con un punto de 2-torsión sobre K con ecuación minimal como en* (6.5)*. Sea $\mathfrak{q} = (\tau)$ ideal primo arriba de 2.*

- *Si E tiene reducción ordinaria en $\mathfrak{q}$, entonces $\nu_\mathfrak{q}(a_1) = 0$ y el "scaling" que hace a* (6.6) *integral es $x \mapsto 2^2x$ ($r = 2e_2$ siendo e_2 el índice de ramificación de 2 en K).*
- *Si E tiene reducción supersingular en $\mathfrak{q}$, entonces 2 ramifica en K, $\nu_\mathfrak{q}(a_1) = 1$ y el "scaling" que hace a* (6.6) *integral es $x \mapsto \tau^2x$ ($r = 2$).*

Demostración. Ver proposición 5.2 de [8]. □

Sea $(x_0, 0)$ el punto de 2-torsión de E. Si tomamos el cambio de variable $x \mapsto x - x_0$, entonces pasamos E a un modelo de la forma

$$E_{a,b} : y^2 = x(x^2 + ax + b) \tag{6.7}$$

donde ahora el $(0, 0)$ es el punto de 2-torsión.

Podemos comparar los discriminantes de los modelos (6.5) y (6.7). En efecto, si $\Delta^{min}(E)$ es el discriminante de (6.5), entonces el modelo (6.6) tiene el mismo discriminante (las traslaciones no cambian el discriminante). Lo siguiente fue aplicar el Teorema 6.18 que cambia el discriminante por una potencia 6 del número por el cual x fue escalado. El último cambio de variable fue también una traslación que tampoco cambia el discriminante. Tenemos entonces que:

$$2^4 b^2(a^2 - 4b) = \Delta(E_{a,b}) = \begin{cases} 2^{12}\Delta^{min}(E) & \text{si } E \text{ tiene reducción ordinaria,} \\ \tau^{12}\Delta^{min}(E) & \text{si } E \text{ tiene reducción supersingular.} \end{cases}$$

Como mencionábamos en el Teorema 6.18, el caso de reducción supersingular, solo puede ocurrir en cuerpos K donde 2 ramifica. En nuestro caso, estos cuerpos son cuando $d = 2$ o $d = 3$. Si $d = 2$, tomamos $\tau = \sqrt{2}$ y entonces $\tau^{12} = 2^6$, y tenemos que

$$b^2(a^2 - 4b) = 2^2\Delta^{min}(E).$$

Si $d = 3$, tomamos $\tau = 1 - \sqrt{3}$ y entonces $\tau^2 = \epsilon_f 2$ siendo $\epsilon_f = 2 - \sqrt{3}$ la unidad fundamental y entonces

$$b^2(a^2 - 4b) = \epsilon_f^6 2^2 \Delta^{min}(E).$$

Teorema **6.19.** *Sea $(x_0, 0)$ el punto de 2-torsión de E y $E_{a,b}$ el modelo de E obtenido como se explicó previamente. Entonces:*

- *Si E tiene reducción ordinaria y $\nu_{\mathfrak{q}}(x_0) > 0$, entonces $(\nu_{\mathfrak{q}}(a), \nu_{\mathfrak{q}}(b)) = (0, 4e_2)$ y si $\nu_{\mathfrak{q}}(x_0) = 0$, entonces $(\nu_{\mathfrak{q}}(a), \nu_{\mathfrak{q}}(b)) = (e_2, 0)$.*
- *Si E tiene reducción supersingular, entonces $\nu_{\mathfrak{q}}(x_0) = 0$ y $(\nu_{\mathfrak{q}}(a), \nu_{\mathfrak{q}}(b)) = (k, 0)$ con $k \geq 3$.*

Demostración. Ver corolario 5.3 de [8]. □

El Teorema 6.19 muestra que alguno de a o b tiene valuación 0 para $\mathfrak{q}$ en cualquiera de lo dos casos posibles. Como $\mathfrak{q}$ es alguno de los primos que divide a 2 (recordar que si 2 descompone en $\mathcal{O}_K$ tenemos dos primos arriba de 2), entonces podemos escribir $(2) = \mathfrak{q}_a\mathfrak{q}_b$ donde $\mathfrak{q}_\alpha = (\tau_\alpha)$ para $\alpha = a, b$, es un ideal que divide a α. Observar que $\mathfrak{q}_\alpha$ puede ser un ideal primo arriba de 2 o ser (1). Esto va a depender de la curva elíptica en cuestión y del cuerpo K. En nuestro caso, si $d = 5, 13, 21$, tenemos que 2 es inerte, y por lo tanto las combinaciones posibles para (τ_a, τ_b) son $(2, 1)$ o $(1, 2)$. En $d = 17$, tenemos que 2 descompone en los ideales primos

$(2+\sqrt{17})$ y $(2-\sqrt{17})$, y dependiendo de la curva elíptica tenemos cuatro combinaciones posibles para (τ_a, τ_b): $(2,1), (1,2), (2+\sqrt{17}, 2-\sqrt{17}), (2-\sqrt{17}, 2+\sqrt{17})$.

El siguiente teorema permite reducir las posibilidades para a y b si conocemos el primo $\mathfrak{p}$ que divide al conductor de E:

Teorema **6.20.** *Sea K cuerpo cuadrático, $E_{a,b}/K$ una curva elíptica con conductor potencia de primo impar. Definimos:*

- $P = \gcd(\Delta^{min}(E), b, a^2-4b) = As^2$ *con A libre de cuadrados,*
- $B = \frac{a^2-4b}{\tau_a^2 P}$,
- $C = \frac{4b}{\tau_a^2 P}$,
- $\widetilde{a} = \frac{as}{\tau_a^2 P}$.

Entonces se cumple que

- $\widetilde{a}, A, B, C \in \mathcal{O}_K$,
- $\gcd(B, C) = 1$,
- *A, B, C solo son divisibles por primos que dividan a 2 y por $\mathfrak{p}$,*
- $j = \min\left\{\nu_{\mathfrak{p}}(b), \nu_{\mathfrak{p}}(a^2-4b)\right\} \leq 3$,
- $\widetilde{a}^2 A = B + C$,
- *Los valores posibles para las valuaciones de las variables anteriores según $\mathfrak{p}$ y según $\mathfrak{q}$ (primo arriba de 2), vienen dados por las tablas 6.1 y 6.2 donde $k = \nu_{\mathfrak{p}}(\Delta^{min}(E))$:*

$\nu_{\mathfrak{p}}(a)$	$\nu_{\mathfrak{p}}(b)$	$\nu_{\mathfrak{p}}(a^2-4b)$	j	k	$\nu_{\mathfrak{p}}(A)$	$\nu_{\mathfrak{p}}(B)$	$\nu_{\mathfrak{p}}(C)$
0	0	≥ 0	0	≥ 0	0	k	0
≥ 1	0	0	0	0	0	0	0
0	≥ 1	0	0	≥ 2, par	0	0	$\frac{k}{2}$
≥ 1	1	1	1	3	1	0	0
1	2	≥ 2	2	≥ 6	0	$k-6$	0
≥ 2	2	2	2	6	0	0	0
1	≥ 3	2	2	≥ 8, par	0	0	$\frac{k-6}{2}$
≥ 2	3	3	3	9	1	0	0

Tabla 6.1: Distintas opciones de valuaciones $\mathfrak{p}$-ádicas.

Recíprocamente, dados $A, B, C, \widetilde{a} \in \mathcal{O}_K$ que satisfacen las condiciones de arriba, definen una curva elíptica $E_{a,b}$ con $a = \frac{2A\widetilde{a}}{\gcd(2,C)}$ y $b = \frac{AC}{\gcd(2,C)^2}$ con buena reducción fuera de $2\mathfrak{p}$.

Demostración. Ver Teorema 5.4 de [8]. □

Reducción	$\nu_{\mathfrak{q}}(a)$	$\nu_{\mathfrak{q}}(b)$	$\nu_{\mathfrak{q}}(a^2-4b)$	$\nu_{\mathfrak{q}}(4b)$	$\nu_{\mathfrak{q}}(A)$	$\nu_{\mathfrak{q}}(B)$	$\nu_{\mathfrak{q}}(C)$
Ordinaria	0	$4e_2$	0	$6e_2$	0	0	$6e_2$
Supersingular	≥ 3	0	4	4	0	0	0

Tabla 6.2: Distintas opciones de valuaciones $\mathfrak{q}$-ádicas.

Definición **6.21.** *Sea E/K una curva elíptica. Un* ***twist cuadrático*** *de E es una curva elíptica isomorfa a E en una extensión cuadrática de K.*

Para curvas elípticas de la forma $E_{a,b}$, los twists cuadráticos son de la forma $E_{\lambda a,\lambda^2 b}$ con $\lambda \in K^\times$. No es difícil ver que

$$\Delta(E_{a,b}) = \lambda^6 \Delta(E_{\lambda a,\lambda^2 b}),$$

por lo que el discriminante puede escalarse por potencias sextas si nos restringimos a estudiar las curvas elípticas módulo twists cuadráticos. El siguiente resultado simplifica un poco más la clasificación si también trabajamos módulo isogenias:

Teorema **6.22.** *Sea $E_{a,b}$ una curva elíptica con parámetros (A, B, C) según la notación del Teorema 6.20. Entonces E_{-2a,a^2-4b} es isógena y tiene parámetros (A, C, B).*

Demostración. Ver proposición 5.6 de [8]. □

Teorema **6.23.** *Sea K algunos de los cuerpos considerados, E/K una curva elíptica con conductor potencia de primo impar $\mathfrak{p}$ y con un twist cuadrático con buena reducción en $\mathfrak{p}$. Entonces, las opciones para E son:*

1. *E tiene reducción ordinaria sobre K, $A = \pm\epsilon_f^k \pi^j$ con π generador de $\mathfrak{p}$, $k \in \mathbb{Z}$ y $j \in \mathbb{N}$, $B = u2^6$ con $u \in \mathcal{O}_K^\times$, $C = 1$ y alguno del conjunto $\{\pm(B+C), \pm(B+C)/\epsilon_f, \pm(B+C)/\pi, \pm(B+C)/\epsilon_f\pi\}$ es un cuadrado.*
2. *E tiene reducción ordinaria en $K = \mathbb{Q}(\sqrt{17})$, $A = \pm\epsilon_f^k \pi^j$ con π generador de $\mathfrak{p}$, $k \in \mathbb{Z}$ y $j \in \mathbb{N}$, $B = u\tau_1^6$ con $u \in \mathcal{O}_K^\times$, $C = \tau_2^6$ y alguno de $\{\pm(B+C), \pm(B+C)/\epsilon_f, \pm(B+C)/\pi, \pm(B+C)/\epsilon_f\pi\}$ es un cuadrado (recordar que τ_α son los generadores de los ideales arriba de 2).*
3. *E tiene reducción supersingular en $K = \mathbb{Q}(\sqrt{d})$ con $d = 2, 3$, $A = \pm\epsilon_f^k \pi^j$ con π generador de $\mathfrak{p}$, $k \in \mathbb{Z}$ y $j \in \mathbb{N}$, $B \in \mathcal{O}_K^\times$, $C = 1$ y alguno de $\{\pm(B+C), \pm(B+C)/\epsilon_f, \pm(B+C)/\pi, \pm(B+C)/\epsilon_f\pi\}$ es un cuadrado.*

Demostración. Por la observación de que podemos escalar el discriminante por potencias sextas, sabemos que k es múltiplo de 6. Como tiene mala reducción en $\mathfrak{p}$, no puede ser múltiplo de 12. Luego, $k = 6$. La tabla 6.1 solo da dos columnas posibles para $k = 6$, y en ambos casos, $(\nu_{\mathfrak{p}}(B), \nu_{\mathfrak{p}}(C)) = (0, 0)$. Si miramos la tabla 6.2, solo uno de B o C puede ser dividido por $\mathfrak{q}$. Más aún, por el Teorema 6.22, podemos asumir que $(\nu_{\mathfrak{q}}(B), \nu_{\mathfrak{q}}(C)) = (6e_2, 0)$ en el caso ordinario. En el caso supersingular,

$(\nu_{\mathfrak{p}}(B), \nu_{\mathfrak{p}}(C)) = (0, 0)$.

Consideremos primero los cuerpos donde 2 no descompone. Como solo $\mathfrak{p}$ y $\mathfrak{q}$ pueden dividir a B y a C, tenemos que en ambos casos C es una unidad. Dado que P es un máximo común divisor, está definido a menos de unidades, y por ende se puede elegir un representante tal que $C = 1$. Por otro lado, como la valuación en una suma es mayor o igual al mínimo de las valuaciones de los elementos, tenemos que $B + C = \widetilde{a}^2 A$ no es divisible por $\mathfrak{q}$, y como $\mathfrak{p}$ y $\mathfrak{q}$ son los únicos primos que pueden dividir a A (por el Teorema 6.20 y porque 2 no descompone), concluimos que $A = \pm\epsilon_f^k \pi^j$ con π generador de $\mathfrak{p}$, $k \in \mathbb{Z}$ y $j \in \mathbb{N}$. Agrupando en $\widetilde{a}$, obtenemos que alguno del conjunto $\{\pm(B+C), \pm(B+C)/\epsilon_f, \pm(B+C)/\pi, \pm(B+C)/\epsilon_f\pi\}$ debe ser un cuadrado.

Si 2 descompone, tiene dos ideales primos generados por τ_1 y τ_2 arriba, y entonces C no necesariamente es una unidad, ya que puede ser divisible por el otro primo arriba de 2. Si C no es una unidad, entonces C puede tomarse como τ_2^6, escalando por unidades como se explicaba en el párrafo anterior. La potencia sexta, surge de aplicar la tabla 6.2 al primo $\mathfrak{q}_2$ y el hecho de que si 2 descompone, entonces $e_2 = 1$. En nuestro caso, esto solo puede ocurrir si $d = 17$ y E tiene reducción ordinaria en ambos primos arriba de 2 (porque si no, 2 debería ramificar por el Teorema 6.18). Si $\nu_{\mathfrak{q}_2}(C) = 6$, entonces la tabla 6.2, indica que $\nu_{\mathfrak{q}_2}(B) = 0$, y como estamos considerando que $\nu_{\mathfrak{q}_1}(B) = 6$, entonces tenemos que $B = u\tau_1^6$ con $u \in \mathcal{O}_K^\times$. El parámetro A sigue siendo $\pm\epsilon_f^k \pi^j$ y por lo tanto alguno del conjunto $\{\pm(B+C), \pm(B+C)/\epsilon_f, \pm(B+C)/\pi, \pm(B+C)/\epsilon_f\pi\}$ debe ser un cuadrado.

Consideremos el caso que E tiene reducción ordinaria en algún primo arriba de 2 y C es una unidad. Por el Teorema 6.18 aplicado como en el párrafo anterior, tenemos que E tiene reducción ordinaria en todos los primos arriba de 2 y por lo tanto $B = u2^6$ con $u \in \mathcal{O}_K^\times$ en cualquiera de los tres casos de ramificación del 2. Las opciones de π posibles se obtienen del hecho de que $(B, C) = (u2^6, 1)$.

Si E tiene reducción supersingular, entonces $d = 2, 3$ y B es también una unidad. □

No tenemos ejemplos porque no fueron implementados los programas que realizan los casos del Teorema 6.23.

6.5. Curvas elípticas con 3-torsión

En esta sección, solo analizaremos el caso de curvas elípticas E/K con conductor primo impar que tienen puntos de 3-torsión en K, donde 3 no ramifica en K. Las curvas con un punto de 3-torsión en K, tienen un modelo de la forma

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

donde $(0,0)$ es el punto de orden 3 (ver [24]). El discriminante para una curva de esa forma es

$$\Delta(E) = a_3^3(a_1^3 - 27a_3),$$

y por lo tanto $a_3 \neq 0$. El cambio de variable admisible, transforma $(a_1, a_3) \mapsto (ua_1, u^3a_3)$. Por lo tanto, podemos escalar en cada primo $\mathfrak{q}$, de forma que $\mathfrak{q} \nmid a_1$ o que $\mathfrak{q}^3 \nmid a_3$.

La estrategia será encontrar la forma que deben tener a_1 y a_3 y luego programar para encontrar posibles curvas elípticas.

Teorema **6.24.** *Sea K alguno de los cuerpos considerados donde 3 no ramifica. Sea E/K una curva elíptica con conductor potencia de primo que tiene un punto de 3-torsión en K. Tenemos los siguientes casos:*

1. $(a_1, a_3) = (1, \frac{1+u}{27})$, *con $u \in \mathcal{O}_K^\times$ y solo un primo $\mathfrak{p}$ divide a a_3,*
2. $(a_1, a_3) = (1, u)$, *con $u \in \mathcal{O}_K^\times$ y solo un primo $\mathfrak{p}$ divide a $1 - 27u$,*
3. $(a_1, a_3) = (0, \epsilon_f^k \pi^j)$, *con $j, k \leq 2$ y $\mathfrak{p} \mid 3$,*
4. $(a_1^3, a_3) = (\pi^j(27\epsilon_f^k + u), \epsilon_f^k \pi^j)$ *con $u \in \mathcal{O}_K^\times$ y $j, k \leq 2$, $\mathfrak{p} \nmid 3$ y $\mathfrak{p} \mid a_1$,*
5. $(a_1^3, a_3) = (u\pi^r + 27\epsilon_f^k, \epsilon_f^k)$, *con $u \in \mathcal{O}_K^\times$, $k \leq 2$ y $r \leq 11$. Si $\mathfrak{p} \mid a_1$ entonces $3 \leq r \leq 11$, $\mathfrak{p} \mid 3$ y $\nu_{\mathfrak{p}}(a_1) = 1$ (esta última condición se cumple automáticamente si $r > 3$).*
6. $(a_1^3, a_3) = (27\epsilon_f^k \pi^j + u\pi^3, \epsilon_f^k \pi^j)$, *con $u \in \mathcal{O}_K^\times$, $k \leq 2$, $0 < j \leq 2$ y $\mathfrak{p} \mid 3$,*
7. $(a_1^3, a_3) = (\pi^j(27\epsilon_f^k + \pi^3 u), \epsilon_f^k \pi^j)$ *con $u \in \mathcal{O}_K^\times$, $j, k \leq 2$, y $\mathfrak{p} \mid 3$,*
8. $(a_1^3, a_3) = (27u\pi^j + \epsilon_f^k, u\pi^j)$, *con $u \in \mathcal{O}_K^\times$ y $k \leq 2$,*

Demostración. De forma análoga al Teorema 4.3 de [8], veamos que el modelo es minimal en todos los primos. En efecto, supongamos que no lo es para algún primo $\mathfrak{q}$. Por el Teorema 3.21, $\mathfrak{q}^6 \mid c_6$ y $\mathfrak{q}^{12} \mid \Delta(E)$. Usando las igualdades de la página 42 de [46], se puede ver que el ideal generado por c_6 y $\Delta(E)$ en $\mathbb{Z}[a_1, a_3]$ contiene a a_1^{15} y a $3^3 a_3^5$, y por lo tanto $\mathfrak{q} \mid a_1$, $\mathfrak{q} \mid a_3$ y por ende $\nu_{\mathfrak{q}}(a_3) \leq 2$. Utilizando la ecuación del discriminante, obtenemos que $\nu_{\mathfrak{q}}(\Delta(E)) \leq 11$ lo que nos lleva a una contradicción (si $\mathfrak{q} \mid 3$, hay que usar también el hecho de que como 3 no ramifica en K, $\nu_{\mathfrak{q}}(27) = 3$).

Para inspeccionar en los valores posibles de a_1 y a_3 separaremos en casos.

(1) Si a_1 es una unidad, escalando puedo asumir que $a_1 = 1$ y entonces $\Delta(E) = a_3^3(1 - 27a_3)$. Observamos que $\mathfrak{p}$ no puede dividir a ambos factores, puesto que si lo hace, $\mathfrak{p} \mid 1$. Esto nos da dos casos:

(1.1) Si $\mathfrak{p} \mid a_3$, entonces $1 - 27a_3 = u \in \mathcal{O}_K^\times$ (caso 1).

(1.2) Si $\mathfrak{p} \mid (1 - 27a_3)$, entonces $a_3 \in \mathcal{O}_K^\times$ (caso 2).

(2) Si $a_1 = 0$, entonces $\Delta(E) = -27a_3^4$, y como solo un primo divide al discriminante, entonces $\mathfrak{p} \mid 3$. Por lo tanto $a_3 = u\pi^j$ siendo π generador de $\mathfrak{p}$. Como el modelo es minimal, entonces $j \leq 2$, y escalando la curva por unidades tenemos que $u = \epsilon_f^k$ con $k = 0, 1, 2$ (caso 3).

(3) Si $a_1 \notin \mathcal{O}_K^\times \cup \{0\}$, separamos según $\mathfrak{p}$:

(3.1) Si $\mathfrak{p} \mid a_1$, entonces $\mathfrak{p}^3 \nmid a_3$. Escalando por unidades como en el caso (2.2), tenemos que $a_3 = \epsilon_f^k \pi^j$ con $k, j \in \{0, 1, 2\}$ (no puede haber otro primo que divida a a_3 por que el discriminante es potencia de $\mathfrak{p}$).

(3.1.1) Si $\mathfrak{p} \nmid 3$, tenemos que $\nu_\mathfrak{p}(a_1^3) \geq 3$ y que $\nu_\mathfrak{p}(-27a_3) = \nu_\mathfrak{p}(a_3) = j < 3$, así que $\nu_\mathfrak{p}(a_1^3 - 27a_3) = j$ y entonces $a_1^3 - 27a_3 = u\pi^j$ con $u \in \mathcal{O}_K^\times$. Juntando ambas expresiones y despejando tenemos que $a_1^3 = \pi^j(27\epsilon_f^k + u)$ (caso 4).

(3.1.2) Si $\mathfrak{p} \mid 3$, separamos en dos casos:

(3.1.2.1) Si $\nu_\mathfrak{p}(a_1) = 1$, entonces separamos aún más:

(3.1.2.1.1) Si $\nu_\mathfrak{p}(a_3) = 0$, las valuaciones de $\nu_\mathfrak{p}(a_1^3)$ y $\nu_\mathfrak{p}(-27a_3)$ se igualan y no podemos saber la valuación de $\nu_\mathfrak{p}(a_1^3 - 27a_3)$. Lo que sí sabemos es que $a_3 = \epsilon_f^k$ y que a $a_1^3 - 27a_3$ solo lo divide $\mathfrak{p}$, por lo que entonces $\Delta(E) = u\pi^r = \epsilon_f^{3k}(a_1^3 - 27\epsilon_f^k)$ con $u \in \mathcal{O}_K^\times$ y $r = 3, ..., 11$ debido a que $\nu_\mathfrak{p}(a_1^3 - 27a_3) \geq \min\left\{\nu_\mathfrak{p}(a_1^3), \nu_\mathfrak{p}(-27a_3)\right\} = 3$. Despejando, tenemos que $a_1^3 = \frac{u\pi^r}{\epsilon_f^{3k}} + 27\epsilon_f^k$ (caso 5).

(3.1.2.1.2) Si $\nu_\mathfrak{p}(a_3) = j \geq 1$, entonces $\nu_\mathfrak{p}(a_1^3 - 27a_3) = 3$, y por lo tanto $a_1^3 = 27a_3 + u\pi^3$ (caso 6).

(3.1.2.2) Si $\nu_\mathfrak{p}(a_1) \geq 2$, entonces $\nu_\mathfrak{p}(a_1^3) \geq 6$ y $\nu_\mathfrak{p}(-27a_3) \leq 5$, así que entonces $\nu_\mathfrak{p}(a_1^3 - 27a_3) = 3 + j$, lo que implica que $a_1^3 = 27a_3 + \pi^{3+j}u = \pi^j(27\epsilon_f^k + \pi^3 u)$ con $u \in \mathcal{O}_K^\times$ (caso 7).

(3.2) Si $\mathfrak{p} \nmid a_1$, separamos según a_3:

(3.2.1) Si $a_3 \notin \mathcal{O}_K^\times$, entonces $\mathfrak{p}$ es el único primo que divide a a_3. Observar que si $\mathfrak{p} \mid (a_1^3 - 27a_3)$, entonces $\mathfrak{p} \mid a_1$ lo cual es absurdo. Esto muestra entonces que $a_1^3 - 27a_3 = v \in \mathcal{O}_K^\times$. Escalando por u, nos queda $u^3 v$, y por lo tanto podemos tomar $v = \epsilon_f^k$ con $k = 0, 1, 2$. Por otro lado, $a_3 = u\pi^j$ y entonces $a_1^3 = 27u\pi^j + \epsilon_f^k$ (caso 8).

(3.2.2) Si $a_3 \in \mathcal{O}_K^\times$, escalando podemos tomar $a_3 = \epsilon_f^k$ con $k = 0, 1, 2$. Ob-

servemos que $\mathfrak{p} \nmid 3$. En efecto, si lo hace, $\mathfrak{p} \mid (a_1^3 - 27a_3)$ y $\mathfrak{p} \mid 27a_3$, y por lo tanto $\mathfrak{p} \mid a_1$ lo cual es absurdo. Por otro lado, como en el caso (3.1.2.1.1), $\Delta(E) = u\pi^r = \epsilon_f^{3k}(a_1^3 - 27\epsilon_f^k)$, y entonces $a_1^3 = \frac{u\pi^r}{\epsilon_f^{3k}} + 27\epsilon_f^k$ (caso 5).

□

Como no sabemos quien es $\mathfrak{p}$, en el punto 4, a la hora de buscar curvas elípticas, tomamos π en función de los primos que dividen a $(27\epsilon_f^k + u)$, de forma que la expresión de a_1 sea un cubo. Los puntos 5 y 8, no pueden ser actualmente implementados en su totalidad, debido que dependen del primo $\mathfrak{p}$. Para el resto de los puntos (incluido un caso del 5), aparecen involucrados una cantidad finita de primos, que son los que dividen a 3. Los programas que buscan curvas elípticas usando el Teorema 6.24 se encuentran en PROGRAMA 4 en el apéndice. El mismo se encuentra separado por procedimientos según el caso, numerados como en el Teorema 6.24.

Para el caso 1 buscamos curvas para unidades $u = \pm\epsilon_f^k$ con $k \in [-2000, 2000]$ y no encontramos ninguna en ninguno de los cuerpos considerados.

Para el caso 2, buscamos curvas en el rango de $k \in [-2000, 2000]$ para $d = 2, 5, 17$. En $\mathbb{Q}(\sqrt{2})$ no obtuvimos curvas, en $\mathbb{Q}(\sqrt{5})$ obtuvimos 160 curvas elípticas todas con $\nu_{\mathfrak{p}}(\Delta(E)) = 1$ y en $\mathbb{Q}(\sqrt{17})$ no obtuvimos curvas. Para $\mathbb{Q}(\sqrt{13})$ buscamos en el rango $k \in [-1000, 1000]$ y obtuvimos 46 curvas elípticas todas con $\nu_{\mathfrak{p}}(\Delta(E)) = 1$.

En el caso 3, debemos analizar tres curvas por cada cuerpo. Es claro que $(\Delta(E)) = (27\pi^{4j})$, por lo que solo en los cuerpos K donde 3 es primo, la curva E va a tener conductor potencia de primo. Estos cuerpos son $d = 2, 5, 17$. En todos los cuerpos, el valor de $\nu_{\mathfrak{p}}(N(E))$ depende de j, siendo $j = \nu_{\mathfrak{p}}(a_3)$, de la siguiente forma:

$$\nu_{\mathfrak{p}}(N(E)) = \begin{cases} 3 & \text{si } j = 0 \\ 5 & \text{si } j = 1, 2 \end{cases}$$

En el caso 4, el programa era más complejo, y buscamos en el rango de $k \in [-100, 100]$ para $d = 2, 5, 13$. De la propia demostración del Teorema 6.24 obteníamos que $\nu_{\mathfrak{p}}(\Delta(E)) = 4, 8$, pero sólo obtuvimos curvas con valuación de discriminante 8. En $\mathbb{Q}(\sqrt{2})$ obtuvimos 10 curvas. En $\mathbb{Q}(\sqrt{5})$ obtuvimos 70 curvas elípticas. En $\mathbb{Q}(\sqrt{13})$, obtuvimos 26 curvas. En $\mathbb{Q}(\sqrt{17})$ no obtuvimos curvas en el rango de $k \in [-85, 85]$, aunque sospechamos que existen curvas en el rango entre ± 80 y ± 100 puesto que el programa se estancaba ahí. Debido a que son muchas, no mostraremos los resultados.

En el caso 5, solo para cuando $\mathfrak{p} \mid 3$, en el rango $k \in [-2000, 2000]$ obtuvimos 25 curvas entre todos los cuerpos considerados. De la propia demostración del Teorema 6.24 obteníamos que $\nu_{\mathfrak{p}}(\Delta(E)) \geq 3$, pero obtuvimos curvas con valuación de discriminante hasta 5 (ver tabla 6.4).

En el caso 6, en el rango de $k \in [-2000, 2000]$ obtuvimos 9 curvas entre todos los cuerpos considerados. De la propia demostración del Teorema 6.24 obteníamos que $\nu_{\mathfrak{p}}(\Delta(E)) = 3, 6$ o 9, y obtuvimos curvas en cada uno de los casos (ver tabla 6.3).

d	a_1	a_3	$N(E)$	**Norma de $N(E)$**	**Discriminante**
2, 5, 17	6	9	$(3)^3$	729	-3^9
2	$-3\sqrt{2}$	3	$(3)^4$	6561	$-\epsilon_f^{-2}\, 3^6$
2	$3\sqrt{2}$	3	$(3)^4$	6561	$-\epsilon_f^{2}\, 3^6$
5	6	$\epsilon_f^2\, 3$	$(3)^4$	6561	$\epsilon_f^{2}\, 3^6$
5	$\frac{3+3\sqrt{2}}{2}$	ϵ_f^3	$(3)^4$	6561	$-\epsilon_f^{2}\, 3^6$
5	3	$\epsilon_f^2\, 3$	$(3)^4$	6561	$-\epsilon_f^{10}\, 3^6$
5	$3+3\sqrt{2}$	$\epsilon_f\, 3$	$(3)^4$	6561	$\epsilon_f^{10}\, 3^6$

Tabla 6.3: Curvas elípticas en el caso 7 del Teorema 6.24.

Finalmente en el caso 7, en el rango de $k \in [-2000, 2000]$ obtuvimos 43 curvas entre todos los cuerpos considerados. De la propia demostración del Teorema 6.24 obteníamos que $\nu_{\mathfrak{p}}(\Delta(E)) = 3, 7$ u 11, y obtuvimos curvas en cada uno de los casos. Debido a que son muchas, no mostraremos los resultados.

Si en analogía con la tabla 5.2, buscamos las curvas elípticas de conductor primo con $\nu_{\mathfrak{p}}(\Delta(E)) > 1$, no encontramos ninguna en esta sección.

d	a_1	a_3	$N(E)$	**Norma de $N(E)$**	**Discriminante**
2, 5, 17	-6	1	$(3)^3$	729	-3^5
2	$-3\sqrt{2}$	ϵ_f	$(3)^2$	81	$\epsilon_f^2\, 3^3$
2	$-6+3\sqrt{2}$	ϵ_f	$(3)^4$	6561	$-\epsilon_f^6\, 3^4$
2	$-3\sqrt{2}$	ϵ_f^2	$(3)^4$	6561	$-\epsilon_f^6\, 3^4$
2	$6-3\sqrt{2}$	ϵ_f^2	$(3)^2$	81	$\epsilon_f^{10}\, 3^3$
5	$-3+3\sqrt{2}$	ϵ_f	$(3)^4$	6561	$\epsilon_f^{-2}\, 3^4$
5	$\frac{15-3\sqrt{2}}{2}$	ϵ_f^2	$(3)^2$	81	$\epsilon_f^{-2}\, 3^3$
5	3	ϵ_f	$(3)^2$	81	$-\epsilon_f^2\, 3^3$
5	$\frac{3-3\sqrt{2}}{2}$	ϵ_f	$(3)^4$	6561	$-\epsilon_f^2\, 3^4$
5	-3	ϵ_f	$(3)^3$	729	$-\epsilon_f^5\, 3^3$
5	$\frac{3+3\sqrt{2}}{2}$	ϵ_f	$(3)^3$	729	$\epsilon_f^5\, 3^3$
5	3	ϵ_f^2	$(3)^3$	729	$-\epsilon_f^7\, 3^3$
5	$\frac{3+3\sqrt{2}}{2}$	ϵ_f^2	$(3)^3$	729	$\epsilon_f^7\, 3^3$
5	$\frac{-3-3\sqrt{2}}{2}$	ϵ_f^2	$(3)^2$	81	$-\epsilon_f^{10}\, 3^3$
5	$\frac{-9-3\sqrt{2}}{2}$	ϵ_f^2	$(3)^4$	6561	$-\epsilon_f^{10}\, 3^4$
5	$\frac{15+9\sqrt{2}}{2}$	ϵ_f	$(3)^2$	81	$\epsilon_f^{14}\, 3^3$
5	$9+3\sqrt{2}$	ϵ_f^2	$(3)^4$	6561	$\epsilon_f^{14}\, 3^4$
13	$1+\sqrt{13}$	ϵ_f	$(\frac{1+\sqrt{13}}{2})^4$	81	$\epsilon_f^2\, (\frac{1+\sqrt{13}}{2})^4$
13	$\frac{5+\sqrt{13}}{2}$	ϵ_f	$(\frac{1-\sqrt{13}}{2})^4$	81	$-\epsilon_f^4\, (\frac{1-\sqrt{13}}{2})^4$
13	$\frac{-1-\sqrt{13}}{2}$	ϵ_f^2	$(\frac{1+\sqrt{13}}{2})^4$	81	$-\epsilon_f^8\, (\frac{1+\sqrt{13}}{2})^4$
13	$5+\sqrt{13}$	ϵ_f^2	$(\frac{1-\sqrt{13}}{2})^4$	81	$\epsilon_f^{10}\, (\frac{1-\sqrt{13}}{2})^4$
17	6	ϵ_f	$(3)^2$	81	$-\epsilon_f^2\, 3^3$
17	$-24-6\sqrt{17}$	ϵ_f^2	$(3)^2$	81	$-\epsilon_f^{10}\, 3^3$

Tabla 6.4: Curvas elípticas en el caso 6 del Teorema 6.24.

6.6. Curvas elípticas con 5-torsión

Ahora nos encargamos de las curvas elípticas E/K con conductor primo impar que tienen puntos de 5-torsión en K, donde 5 no ramifica en K. Las curvas con un

punto de 5-torsión en K, tienen un modelo de la forma

$$E : y^2 + (b-a)xy - ab^2y = x^3 - abx^2$$

con $\gcd(a,b) = 1$ (ver [24]). El discriminante para una curva de esa forma es

$$\Delta(E) = a^5b^5(a^2 - 11ab - b^2),$$

y por lo tanto $a, b \neq 0$. El cambio de variable admisible, transforma $(a,b) \mapsto (ua, ub)$. Por lo tanto, podemos escalar en cada primo $\mathfrak{q}$, de forma que $\mathfrak{q} \nmid a$ o que $\mathfrak{q} \nmid b$.

Como en la sección 6.5, la estrategia será encontrar la forma que deben tener a y b y luego programar para encontrar posibles curvas elípticas.

Teorema **6.25.** *Sea K alguno de los cuerpos considerados donde 5 no ramifica. Sea E/K una curva elíptica con conductor potencia de primo que tiene un punto de 5-torsión en K. Tenemos los siguientes casos:*

1. $(a,b) = (1, \pm\epsilon_f^k)$ *tal que* $(\Delta(E)) = (1 \pm 11\epsilon_f^k - \epsilon_f^{2k})$ *es potencia de un primo.*
2. $(a, 1 - 11b - b^2) = (1, u)$ *con* $u \in \mathcal{O}_K^\times$ *y tal que* $(\Delta(E)) = (b^5)$ *es potencia de un primo.*
3. $(a^2 - 11a - 1, b) = (u, 1)$ *con* $u \in \mathcal{O}_K^\times$ *y tal que* $(\Delta(E)) = (a^5)$ *es potencia de un primo.*

Demostración. Veamos que el modelo es minimal en todos los primos de igual forma que es hecho en el Teorema 4.7 de [8]. En efecto, como en el Teorema 6.24 supongamos que no lo es para un primo $\mathfrak{q}$. Por el teorema 3.21, $\mathfrak{q}^4 \mid c_4$ y $\mathfrak{q}^{12} \mid \Delta(E)$, donde $c_4 = a^4 - 12a^3b + 14a^2b^2 + 12ab^3 + b^4$. En el anillo $\mathbb{Z}[a,b]$ el ideal generado por c_4 y $\Delta(E)$ contiene a $5a^{15}$ y $5b^{15}$, que son coprimos salvo en los primos que dividen a 5. Si $\mathfrak{q} \nmid 5$, entonces divide a uno de a o b y entonces $\nu_{\mathfrak{q}}(\Delta(E)) < 6$. Si ahora $\mathfrak{q} \mid 5$, entonces, $c_4 \equiv (a+2b)^4 \equiv 0 \pmod{\mathfrak{q}}$, lo que implica que $\mathfrak{q} \mid (a+2b)$. Si ponemos $c = a + 2b$ y sustituímos $a = c - 2b$ en la expresión de c_4 y usamos el hecho de que $\mathfrak{q} \mid c$ y que $\mathfrak{q}^2 \nmid 5$ porque 5 no ramifica, obtenemos que $c_4 \equiv -5b^4 \pmod{\mathfrak{q}^2}$. Por otro lado, $\mathfrak{q} \nmid b$, puesto que si lo hace, $\mathfrak{q} \mid a$, pero estos son coprimos. Por lo tanto, $\mathfrak{q}^2 \nmid c_4$, lo cual es absurdo y entonces E es minimal en $\mathfrak{q} \mid 5$ también.

Sea $\mathfrak{p}$ el ideal primo que divide al discriminante. El caso de 5-torsión, es más sencillo que el de 3-torsión, puesto que $\Delta(E)$ está compuesto por tres términos que son dos a dos coprimos, puesto que si divide a dos de ellos, obtenemos que $\mathfrak{p} \mid a, b$. Esto hace que dos de los tres términos sean unidades.

(1) Si a y b son unidades, escalando podemos asumir que $a = 1$ y $b = \pm\epsilon_f^k$. Entonces, basta con ver si $(\Delta(E)) = (1 \pm 11\epsilon_f^k - \epsilon_f^{2k})$ es potencia de un primo.

(2) Si a y $a^2 - 11ab - b^2$ son unidades, escalando podemos asumir que $a = 1$ y entonces $1 - 11b - b^2 = u$ con $u \in \mathcal{O}_K^\times$. Luego, se resuelve b en $\mathcal{O}_K$ y se chequea que $(\Delta(E)) = (b^5)$ sea potencia de un primo.

(3) Si b y $a^2 - 11ab - b^2$ son unidades, escalando podemos asumir que $b = 1$ y entonces $a^2 - 11a - 1 = u$ con $u \in \mathcal{O}_K^\times$. Luego, se resuelve a en $\mathcal{O}_K$ y se chequea que $(\Delta(E)) = (a^5)$ sea potencia de un primo.

□

Los programas que buscan curvas elípticas usando el Teorema 6.25 se encuentran en PROGRAMA 5 en el apéndice. El mismo se encuentra separado por procedimientos según el caso, numerados como en el Teorema 6.25.

Para el caso 1 buscamos curvas para unidades $u = \pm\epsilon_f^k$ con $k \in [-750, 750]$ para $d = 2, 3, 13, 21$. En $\mathbb{Q}(\sqrt{2})$ obtuvimos 56 curvas de las cuales 4 tenían $\nu_{\mathfrak{p}}(\Delta(E)) > 1$, siendo de hecho igual a 2 en los 4 casos. En $\mathbb{Q}(\sqrt{3})$ obtuvimos 64 curvas elípticas todas con $\nu_{\mathfrak{p}}(\Delta(E)) = 1$. En $\mathbb{Q}(\sqrt{13})$ obtuvimos 22 curvas donde solo dos de ellas tenían $\nu_{\mathfrak{p}}(\Delta(E)) > 1$, siendo de hecho igual a 2. Para $\mathbb{Q}(\sqrt{21})$ obtuvimos 2 curvas, ambas con $\nu_{\mathfrak{p}}(\Delta(E)) = 1$. Finalmente, para $\mathbb{Q}(\sqrt{17})$ buscamos en el rango $k \in [-500, 500]$ y obtuvimos 18 curvas elípticas todas con $\nu_{\mathfrak{p}}(\Delta(E)) = 1$. Como en la sección 6.5, mostramos en la tabla sólo las curvas con $\nu_{\mathfrak{p}}(\Delta(E)) > 1$.

d	a	b	$N(E)$	**Norma de** $N(E)$	**Discriminante**
2	1	$-\epsilon_f^{-3}$	$(5)^2$	625	$-\epsilon_f^{-18}\,5^2$
2	1	ϵ_f^{-1}	$(3)^1$	9	$-\epsilon_f^{-6}\,3^2$
2	1	$-\epsilon_f$	$(3)^1$	9	$-\epsilon_f^{6}\,3^2$
2	1	ϵ_f^{3}	$(5)^2$	625	$-\epsilon_f^{18}\,5^2$
13	1	ϵ_f^{-3}	$(5)^2$	625	$\epsilon_f^{-18}\,5^2$
13	1	$-\epsilon_f^{3}$	$(5)^2$	625	$\epsilon_f^{18}\,5^2$

Tabla 6.5: Curvas elípticas en el caso 1.

Para el caso 2, en el rango de $k \in [-2000, 2000]$ obtuvimos 1 curva racional. De la propia demostración del Teorema 6.24 obteníamos que $\nu_{\mathfrak{p}}(\Delta(E))$ debía ser un múltiplo de 5 y de hecho, es 5 (ver tabla 6.6). Esta curva obtenida es la curva 11.a2 según la nomenclatura de [26], que también aparecía en la tabla 5.2.

Finalmente para el caso 3, en el rango de $k \in [-2000, 2000]$ obtuvimos 1 curva racional. De la propia demostración del Teorema 6.24 obteníamos que $\nu_{\mathfrak{p}}(\Delta(E))$ debía ser un múltiplo de 5 y de hecho, es 5 (ver tabla 6.7). Esta curva obtenida es también la curva 11.a2 según la nomenclatura de [26], que mostrábamos en la

d	a	b	$N(E)$	**Norma de** $N(E)$	**Discriminante**
2, 3, 13, 17, 21	1	-11	$(11)^1$	121	-11^5

Tabla 6.6: Curvas elípticas en el caso 2.

tabla 5.2, con un cambio de variable con respecto a la del caso 2.

d	a	b	$N(E)$	**Norma de** $N(E)$	**Discriminante**
2, 3, 13, 17, 21	11	1	$(11)^1$	121	-11^5

Tabla 6.7: Curvas elípticas en el caso 3.

Observar que la tabla 6.5 agrega nuestras dos primeras curvas no racionales con conductor primo y discriminante no primo. Es claro que una es la conjugada de la otra, por lo que nos importa solo una de ellas. El buscador de [26], muestra que esta curva está documentada, rotulada como 9.1-a2.

6.7. Curvas elípticas con 7-torsión

Ahora nos encargamos de las curvas elípticas E/K con conductor primo impar que tienen puntos de 7-torsión en K. Las curvas con un punto de 7-torsión en K, tienen un modelo de la forma

$$E : y^2 + (b^2 + ab - a^2)xy - (a^3b^3 - a^2b^4)y = x^3 - (a^3b - a^2b^2)x^2$$

con $\gcd(a, b) = 1$ (ver [24]). El discriminante para una curva de esa forma es

$$\Delta(E) = a^7b^7(a - b)^7(a^3 - 8a^2b + 5ab^2 + b^3),$$

y por lo tanto $a, b \neq 0$. En la prueba, consideraremos dos cambios de variables admisibles. El cambio admisible $(x, y) \mapsto (u^2x, u^3y)$, con $u = a^{-2}$ transforma $(a, b) \mapsto (1, a^{-1}b)$ y con $u = b^{-2}$ transforma $(a, b) \mapsto (b^{-1}a, 1)$.

Como en la secciones 6.5 y 6.6, la estrategia será encontrar la forma que deben tener a y b y luego programar para encontrar posibles curvas elípticas.

Teorema **6.26.** *Sea K alguno de los cuerpos considerados donde 7 no ramifica. Sea E/K una curva elíptica con conductor potencia de primo que tiene un punto de 7-torsión en K. Tenemos los siguientes casos:*

1. $(a, b) = (1, \pm\epsilon_f^k)$ *tal que* $(\Delta(E)) = ((1 \mp \epsilon_f^k)^7(1 \mp 8\epsilon_f^k + 5\epsilon_f^{2k} \pm \epsilon_f^{3k}))$ *es potencia de un primo.*

2. $(a, (1-b)^7(1-8b+5b^2+b^3)) = (1, u)$ *con* $u \in \mathcal{O}_K^\times$ *y tal que* $(\Delta(E)) = (b^7)$ *es potencia de un primo.*

3. $((a-1)^7(a^3-8a^2+5a+1), b) = (u, 1)$ *con* $u \in \mathcal{O}_K^\times$ *y tal que* $(\Delta(E)) = (a^7)$ *es potencia de un primo.*

Demostración. Como en el Teorema 6.25, tenemos que $\gcd(\Delta(E), c_4)$ puede ser divisible solo por primos arriba de 7. En los cuerpos donde 7 no ramifica, un argumento similar al del Teorema 6.25 demuestra que el modelo de E mencionado al comienzo de la sección es minimal.

Sea $\mathfrak{p}$ el ideal primo que divide al discriminante. Separemos $\Delta(E)$ en tres términos: a^7, b^7 y $(a-b)^7(a^3-8a^2b+5ab^2+b^3)$. Como en el Teorema 6.25, estos tres términos deben ser dos a dos coprimos, puesto que si divide a dos de ellos, obtenemos que $\mathfrak{p} \mid a, b$. Esto hace que dos de los tres términos sean unidades.

(1) Si a y b son unidades, escalando por $u = a^{-2}$, podemos asumir que $a = 1$ y $b = \pm\epsilon_f^k$. Entonces, basta con ver si
$(\Delta(E)) = ((1 \mp \epsilon_f^k)^7(1 \mp 8\epsilon_f^k + 5\epsilon_f^{2k} \pm \epsilon_f^{3k}))$ es potencia de un primo.

(2) Si a y $(a-b)^7(a^3-8a^2b+5ab^2+b^3)$ son unidades, escalando como en el caso anterior, podemos asumir que $a = 1$ y entonces $(1-b)^7(1-8b+5b^2+b^3) = u$ con $u \in \mathcal{O}_K^\times$. Luego, se resuelve b en $\mathcal{O}_K$ y se chequea que $(\Delta(E)) = (b^7)$ sea potencia de un primo.

(3) Si a y $(a-b)^7(a^3-8a^2b+5ab^2+b^3)$ son unidades, escalando por $u = b^{-2}$ podemos asumir que $b = 1$ y entonces $(a-1)^7(a^3-8a^2+5a+1) = u$ con $u \in \mathcal{O}_K^\times$. Luego, se resuelve a en $\mathcal{O}_K$ y se chequea que $(\Delta(E)) = (a^7)$ sea potencia de un primo.

□

Los programas que buscan curvas elípticas usando el Teorema 6.26 se encuentran en PROGRAMA 6 en el apéndice. El mismo se encuentra separado por procedimientos según el caso, numerados como en el Teorema 6.26.

Para el caso 1 buscamos curvas para unidades $u = \pm\epsilon_f^k$ con $k \in [-750, 750]$ para todos los cuerpos considerados. El único cuerpo en el que aparecen curvas es $\mathbb{Q}(\sqrt{5})$, en el cual obtuvimos 6 curvas todas con $\nu_{\mathfrak{p}}(N(E)) = \nu_{\mathfrak{p}}(\Delta(E)) = 1$ (ver tabla 6.8).

Para los casos 2 y 3, buscamos curvas en el rango de $k \in [-2000, 2000]$ y no obtuvimos ninguna en ninguno de los cuerpos considerados.

d	a	b	$N(E)$	**Norma de** $N(E)$	**Discriminante**
5	1	ϵ_f^{-2}	$(\frac{13-\sqrt{5}}{2})^1$	41	$-\epsilon_f^{-24} \quad \frac{13-\sqrt{5}}{2}$
5	1	$-\epsilon_f^{-1}$	$(\frac{13+\sqrt{5}}{2})^1$	41	$-\frac{13+\sqrt{5}}{2}$
5	1	ϵ_f^{-1}	$(\frac{13+\sqrt{5}}{2})^1$	41	$-\epsilon_f^{-24} \quad \frac{13+\sqrt{5}}{2}$
5	1	$-\epsilon_f$	$(\frac{13-\sqrt{5}}{2})^1$	41	$-\epsilon_f^{24} \quad \frac{13+\sqrt{5}}{2}$
5	1	ϵ_f	$(\frac{13-\sqrt{5}}{2})^1$	41	$-\frac{13-\sqrt{5}}{2}$
5	1	ϵ_f^2	$(\frac{13+\sqrt{5}}{2})^1$	41	$-\epsilon_f^{24} \quad \frac{13+\sqrt{5}}{2}$

Tabla 6.8: Curvas elípticas en el caso 1.

Apéndice A

Programas en MAGMA

En este capítulo, simplemente copiamos el código de los programas utilizados para realizar operaciones del capítulo 6.

A.1. PROGRAMA 1

En este programa calculamos los cuerpos cuadráticos para el cual el espacio de formas cuspidales nuevas es trivial. Implementado en MAGMA.

```
N := 1000;

for d in [2..N] do
        printf ".";
        if IsSquarefree(d) then
                K := QuadraticField(d);
                if Dimension(NewSubspace(HilbertCuspForms(K, 1*
                    Integers(K)))) eq 0 then
                        print ".";
                        print d;
                end if;
        end if;
end for;
```

A.2. PROGRAMA 2

Programa que busca extensiones de grado 3 para una determinada extensión de un cuerpo K. Implementado en MAGMA.

```
for d in [2,3,5,13,17,21] do
        K:=QuadraticField(d);
        S<y> := PolynomialRing(K);
```

```
        eps := FundamentalUnit(K);
        C := {eps, -eps, -1, 1};
        for u in C do
                case u:
                        when eps: print "Caso d = ", d, "con
                            extensi n cuadr tica de eps";
                        when -eps: print "Caso d = ", d, "con
                            extensi n cuadr tica de -eps";
                        when -1: print "Caso d = ", d, "con
                            extensi n cuadr tica de -1";
                        when 1: print "Caso d = ", d, "con
                            extensi n cuadr tica de 1";
                end case;
                Ku := SplittingField(y^2-u);
                P:=Factorization(2*Integers(Ku))[1,1];
                ray, m := RayClassGroup(P, [1..#RealPlaces(Ku)]);
                ray1, t := Hom(ray, AbelianGroup([3]));
                for x in ray1 do
                        if x ne 0*x then
                                print NumberField(
                                    AbelianExtension(Inverse(t(x)
                                    )*m));
                        end if;
                end for;
        end for;
end for;
```

A.3. PROGRAMA 3

Programa que calcula los cuerpos donde pueden haber caracteres no triviales según los casos del teorema 6.14. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

// l DESCOMPONE

K := QuadraticField(13);
print "(d,l) = (", 13, ",", 3, "):";
ray1, m1 := RayClassGroup(3*Integers(K),[1,2]);
ray11, t1 := Hom(ray1, AbelianGroup([2]));
for x in ray11 do
        if x ne 0*x then
                print NumberField(AbelianExtension(Inverse(t1(x))
                    *m1));
        end if;
end for;

//CASO theta1/theta2 = 1.
```

```
print "CASO theta1/theta2 = 1";

for d in [5,13,17] do
        K:=QuadraticField(d);
        S<y> := PolynomialRing(Integers(K));
        for l in ramifiedprimes(d) do
                print "(d,l) = (", d, ",", l, "):";
                L := SplittingField(y^l-1);
                P:=Factorization(l*Integers(L))[1,1];
                ray, m := RayClassGroup(P);
                ray1, t := Hom(ray, AbelianGroup([2]));
                for x in ray1 do
                        if x ne 0*x then
                                print NumberField(
                                    AbelianExtension(Inverse(t(x)
                                    )*m));
                        end if;
                end for;
        end for;
end for;

//CASO theta1/theta2 != 1.

print "CASO theta1/theta2 != 1";

for d in [3,21] do
        K := QuadraticField(d);
        for l in ramifiedprimes(d) do
                print "(d,l) = (", d, ",", l, "):";
                P:=Factorization(l*Integers(K))[1,1];
                ray, m := RayClassGroup(P,[1,2]);
                ray1, t := Hom(ray, AbelianGroup([2]));
                for x in ray1 do
                        if x ne 0*x then
                                print NumberField(
                                    AbelianExtension(Inverse(t(x)
                                    )*m));
                        end if;
                end for;
        end for;
end for;
```

A.4. PROGRAMA 4

Caso 1 del teorema 6.24. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC3torsion1(d, minN, maxN)
```

```
K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);

for k in [minN..maxN] do
        printf ".";
for s in [-1,1] do

        a3 := (1 + s * eps^k)/27;
        if (a3 in OK) and (a3 ne 0) then
                if IsPP(a3^3*OK) then
                        print ".";
                        print "Curva eliptica:" , s, "|", k , "|"
                            , "1" , "|", a3, "|";
                        curveinformation(K!1,0,K!a3,0,0,OK);
                end if;
        end if;
end for;
end for;

end procedure;
```

Caso 2 del teorema 6.24. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC3torsion2(d, minN, maxN)

K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);


for k in [minN..maxN] do
        printf ".";
for s in [-1,1] do

        a3 := s * eps^k;
        if IsPP((1-27*a3)*OK) then
                print ".";
                print "Curva eliptica:" , s, "|", k , "|", "1" ,
                    "|", a3 , "|";
                curveinformation(K!1,0,K!a3,0,0,OK);
        end if;

end for;
end for;
```

```
end procedure;
```

Caso 3 del teorema 6.24. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC3torsion4(d, minN, maxN)

K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);


if (#Factorization(3*OK) eq 1) then
        _, pi := IsPrincipal(Factorization(3*OK)[1,1]);
        for k in [0..2] do
        for j in [0..2] do
                a3 := eps^k*pi^j;
                print ".";
                print "Curva eliptica:" , k , "|", j , "|", "0" ,
                    "|", a3 , "|";
                curveinformation(0,0,K!a3,0,0,OK);
        end for;
        end for;
end if;

end procedure;
```

Caso 4 del teorema 6.24. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC3torsion5(d, minN, maxN)

K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);


for t in [minN..maxN] do
        printf ".";
for k in [0,1,2] do
for s in [-1,1] do

a := 27*eps^k + s*eps^t;
pi, j := almostcube(d, a);
if pi ne 0 then
        a13 := pi^j*a;
```

```
        if (not IsDivisibleBy(3, pi)) and (IsDivisibleBy(a13, pi)
            ) then
                if (#Roots(x^3 - a13) ne 0) then
                        a3 := eps^k * pi^j;
                        for a1 in Roots(x^3 - a13) do
                                print ".";
                                print "Curva eliptica:" , s, "|",
                                    t , "|", k, "|", a1[1], "|",
                                    a3, "|";
                                curveinformation(K!a1[1],0,K!a3
                                    ,0,0,OK);
                        end for;
                end if;
        end if;
end if;

end for;
end for;
end for;

end procedure;
```

Caso 5 del teorema 6.24 para cuando $\mathfrak{p} \mid a_1$. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC3torsion6(d, minN, maxN)

K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);

for t in [minN..maxN] do
        printf ".";
for p in Factorization(3*OK) do
for k in [0,1,2] do
for s in [-1,1] do
for r in [3..11] do

_, pi := IsPrincipal(p[1]);
a13 := s*eps^(t-3*k)*pi^r + 27*eps^k;

if (#Roots(x^3 - a13) ne 0) then
        a3 := eps^k;
        for a1 in Roots(x^3 - a13) do
                if (r gt 3) or ((r eq 3) and (Valuation(K!a1[1] ,
                    p[1]) eq 1)) then
                        print ".";
                        print "Curva eliptica:" , s, "|", t , "|"
                            , k, "|", a1[1], "|", a3, "|";
```

```
                        curveinformation(K!a1[1],0,K!a3,0,0,OK);
                end if;
        end for;
end if;

end for;
end for;
end for;
end for;
end for;

end procedure;
```

Caso 6 del teorema 6.24. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC3torsion7(d, minN, maxN)

K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);

for t in [minN..maxN] do
        printf ".";
for p in Factorization(3*OK) do
for k in [0,1,2] do
for s in [-1,1] do
for j in [1,2] do

_, pi := IsPrincipal(p[1]);
a13 := 27*eps^k*pi^j + s*eps^t*pi^3;

if (#Roots(x^3 -a13) ne 0) then
        a3 := eps^k*pi^j;
        for a1 in Roots(x^3 - a13) do
                print ".";
                print "Curva eliptica:" , s, "|", t , "|", k, "|"
                    , a1[1], "|", a3, "|";
                curveinformation(K!a1[1],0,K!a3,0,0,OK);
        end for;
end if;

end for;
end for;
end for;
end for;
end for;

end procedure;
```

Caso 7 del teorema 6.24. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC3torsion8(d, minN, maxN)

K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);

for t in [minN..maxN] do
        printf ".";
for p in Factorization(3*OK) do
for k in [0,1,2] do
for s in [-1,1] do
for j in [0,1,2] do

_, pi := IsPrincipal(p[1]);
a13 := pi^j*(27*eps^k + pi^3*s*eps^t);

if (#Roots(x^3 - a13) ne 0) then
        a3 := eps^k*pi^j;
        for a1 in Roots(x^3 - a13) do
                print ".";
                print "Curva eliptica:" , s, "|", t , "|", k, "|"
                    , a1[1], "|", a3, "|";
                curveinformation(K!a1[1],0,K!a3,0,0,OK);
        end for;
end if;

end for;
end for;
end for;
end for;
end for;

end procedure;
```

En los procedimientos anteriores se usan algunas funciones auxiliares que listamos aquí:

IsPP, revisa si la norma es potencia de primo (que es mas fácil) y si eso funciona lo factoriza. Esto es para evitar factorizar innecesariamente que es mas complejo para MAGMA.

```
function IsPP(I)

if not IsPrimePower(Norm(I)) then
return false;
```

```
end if;

return #Factorization(I) eq 1;
end function;
```

curveinformation, es un procedimiento que despliega datos de una curva dada en el siguiente formato:

(generador ideal primo) | (potencia en el conductor) | (norma del conductor) | (discriminante) | (potencia en el discriminante);

```
procedure curveinformation(a1,a2,a3,a4,a6, OK)

E := EllipticCurve([a1,a2,a3,a4,a6]);
C := Conductor(E);
Cfact := Factorization(C);
D := Discriminant(E);
Dfact := Factorization(D*OK);

print Cfact[1,1], "|", Cfact[1,2], "|", Norm(C), "|", D, "|",
    Dfact[1,2];

end procedure;
```

Para el caso 5, utilizamos la función auxiliar **almostcube** que acomoda, si es posible, para que un elemento sea un cubo multiplicado por un primo.

```
function almostcube(d, a)

K := QuadraticField(d);
OK := Integers(K);
P := Factorization(a*OK);
cont := 0;
pi := 1;
j := 0;

for p in P do
        if ((p[2] mod 3) ne 0) and (cont lt 2)  then
                cont := cont + 1;
                b, pi := IsPrincipal(p[1]);
                j := 3 - (p[2] mod 3);
        end if;
end for;

if (cont lt 2) then
        return pi, j;
else
        return 0, 0;
end if;
```

```
end function;
```

A.5. PROGRAMA 5

Tres casos para el cálculo de curvas elípticas sobre los cuerpos K consideradaos con un punto de 5-torsión.

Caso 1 del teorema 6.25. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC5torsion1(d, minN, maxN)

K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);

for k in [minN..maxN] do
        printf ".";
for s in [-1,1] do

        b := s*eps^k;
        if IsPP((1-11*b-b^2)*OK) then
                print ".";
                print "Curva eliptica:" , s, "|", k , "|", "1" ,
                    "|", b , "|";
                curveinformation(K!(b-1),-K!b,-K!b^2,0,0,OK);

        end if;
end for;
end for;

end procedure;
```

Caso 2 del teorema 6.25. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC5torsion2(d, minN, maxN)

K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);

for k in [minN..maxN] do
        printf ".";
```

```
for s in [-1,1] do
        if (#Roots(x^2 + 11*x + s*eps^k-1) ne 0) then
                for b in Roots(x^2 + 11*x + s*eps^k-1) do
                        if (b[1] ne 0) then
                                print ".";
                                print "Curva eliptica:" , s, "|",
                                    k , "|", "1", "|", b[1] , "|
                                    ";
                                curveinformation(K!(b[1]-1),-K!b
                                    [1],-K!b[1]^2,0,0,OK);

                        end if;
                end for;
        end if;
end for;
end for;

end procedure;
```

Caso 3 del teorema 6.25. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC5torsion3(d, minN, maxN)

K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);

for k in [minN..maxN] do
        printf ".";
for s in [-1,1] do
        if (#Roots(x^2 - 11*x - s*eps^k - 1) ne 0) then
                for a in Roots(x^2 - 11*x - s*eps^k - 1) do
                        if (a[1] ne 0) then
                                print ".";
                                print "Curva eliptica:" , s, "|",
                                    k , "|", a[1], "|", "1" , "|
                                    ";
                                curveinformation(K!(1-a[1]),-K!a
                                    [1],-K!a[1],0,0,OK);
                        end if;
                end for;
        end if;
end for;
end for;

end procedure;
```

A.6. PROGRAMA 6

Tres casos para el cálculo de curvas elípticas sobre los cuerpos K considerados con un punto de 7-torsión.

Caso 1 del teorema 6.26. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC7torsion1(d, minN, maxN)

K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);

for k in [minN..maxN] do
        printf ".";
for s in [-1,1] do
        b := s*eps^k;
        if (b ne 1) then
                if IsPP((1-b)^7*(1-8*b+5*b^2+b^3)*OK) then
                        print ".";
                        print "Curva eliptica:" , s, "|", k , "|"
                            , "1" , "|", b , "|";
                        curveinformation(K!(b^2+b-1),K!(b^2-b),K
                            !(b^4-b^3),0,0,OK);
                end if;
        end if;
end for;
end for;

end procedure;
```

Caso 2 del teorema 6.26. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC7torsion2(d, minN, maxN)

K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);

for k in [minN..maxN] do
        printf ".";
for s in [-1,1] do
        if (#Roots((1-x)^7*(1-8*x+5*x^2+x^3)-s*eps^k) ne 0) then
```

```
                    for b in Roots((1-x)^7*(1-8*x+5*x^2+x^3)-s*eps^k)
                        do
                            if (b[1] ne 0) then
                                    print ".";
                                    print "Curva eliptica:" , s, "|",
                                        k , "|", "1", "|", b[1] , "|
                                        ";
                                    curveinformation(K!(b[1]^2+b
                                        [1]-1),K!(b[1]^2-b[1]),K!(b
                                        [1]^4-b[1]^3),0,0,OK);
                            end if;
                    end for;
            end if;
end for;
end for;

end procedure;
```

Caso 3 del teorema 6.26. Implementado en MAGMA.

```
load "funciones_auxiliares.m";

procedure EC7torsion3(d, minN, maxN)

K := QuadraticField(d);
OK := Integers(K);
_<x> := PolynomialRing(K);
eps := FundamentalUnit(OK);

for k in [minN..maxN] do
        printf ".";
for s in [-1,1] do
        if (#Roots((x-1)^7*(x^3-8*x^2+5*x+1)-s*eps^k) ne 0) then
                for a in Roots((x-1)^7*(x^3-8*x^2+5*x+1)-s*eps^k)
                    do
                        if (a[1] ne 0) then
                                print ".";
                                print "Curva eliptica:" , "-", "|
                                    ", k , "|", a[1], "|", "1" ,
                                    "|";
                                curveinformation(K!(1+a[1]-a
                                    [1]^2),K!(a[1]^2-a[1]^3),K!(a
                                    [1]^2-a[1]^3),0,0,OK);
                        end if;
                end for;
        end if;
end for;
end for;

end procedure;
```

Esta página ha sido intencionalmente dejada en blanco.

Esta página ha sido intencionalmente dejada en blanco.

Índice

Referencias

[1] *Algebraic number theory.* Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967.

[2] Emil Artin. Beweis des allgemeinen Reziprozitätsgesetzes. *Abh. Math. Sem. Univ. Hamburg*, 5(1):353–363, 1927.

[3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[4] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[5] Jan Hendrik Bruinier, Gerard van der Geer, Günter Harder, and Don Zagier. *The 1-2-3 of modular forms.* Universitext. Springer-Verlag, Berlin, 2008. Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004, Edited by Kristian Ranestad.

[6] Armand Brumer and Kenneth Kramer. The rank of elliptic curves. *Duke Math. J.*, 44(4):715–743, 1977.

[7] Alex Cebrian Galan. Generalization of Fermat's Last Theorem to Real Quadratic Fields, 2016. Available at https://pdfs.semanticscholar.org/f05f/826542fd29ddada786026a85b3a912b1eedb.pdf.

[8] John Cremona and Ariel Pacetti. On elliptic curves of prime power conductor over imaginary quadratic fields with class number 1. *Proc. Lond. Math. Soc. (3)*, 118(5):1245–1276, 2019.

[9] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras.* Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[10] Henri Darnon, Fred Diamond, and Richard Taylor. Fermat's last theorem, 2007. Available at http://www.math.mcgill.ca/darmon/pub/Articles/Expository/05.DDT/paper.pdf.

[11] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530 (1975), 1974.

[12] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[13] Karin Erdmann and Thorsten Holm. *Algebras and representation theory*. Springer Undergraduate Mathematics Series. Springer, Cham, 2018.

[14] Nuno Freitas, Bao V. Le Hung, and Samir Siksek. Elliptic curves over real quadratic fields are modular. *Invent. Math.*, 201(1):159–206, 2015.

[15] Nuno Freitas and Samir Siksek. The asymptotic Fermat's last theorem for five-sixths of real quadratic fields. *Compos. Math.*, 151(8):1395–1415, 2015.

[16] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[17] Frazer Jarvis. On Galois representations associated to Hilbert modular forms. *J. Reine Angew. Math.*, 491:199–216, 1997.

[18] Sheldon Kamienny and Filip Najman. Torsion groups of elliptic curves over quadratic fields. *Acta Arith.*, 152(3):291–305, 2012.

[19] Irving Kaplansky. *Fields and rings*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1995. Reprint of the second (1972) edition.

[20] Chandrashekhar Khare and Jean-Pierre Wintenberger. On Serre's conjecture for 2-dimensional mod p representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Ann. of Math. (2)*, 169(1):229–253, 2009.

[21] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[22] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[23] Alain Kraus. Courbes elliptiques semi-stables et corps quadratiques. *J. Number Theory*, 60(2):245–253, 1996.

[24] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Compositio Math.*, 38(1):121–128, 1979.

[25] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[26] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2020. [Online; accessed 19 September 2020].

[27] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977. With an appendix by Mazur and M. Rapoport.

[28] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[29] J.-F. Mestre and J. Oesterlé. Courbes de Weil semi-stables de discriminant une puissance m-ième. *J. Reine Angew. Math.*, 400:173–184, 1989.

[30] James S. Milne. Algebraic number theory (v3.07), 2017. Available at www.jmilne.org/math/.

[31] J.S. Milne. Class field theory (v4.02), 2013. Available at www.jmilne.org/math/.

[32] Isao Miyawaki. Elliptic curves of prime power conductor with $\mathbf{Q}$-rational points of finite order. *Osaka Math. J.*, 10:309–323, 1973.

[33] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[34] A. M. Odlyzko. Lower bounds for discriminants of number fields. *Acta Arith.*, 29(3):275–297, 1976.

[35] Corentin Perret-Gentil. Associating abelian varieties to weight-2 modular forms: the Eichler-Shimura construction, 2014. Available at https://corentinperretgentil.gitlab.io/static/documents/eichler-shimura.pdf.

[36] Santiago Radi. Relación de Eichler-Shimura y Recíproco del Teorema de Modularidad, 2018. Available at https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/19172/1/uy24-19052.pdf.

[37] Santiago Radi. Representaciones de galois, 2020. Available at http://www.mat.uc.cl/ natalia.garcia/Mod20200526.pdf.

[38] Paulo Ribenboim. *Fermat's last theorem for amateurs.* Springer-Verlag, New York, 1999.

[39] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[40] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[41] Jean-Pierre Serre. *Linear representations of finite groups.* Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[42] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[43] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[44] Bennett Setzer. Elliptic curves of prime conductor. *J. London Math. Soc. (2)*, 10:367–378, 1975.

[45] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1994.

[46] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, Dordrecht, second edition, 2009.

[47] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves.* Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.

[48] Richard Taylor. On Galois representations associated to Hilbert modular forms. *Invent. Math.*, 98(2):265–280, 1989.

[49] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[50] Steven H. Weintraub. *Galois theory.* Universitext. Springer, New York, second edition, 2009.

[51] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Esta es la última página.
Compilado el miércoles 3 febrero, 2021.
http://www.cmat.edu.uy/