TRABAJO FIN DE GRADO

La conjetura de modularidad de Serre

Realizado por

Marta Sánchez Pavón

Para la obtención del título de

Grado en Matemáticas

Dirigido por

Sara Arias de Reyna Domínguez

Abstract

Serre's modularity conjecture is one of the most important results in number theory in recent decades. Proposed by Jean-Pierre Serre in 1975, the conjecture predicts that every odd, irreducible, two-dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ modulo p arises from a modular form. It was fully proven by Chandrashekhar Khare and Jean-Pierre Wintenberger in 2008.

The objective of this project is to gather the necessary concepts and results to state and understand Serre's modularity conjecture. Additionally, it aims to motivate the definition of optimal parameters for which there exists a modular form associated with a Galois representation under the aforementioned conditions. Finally, the conjecture will be illustrated with an example, and Fermat's last theorem will be proved as a consequence of it.

Resumen

La conjetura de modularidad de Serre es uno de los resultados más importantes en la teoría de números de las últimas décadas. Propuesta por Jean-Pierre Serre en 1975, la conjetura predice que cada representación de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ módulo p, impar, irreducible y bidimensional proviene de una forma modular, y fue demostrada en su totalidad por Chandrashekhar Khare y Jean-Pierre Wintenberger en 2008.

El objetivo de este proyecto es recopilar los conceptos y resultados necesarios para enunciar y entender la conjetura de modularidad de Serre. Además, se busca motivar la definición de los parámetros óptimos para los que existe una forma modular asociada a una representación de Galois, en las condiciones mencionadas anteriormente. Finalmente, se ilustrará la conjetura con un ejemplo, y se demostrará el último teorema de Fermat como consecuencia de la misma.

Índice general

1 Teoría algebraica de números

"God made the integers, all else is the work of man."
— Leopold Kronecker.

1.1. Teoría de Galois en extensiones infinitas

Sea K un cuerpo cualquiera, y K^{sep} la máxima extensión separable de K dentro de una clausura algebraica $\overline{K}$. Si K es un cuerpo perfecto, $K^{\text{sep}} \cong \overline{K}$, siendo $\overline{K}$ una clausura algebraica de K. En esta sección, se desarrollan las herramientas necesarias para estudiar el grupo de Galois $\mathrm{Gal}(K^{\text{sep}}/K)$ y sus subgrupos.

Ahora bien, K^{sep}/K es una extensión infinita, y el teorema de correspondencia de Galois no se extiende de manera directa a este caso: en general, existen más subgrupos de un grupo de Galois de una extensión infinita que subextensiones intermedias.[1] Por ello, el primer objetivo de esta sección será generalizar el teorema de correspondencia de Galois.

Comenzamos definiendo una topología que dota de estructura de grupo topológico al grupo de Galois de cualquier extensión, tanto finita como infinita. El contenido de esta sección se basa en el capítulo 7 de [Mil03] y en la sección 1 del capítulo IV de [Neu13]. También se recomienda consultar las secciones A.2 y A.3 del apéndice.

Definición 1.1. Sea Ω/K una extensión de Galois. Dado un subconjunto finito $S \subset \Omega$, se define el conjunto

$$G(S) = \mathrm{Gal}(\Omega/K)^S = \{\sigma \in \mathrm{Gal}(\Omega/K) : \sigma(s) = s \text{ para todo } s \in S\}.$$

Se define la *topología de Krull en* $\mathrm{Gal}(\Omega/K)$ como la topología cuya base de entornos abiertos de la identidad en $\mathrm{Gal}(\Omega/K)$ son los conjuntos $G(S)$, con $S \subset \Omega$ un subconjunto finito.

Es directo comprobar que $G(S)$ es un subgrupo de $\mathrm{Gal}(\Omega/K)$. La topología de Krull está bien definida, pues si $S_1, S_2 \subset \Omega$ son dos subconjuntos finitos, entonces $G(S_1) \cap G(S_2) = G(S_1 \cup S_2)$ es un elemento de la base de entornos de la identidad en $\mathrm{Gal}(\Omega/K)$. Además, un entorno de $\sigma \in \mathrm{Gal}(\Omega/K)$ viene dado por

$$\sigma G(S) = \{\tau \in \mathrm{Gal}(\Omega/K) : \tau(s) = \sigma(s) \text{ para todo } s \in S\},$$

con $S \subset \Omega$ un subconjunto finito.

Observemos que si $S_1 \subset S_2$ entonces $G(S_2) \subset G(S_1)$, por definición. El producto y la inversión en $\mathrm{Gal}(\Omega/K)$ son aplicaciones continuas respecto de la topología de Krull, por lo que $\mathrm{Gal}(\Omega/K)$ tiene estructura de grupo topológico.

[1] Un ejemplo de este fenómeno ocurre con la extensión $\overline{\mathbb{F}}_p/\mathbb{F}_p$. Se puede consultar el primer ejemplo de la sección 1 del capítulo IV de [Neu13] para ver detalladamente por qué.

A partir de ahora, siempre pensaremos en el grupo de Galois de cualquier extensión como un grupo topológico con la topología de Krull. Observemos que si $S \subset \Omega$ es un conjunto finito tal que $\sigma(S) = S$ para todo $\sigma \in \mathrm{Gal}(\Omega/K)$, entonces $K(S)/K$ es una subextensión de Ω/K finita de Galois. Por tanto,

$$\{\mathrm{Gal}(\Omega/L) : L/K \text{ subextensión de } \Omega/K \text{ finita de Galois}\}$$

también es una base de entornos abiertos de la identidad en $\mathrm{Gal}(\Omega/K)$, con la ventaja de que está formada por subgrupos normales de $\mathrm{Gal}(\Omega/K)$.

Proposición 1.1. Para toda extensión de Galois Ω/K, el grupo de Galois $\mathrm{Gal}(\Omega/K)$ es compacto y Hausdorff.

Demostración. Ver página 262, proposición (1.1) de [Neu13]. □

Proposición 1.2. Sean Ω/K una extensión de Galois, y L/K una subextensión de Ω/K finita de Galois. Entonces, el homomorfismo $\pi_L \colon \mathrm{Gal}(\Omega/K) \to \mathrm{Gal}(L/K)$ dado por la restricción $\sigma \mapsto \sigma|_L$ es sobreyectivo y continuo.

Demostración. Todo $\sigma \in \mathrm{Gal}(L/K)$ es un automorfismo $\sigma \colon L \to L$ que deja fijo a K, y se puede extender trivialmente a $\sigma \colon L \to \Omega$. Gracias al lema de Zorn y a que la extensión Ω/K es de Galois, se puede probar que[2] σ se extiende a un automorfismo $\overline{\sigma} \colon \Omega \to \Omega$ que deja fijo a K. Es decir, $\overline{\sigma} \in \mathrm{Gal}(\Omega/K)$ y $\overline{\sigma}|_L = \sigma$ para todo $\sigma \in \mathrm{Gal}(L/K)$, por lo que π_L es sobreyectivo.

Por otro lado, $\ker \pi_L = \mathrm{Gal}(\Omega/L)$. Además, como L/K es finita, si tomamos S como el conjunto formado por los generadores de L sobre K, entonces S es un conjunto finito y $G(S) = \mathrm{Gal}(\Omega/L)$. Por tanto, $\mathrm{Gal}(\Omega/L)$ es abierto. Finalmente, como $\{\mathrm{id}\} \subset \mathrm{Gal}(L/K)$ es abierto y

$$\pi_L^{-1}(\{\mathrm{id}\}) = \ker \pi_L = \mathrm{Gal}(\Omega/L)$$

también es abierto, concluimos que π_L es continuo, gracias al corolario A.1. □

Teorema 1.1 (Teorema de correspondencia de Galois)**.** *Sea Ω/K una extensión de Galois. Existe una correspondencia biunívoca entre*

$$\{\textit{subextensiones de } \Omega/K\} \longleftrightarrow \{\textit{subgrupos cerrados de } \mathrm{Gal}(\Omega/K)\}$$

dada por

$$L \mapsto \mathrm{Gal}(\Omega/L) \textit{ para toda subextension } L/K \textit{ de } \Omega/K, \textit{ y}$$
$$\Omega^H \hookleftarrow H \textit{ para todo subgrupo cerrado } H \subset \mathrm{Gal}(\Omega/K),$$

de modo que los subgrupos cerrados de $\mathrm{Gal}(\Omega/K)$ que son abiertos se corresponden exactamente con las subextensiones finitas de Ω/K. Además, un subgrupo cerrado $H \subset \mathrm{Gal}(\Omega/K)$ es normal si y sólo si Ω^H/K es de Galois. En este caso, denotando $L = \Omega^H$, la restricción

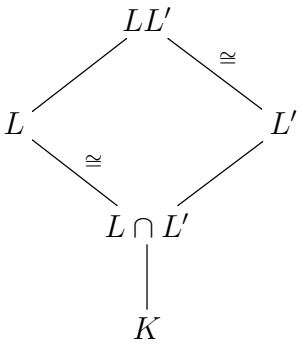
$$\mathrm{Gal}(\Omega/K) \to \mathrm{Gal}(L/K)$$
$$\sigma \mapsto \sigma|_L$$

induce un isomorfismo de grupos topológicos

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\Omega/K)/\mathrm{Gal}(\Omega/L).$$

[2] Para ver los detalles de este razonamiento, se puede consultar la demostración del teorema 6.6 de [Mil03].

Demostración. Ver página 98, teorema 7.3 de [Mil03]. □



Proposición 1.3. Sea K un cuerpo, y fijemos una clausura algebraica $\overline{K}$. Sean L/K y L'/K dos subextensiones de $\overline{K}/K$. Si L/K es de Galois, entonces las extensiones LL'/L' y $L/L \cap L'$ también son de Galois. Además, la restricción

$$\begin{aligned} \mathrm{Gal}(LL'/L') &\to \mathrm{Gal}(L/L \cap L') \\ \sigma &\mapsto \sigma|_L \end{aligned}$$

es un isomorfismo de grupos topológicos.

Demostración. Ver página 99, proposición 7.15 de [Mil03]. □

Grupos de Galois como límites inversos

A continuación, vamos a deducir que todo grupo de Galois se puede expresar como un límite inverso de subgrupos finitos del mismo, gracias a la topología de Krull. Sea K un cuerpo, y consideremos una extensión de Galois Ω/K. Definimos el conjunto

$$\mathcal{F} = \{L \subset \Omega : L/K \text{ es finita de Galois}\},$$

con el orden parcial dado por la inclusión. El compositum de un número finito de subextensiones de Ω/K finitas de Galois es una subextensión de Ω/K finita de Galois, por lo que $(\mathcal{F}, \subset)$ es un conjunto dirigido. Además, si $L, L' \in \mathcal{F}$ son tales que $L \subset L'$, consideramos el homomorfismo

$$\begin{aligned} \pi_{LL'} \colon \mathrm{Gal}(L'/K) &\to \mathrm{Gal}(L/K) \\ \sigma &\mapsto \sigma|_L, \end{aligned}$$

que es sobreyectivo y continuo por la proposición 1.2. No es difícil comprobar que $(\mathrm{Gal}(L/K), \pi_{LL'})$ es un sistema inverso indexado por $\mathcal{F}$ en la categoría de grupos topológicos. Denotemos $\varprojlim_{L \in \mathcal{F}} \mathrm{Gal}(L/K)$ a su límite inverso. La siguiente demostración se basa en [Mar].

Teorema 1.2. *Sea Ω/K una extensión de Galois. Existe un isomorfismo de grupos topológicos*

$$\varphi \colon \mathrm{Gal}(\Omega/K) \to \varprojlim_{L \in \mathcal{F}} \mathrm{Gal}(L/K),$$

dado por $\varphi(\sigma) = (\sigma|_L)_{L \in \mathcal{F}}$.

Demostración. Veamos que φ es inyectiva. Si $\varphi(\sigma) = (\mathrm{id}_L)_{L \in \mathcal{F}}$, entonces $\sigma|_L = \mathrm{id}_L$ para todo $L \in \mathcal{F}$. Dado que

$$\Omega = \bigcup_{L \in \mathcal{F}} L, \tag{1.1}$$

entonces $\sigma = \mathrm{id}_\Omega$, por lo que φ es inyectiva.

Por otro lado, sean $(\sigma_L)_L \in \varprojlim_{L\in\mathcal{F}} \mathrm{Gal}(L/K)$ y $x \in \Omega$. Definimos $\sigma \in \mathrm{Gal}(\Omega/K)$ como

$$\sigma(x) = \sigma_L(x) \text{ para algún } L \in \mathcal{F} \text{ tal que } x \in L.$$

Un tal L siempre existe por (1.1). Para ver que σ está bien definida, consideramos $L, L' \in \mathcal{F}$ tales que $x \in L \cap L'$. Entonces, $\sigma_L(x) = \sigma_{L\cap L'}(x) = \sigma_{L'}(x)$, pues $\sigma_L|_{L\cap L'} = \sigma_{L\cap L'} = \sigma_{L'}|_{L\cap L'}$. De manera similar se comprueba que $\sigma \in \mathrm{Gal}(\Omega/K)$, ya que la restricción de σ a cualquier $L \in \mathcal{F}$ es un automorfismo que deja fijo a K. Por construcción, $\varphi(\sigma) = (\sigma_L)_{L\in\mathcal{F}}$, por lo que φ es sobreyectiva.

Por último, φ es continua pues las proyecciones $\sigma \mapsto \sigma|_L$ son continuas para todo $L \in \mathcal{F}$, por la proposición 1.2. □

De ahora en adelante, denotaremos $\varprojlim \mathrm{Gal}(L/K) = \varprojlim_{L\in\mathcal{F}} \mathrm{Gal}(L/K)$, quedando implícito que L recorre las extensiones finitas de Galois de K dentro de K^{sep}.

1.2. Cuerpos de números

Esta sección presenta los conceptos fundamentales de la teoría algebraica de números, que es la rama de las matemáticas que estudia las propiedades algebraicas de las extensiones finitas de $\mathbb{Q}$. Estas extensiones reciben el nombre de *cuerpos de números*. Se puede encontrar una exposición más detallada junto con las demostraciones omitidas en [Neu13] y [Mil08].

Definición 1.2. Sea A un dominio de integridad noetheriano. Se dice que A es un *dominio de Dedekind* si todo ideal primo no nulo de A es maximal y A es íntegramente cerrado en su cuerpo de fracciones.

Proposición 1.4. Sea A un dominio de Dedekind. Todo ideal propio $I \subset A$ se expresa de manera única como

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

donde $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ son ideales primos de A y $e_1, \ldots, e_r$ son enteros positivos.

Demostración. Ver página 49, teorema 3.7 de [Mil08]. □

Este resultado es muy importante en teoría algebraica de números, pues si K es un cuerpo de números entonces la clausura entera de $\mathbb{Z}$ en K es un dominio de Dedekind[3], y por tanto, se cumple la factorización única de ideales en ideales primos.

Definición 1.3. Sea K un cuerpo de números. Se define el *anillo de enteros de* K, y se denota $\mathcal{O}_K$, como la clausura entera de $\mathbb{Z}$ en K.

Sea L/K una extensión finita de cuerpos de números, y sean $\mathcal{O}_K$ y $\mathcal{O}_L$ los anillos de enteros de K y L, respectivamente. Fijemos un ideal primo no nulo $\mathfrak{p} \subset \mathcal{O}_K$. Por la proposición anterior, el ideal $\mathfrak{p}\mathcal{O}_L$ se expresa de manera única como

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r},$$

[3]Ver página 17, teorema (3.5) de [Neu13].

donde $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ son ideales primos de $\mathcal{O}_L$ y $e_1, \ldots, e_r$ son enteros positivos. Si $\mathfrak{P}$ es un ideal de $\mathcal{O}_L$ tal que $\mathfrak{P} = \mathfrak{P}_i$ para algún $i = 1, \ldots, r$, se dice que $\mathfrak{P}$ *divide a* $\mathfrak{p}$, y se denota $\mathfrak{P} \mid \mathfrak{p}$. De hecho, $\mathfrak{P}$ divide a $\mathfrak{p}$ si y sólo si $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Además, para todo $i = 1, \ldots, r$, el exponente e_i es un entero positivo, llamado *índice de ramificación de* $\mathfrak{P}_i$ *sobre* $\mathfrak{p}$, y denotado $e(\mathfrak{P}_i/\mathfrak{p})$.

Como $\mathfrak{p}$ es maximal, el cociente $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo, llamado *cuerpo de residuos de* K *en* $\mathfrak{p}$, y denotado $k_\mathfrak{p}$. Se verifica que $k_\mathfrak{p}$ es un cuerpo finito de característica $p > 0$, siendo p un primo entero tal que $\mathfrak{p} \mid p$. Al cardinal de $k_\mathfrak{p}$ lo denotamos $N(\mathfrak{p})$.

Dado un ideal primo $\mathfrak{P} \subset \mathcal{O}_L$ tal que $\mathfrak{P} \mid \mathfrak{p}$, podemos ver $k_\mathfrak{p}$ como un subcuerpo de $k_\mathfrak{P}$. En efecto, la inclusión $\mathcal{O}_K \subset \mathcal{O}_L$ induce un homomorfismo de anillos $\mathcal{O}_K \to \mathcal{O}_L/\mathfrak{P}$ cuyo núcleo es $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Así, obtenemos un homomorfismo inyectivo $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}$ y podemos definir el *grado de inercia de* $\mathfrak{P}$ *sobre* $\mathfrak{p}$ como $f(\mathfrak{P}/\mathfrak{p}) = [k_\mathfrak{P} : k_\mathfrak{p}]$.

La extensión $k_\mathfrak{P}/k_\mathfrak{p}$ es de Galois por ser una extensión finita de cuerpos finitos. El grupo $\mathrm{Gal}(k_\mathfrak{P}/k_\mathfrak{p})$ es cíclico de orden $f(\mathfrak{P}/\mathfrak{p})$, y está generado por el *automorfismo de Frobenius*

$$x \mapsto x^{N(\mathfrak{p})}.$$

El índice de ramificación y el grado de inercia están relacionados por la siguiente fórmula.

Proposición 1.5 (Identidad fundamental)**.** Sean L/K una extensión finita de cuerpos de números, $\mathfrak{p} \subset \mathcal{O}_K$ un ideal primo no nulo, y r la cantidad de ideales primos de $\mathcal{O}_L$ que dividen a $\mathfrak{p}$. Entonces,

$$\sum_{i=1}^{r} e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}) = [L : K].$$

Demostración. Ver página 46, proposición (8.2) de [Neu13]. □

Ramificación

En el contexto anterior, es natural tratar de clasificar la estructura de la factorización única de $\mathfrak{p}$ en $\mathcal{O}_L$. Distinguimos los siguientes casos:

- Se dice que $\mathfrak{p}$ es *no ramificado en* L/K si $e(\mathfrak{P}/\mathfrak{p}) = 1$ para todo ideal primo $\mathfrak{P} \subset \mathcal{O}_L$ que divida a $\mathfrak{p}$. De lo contrario, se dice que $\mathfrak{p}$ *ramifica en* L/K.
- Se dice que $\mathfrak{p}$ es *inerte en* L/K si sigue siendo primo en $\mathcal{O}_L$, es decir, si el único ideal primo $\mathfrak{P} \subset \mathcal{O}_L$ que divide a $\mathfrak{p}$ verifica $e(\mathfrak{P}/\mathfrak{p}) = 1$.
- Por último, si la cantidad de ideales primos de $\mathcal{O}_L$ que dividen a $\mathfrak{p}$ coincide con el grado de L/K, se dice que $\mathfrak{p}$ *se descompone totalmente en* L/K.

Nuestro objetivo actual es caracterizar los ideales primos no ramificados en una extensión finita de Galois de cuerpos de números. Así, supongamos además que L/K es de Galois, y definimos

$$\Sigma_{L,\mathfrak{p}} = \{\mathfrak{P} \subset \mathcal{O}_L : \mathfrak{P} \text{ ideal primo no nulo tal que } \mathfrak{P} \mid \mathfrak{p}\}.$$

Se puede probar[4] que $\mathrm{Gal}(L/K)$ actúa transitivamente en $\Sigma_{L,\mathfrak{p}}$. Esto significa que para todo $\mathfrak{P},\mathfrak{P}' \in \Sigma_{L,\mathfrak{p}}$ existe $\sigma \in \mathrm{Gal}(L/K)$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$. De esta propiedad se deduce que

$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}'/\mathfrak{p}) \text{ y } f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}'/\mathfrak{p}) \text{ para todo } \mathfrak{P},\mathfrak{P}' \in \Sigma_{L,\mathfrak{p}},$$

por lo que denotamos $e_\mathfrak{p} = e(\mathfrak{P}/\mathfrak{p})$ y $f_\mathfrak{p} = f(\mathfrak{P}/\mathfrak{p})$. Así, la identidad fundamental se reduce a $e_\mathfrak{p} f_\mathfrak{p} r_\mathfrak{p} = [L:K]$, siendo $r_\mathfrak{p} = |\Sigma_{L,\mathfrak{p}}|$ la cantidad de ideales primos de $\mathcal{O}_L$ que dividen a $\mathfrak{p}$.

Estas propiedades nos permiten estudiar la ramificación de los ideales primos de $\mathcal{O}_K$ en la extensión L/K a partir de ciertos subgrupos de $\mathrm{Gal}(L/K)$, que definimos a continuación.

Definición 1.4. Dado $\mathfrak{P} \in \Sigma_{L,\mathfrak{p}}$, se define el *grupo de descomposición de* $\mathfrak{P}$ *sobre* $\mathfrak{p}$ como el estabilizador de la acción de $\mathrm{Gal}(L/K)$ en $\mathfrak{P}$, y se denota $D(\mathfrak{P}/\mathfrak{p})$. Es decir,

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Sean $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ y $x \in \mathcal{O}_L$. Entonces, $\sigma(x) \bmod \mathfrak{P}$ no depende del representante x de la clase $x + \mathfrak{P}$. En efecto, si y es otro representante, entonces $x - y \in \mathfrak{P}$ y por tanto $\sigma(x-y) = \sigma(x) - \sigma(y) \in \sigma(\mathfrak{P}) = \mathfrak{P}$. Entonces, todo $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ induce un automorfismo en $k_\mathfrak{P}$ que deja fijo a $k_\mathfrak{p}$. Esto nos permite definir el homomorfismo reducción

$$\begin{aligned} \pi_{\mathfrak{P}/\mathfrak{p}} \colon D(\mathfrak{P}/\mathfrak{p}) &\to \mathrm{Gal}(k_\mathfrak{P}/k_\mathfrak{p}) \\ \sigma &\mapsto \sigma \bmod \mathfrak{P}. \end{aligned} \tag{1.2}$$

Definición 1.5. Dado $\mathfrak{P} \in \Sigma_{L,\mathfrak{p}}$, se define el *grupo de inercia de* $\mathfrak{P}$ *sobre* $\mathfrak{p}$ como el núcleo de $\pi_{\mathfrak{P}/\mathfrak{p}}$, y se denota $I(\mathfrak{P}/\mathfrak{p})$. Explícitamente,

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in D(\mathfrak{P}/\mathfrak{p}) : \sigma(x) \equiv x \bmod \mathfrak{P} \text{ para todo } x \in \mathcal{O}_L\}.$$

El homomorfismo $\pi_{\mathfrak{P}/\mathfrak{p}}$ es sobreyectivo[5], y por tanto, induce una sucesión exacta corta

$$1 \to I(\mathfrak{P}/\mathfrak{p}) \to D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(k_\mathfrak{P}/k_\mathfrak{p}) \to 1.$$

Además, no es difícil comprobar que para todo $\sigma \in \mathrm{Gal}(L/K)$ se verifica

$$D(\sigma(\mathfrak{P})/\mathfrak{p}) = \sigma D(\mathfrak{P}/\mathfrak{p})\sigma^{-1} \text{ y } I(\sigma(\mathfrak{P})/\mathfrak{p}) = \sigma I(\mathfrak{P}/\mathfrak{p})\sigma^{-1}.$$

Proposición 1.6. Dado $\mathfrak{P} \in \Sigma_{L,\mathfrak{p}}$, se verifica $|D(\mathfrak{P}/\mathfrak{p})| = e_\mathfrak{p} f_\mathfrak{p}$ y $|I(\mathfrak{P}/\mathfrak{p})| = e_\mathfrak{p}$.

Demostración. Denotemos $\mathrm{orb}_G(\mathfrak{P})$ a la órbita de $\mathfrak{P}$ por la acción de $G = \mathrm{Gal}(L/K)$. Dado que $r_\mathfrak{p} = |\Sigma_{L,\mathfrak{p}}| = |\mathrm{orb}_G(\mathfrak{P})|$, se sigue del teorema de la órbita-estabilizador y de la identidad fundamental que

$$|D(\mathfrak{P}/\mathfrak{p})| = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{orb}_G(\mathfrak{P})|} = \frac{e_\mathfrak{p} f_\mathfrak{p} r_\mathfrak{p}}{r_\mathfrak{p}} = e_\mathfrak{p} f_\mathfrak{p}.$$

[4] Ver página 54, proposición (9.1) de [Neu13].
[5] Ver página 56, proposición (9.4) de [Neu13].

Por otro lado, $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}) \cong D(\mathfrak{P}/\mathfrak{p})/I(\mathfrak{P}/\mathfrak{p})$ por el primer teorema de isomorfía de Noether. Finalmente, por el teorema de Lagrange,

$$|I(\mathfrak{P}/\mathfrak{p})| = \frac{|D(\mathfrak{P}/\mathfrak{p})|}{|\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})|} = \frac{e_{\mathfrak{p}} f_{\mathfrak{p}}}{f_{\mathfrak{p}}} = e_{\mathfrak{p}},$$

como queríamos. □

Teorema 1.3. *Sean L/K una extensión finita de Galois de cuerpos de números, y $\mathfrak{p} \subset \mathcal{O}_K$ un ideal primo no nulo. Entonces, $\mathfrak{p}$ es no ramificado en L/K si y sólo si $I(\mathfrak{P}/\mathfrak{p}) = \{\mathrm{id}\}$ para cualquier ideal primo $\mathfrak{P} \subset \mathcal{O}_L$ tal que $\mathfrak{P} \mid \mathfrak{p}$.*

Demostración. Sea $\mathfrak{P} \subset \mathcal{O}_L$ un ideal primo tal que $\mathfrak{P} \mid \mathfrak{p}$. Por definición, $\mathfrak{p}$ es no ramificado en L/K si y sólo si $e_{\mathfrak{p}} = 1$. Por la proposición anterior, esto ocurre si y sólo si $|I(\mathfrak{P}/\mathfrak{p})| = 1$. Equivalentemente, $I(\mathfrak{P}/\mathfrak{p}) = \{\mathrm{id}\}$, como queríamos. □

Elemento de Frobenius

Manteniendo la notación anterior, supongamos que $\mathfrak{p}$ es no ramificado en L/K. Es decir, para todo $\mathfrak{P} \in \Sigma_{L,\mathfrak{p}}$, el grupo de inercia $I(\mathfrak{P}/\mathfrak{p})$ es trivial y por tanto $\pi_{\mathfrak{P}/\mathfrak{p}}$ induce un isomorfismo $D(\mathfrak{P}/\mathfrak{p}) \cong \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$. Entonces, existe un único elemento en $D(\mathfrak{P}/\mathfrak{p})$ cuya imagen por $\pi_{\mathfrak{P}/\mathfrak{p}}$ es el automorfismo de Frobenius. Dicho elemento se llama *elemento de Frobenius de $\mathfrak{P}$ sobre $\mathfrak{p}$*, se denota $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$, y se caracteriza por ser el único $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ tal que

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \text{ mód } \mathfrak{P} \text{ para todo } x \in \mathcal{O}_L.$$

Además, no es difícil comprobar que

$$\mathrm{Frob}(\sigma(\mathfrak{P})/\mathfrak{p}) = \sigma \mathrm{Frob}(\mathfrak{P}/\mathfrak{p})\sigma^{-1} \text{ para todo } \sigma \in \mathrm{Gal}(L/K).$$

Fijamos la siguiente notación:

- Dado $\sigma \in \mathrm{Gal}(L/K)$, denotamos $[\sigma]$ a su clase de conjugación en $\mathrm{Gal}(L/K)$, y denotamos $\#[\sigma]$ al orden de $[\sigma]$.
- De manera análoga, denotamos $[\mathrm{Frob}_{\mathfrak{p}}]$ a la clase de conjugación de $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ en $\mathrm{Gal}(L/K)$, para cualquier ideal primo $\mathfrak{P} \subset \mathcal{O}_L$ tal que $\mathfrak{P} \mid \mathfrak{p}$.
- Por último, denotamos Σ_K al conjunto de ideales primos no nulos de $\mathcal{O}_K$.

Definición 1.6. Dado $S \subset \Sigma_K$, se define la *densidad de Dirichlet de S* como

$$d(S) = \lim_{s \to 1,\, s>1} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \Sigma_K} N(\mathfrak{p})^{-s}},$$

siempre que el límite exista.

De esta definición, se observa que si $S \subset \Sigma_K$ es finito entonces $d(S) = 0$. Es decir, los subconjuntos de Σ_K con densidad de Dirichlet positiva tienen cardinal infinito.

Teorema 1.4 (Teorema de densidad de Chebotarev)**.** *Sea L/K una extensión finita de Galois de cuerpos de números. Dado $\sigma \in \mathrm{Gal}(L/K)$, se define el conjunto*

$$P_{L/K}(\sigma) = \{\mathfrak{p} \in \Sigma_K : [\mathrm{Frob}_{\mathfrak{p}}] = [\sigma]\}.$$

Entonces, $P_{L/K}(\sigma)$ tiene densidad de Dirichlet, y viene dada por

$$d\left(P_{L/K}(\sigma)\right) = \frac{\#[\sigma]}{|\mathrm{Gal}(L/K)|}.$$

Corolario 1.1. Sea L/K una extensión finita de Galois de cuerpos de números. Para todo $\sigma \in \mathrm{Gal}(L/K)$, existen infinitos ideales primos $\mathfrak{p} \subset \mathcal{O}_K$ tales que, para algún ideal primo $\mathfrak{P} \subset \mathcal{O}_L$ con $\mathfrak{P} \mid \mathfrak{p}$, se verifica $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p}) = \sigma$.

Demostración. Sea $\sigma \in \mathrm{Gal}(L/K)$. Por el teorema de densidad de Chebotarev, el conjunto

$$P_{L/K}(\sigma) = \{\mathfrak{p} \in \Sigma_K : [\mathrm{Frob}_{\mathfrak{p}}] = [\sigma]\}$$

tiene densidad de Dirichlet positiva, y por tanto, tiene cardinal infinito. Es decir, existen infinitos ideales primos $\mathfrak{p} \in \Sigma_K$ tales que $[\mathrm{Frob}_{\mathfrak{p}}] = [\sigma]$. Concluimos el resultado, pues para todo $\mathfrak{p} \in P_{L/K}(\sigma)$, existe un ideal primo $\mathfrak{P} \subset \mathcal{O}_L$ tal que $\mathfrak{P} \mid \mathfrak{p}$ y $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p}) = \sigma$. □

El grupo absoluto de Galois de un cuerpo de números

Para terminar la sección, veamos cómo extender el elemento de Frobenius al grupo absoluto de Galois de un cuerpo de números K. Esta parte se basa en el post [grg], donde se pueden consultar más detalles. Fijemos una clausura algebraica $\overline{K}$ de K, y denotemos $\overline{\mathcal{O}}_K$ a la clausura entera de $\mathcal{O}_K$ en $\overline{K}$. Si $K = \mathbb{Q}$, denotamos $\overline{\mathbb{Z}} = \overline{\mathcal{O}}_{\mathbb{Q}}$. Consideramos el conjunto

$$\mathcal{F} = \{L \subset \overline{K} : L/K \text{ finita de Galois}\},$$

con el orden parcial dado por la inclusión. El cuerpo $\overline{K}$ es la unión directa de todas las extensiones de K finitas de Galois, luego un ideal primo no nulo $\mathfrak{P} \subset \overline{\mathcal{O}}_K$ se corresponde con una sucesión de ideales primos no nulos $(\mathfrak{P}_L)_{L\in\mathcal{F}}$ tales que

$$\mathfrak{P}_{L'} \cap \mathcal{O}_L = \mathfrak{P}_L \text{ siempre que } L \subset L'.$$

Fijemos un ideal primo no nulo $\mathfrak{p} \subset \mathcal{O}_K$. El grupo de Galois $G_K = \mathrm{Gal}(\overline{K}/K)$ actúa transitivamente en el conjunto

$$\overline{\Sigma}_{K,\mathfrak{p}} = \{\mathfrak{P} \subset \overline{\mathcal{O}}_K : \mathfrak{P} \text{ ideal primo no nulo tal que } \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}\}.$$

Definición 1.7. Dado $\mathfrak{P} \in \overline{\Sigma}_{K,\mathfrak{p}}$, se define el *grupo de descomposición de* $\mathfrak{P}$ *sobre* $\mathfrak{p}$ como

$$D(\mathfrak{P}/\mathfrak{p}) = \varprojlim_{L\in\mathcal{F}} D(\mathfrak{P}_L/\mathfrak{p}) = \{\sigma \in G_K : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Fijemos $\mathfrak{P} \in \overline{\Sigma}_{K,\mathfrak{p}}$, y consideremos el homomorfismo $\pi_L \colon G_K \to \mathrm{Gal}(L/K)$ dado por la restricción $\pi_L(\sigma) = \sigma|_L$ para todo $L \in \mathcal{F}$. La acción de G_K en $\overline{\Sigma}_K$ es transitiva y π_L es sobreyectivo, luego

$$\pi_L\left(D(\mathfrak{P}/\mathfrak{p})\right) = D(\mathfrak{P}_L/\mathfrak{p}) \text{ para todo } L \in \mathcal{F}.$$

Sean $L, L' \in \mathcal{F}$ tales que $L \subset L'$, y $\pi_{LL'} \colon \mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K)$ el homomorfismo dado por la restricción $\pi_{LL'}(\sigma) = \sigma|_L$. Entonces, $\pi_{LL'}$ lleva el grupo de descomposición $D(\mathfrak{P}_{L'}/\mathfrak{p})$ en $D(\mathfrak{P}_L/\mathfrak{p})$, y lleva el grupo de inercia $I(\mathfrak{P}_{L'}/\mathfrak{p})$ en $I(\mathfrak{P}_L/\mathfrak{p})$. Esto nos permite dar la siguiente definición.

Definición 1.8. Dado $\mathfrak{P} \in \overline{\Sigma}_{K,\mathfrak{p}}$, se define el grupo de inercia de $\mathfrak{P}$ sobre $\mathfrak{p}$ como

$$I(\mathfrak{P}/\mathfrak{p}) = \varprojlim_{L \in \mathcal{F}} I(\mathfrak{P}_L/\mathfrak{p}) = \{\sigma \in G_K : \sigma(x) \equiv x \bmod \mathfrak{P} \text{ para todo } x \in \overline{\mathcal{O}}_K\}.$$

Ahora bien, no podemos definir "el elemento de Frobenius de $\mathfrak{P}$ sobre $\mathfrak{p}$" en G_K directamente como $\varprojlim_{L \in \mathcal{F}} \mathrm{Frob}(\mathfrak{P}_L/\mathfrak{p})$, pues sólo tiene sentido considerar $\mathrm{Frob}(\mathfrak{P}_L/\mathfrak{p})$ cuando $\mathfrak{p}$ es no ramificado en L/K. Aún así, para cualquier $L \in \mathcal{F}$, podemos considerar el *conjunto de elementos de Frobenius de* $\mathfrak{P}_L$ *sobre* $\mathfrak{p}$, definido como la preimagen por $\pi_{\mathfrak{P}_L/\mathfrak{p}}$ del automorfismo de Frobenius $x \mapsto x^{N(\mathfrak{p})}$, y denotado $\phi(\mathfrak{P}_L/\mathfrak{p})$. Además, si $L' \in \mathcal{F}$ es tal que $L \subset L'$, entonces $\pi_{LL'}$ lleva $\phi(\mathfrak{P}_{L'}/\mathfrak{p})$ en $\phi(\mathfrak{P}_L/\mathfrak{p})$, lo que nos permite dar la siguiente definición.

Definición 1.9. Dado $\mathfrak{P} \in \overline{\Sigma}_{K,\mathfrak{p}}$, se define el *conjunto de elementos de Frobenius de* $\mathfrak{P}$ *sobre* $\mathfrak{p}$ como

$$\phi(\mathfrak{P}/\mathfrak{p}) = \varprojlim_{L \in \mathcal{F}} \phi(\mathfrak{P}_L/\mathfrak{p}).$$

Cualquier elemento de $\phi(\mathfrak{P}/\mathfrak{p})$ se denota $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ o $\mathrm{Frob}_{\mathfrak{p}}$, y se llama *elemento de Frobenius sobre* $\mathfrak{p}$, teniendo en cuenta que está definido en el cociente $D(\mathfrak{P}/\mathfrak{p})/I(\mathfrak{P}/\mathfrak{p})$.

Proposición 1.7. Sea S un conjunto finito de primos enteros. Entonces, $\{\mathrm{Frob}_\ell : \ell \notin S\}$ es denso en $G_{\mathbb{Q}}$.

Demostración. Sea $\sigma \in G_{\mathbb{Q}}$. Consideremos un entorno abierto de σ, es decir,

$$\sigma\mathrm{Gal}(\overline{\mathbb{Q}}/K) = \{\tau \in G_{\mathbb{Q}} : \tau|_K = \sigma|_K\},$$

siendo $K/\mathbb{Q}$ una extensión finita de Galois. Por el corolario 1.1, existen infinitos primos $\ell \in \mathbb{Z}$ tales que, para algún ideal primo $\mathfrak{l} \subset \mathcal{O}_K$ con $\mathfrak{l} \mid \ell$, se verifica $\mathrm{Frob}(\mathfrak{l}/\ell) = \sigma|_K$. Podemos suponer que $\ell \notin S$, y consideremos $\mathfrak{l} \subset \mathcal{O}_K$ un tal ideal primo. Entonces, existe un ideal primo $\mathfrak{L} \subset \overline{\mathbb{Z}}$ tal que $\mathfrak{L} \cap \mathcal{O}_K = \mathfrak{l}$ y $\mathrm{Frob}(\mathfrak{L}/\ell)|_K = \mathrm{Frob}(\mathfrak{l}/\ell) = \sigma|_K$. Es decir, $\mathrm{Frob}(\mathfrak{L}/\ell) \in \sigma\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Concluimos que

$$\{\mathrm{Frob}_\ell : \ell \notin S\} \cap \sigma\mathrm{Gal}(\overline{\mathbb{Q}}/K) \neq \emptyset,$$

como queríamos. □

1.3. Valoraciones asociadas a cuerpos de números

Sean K un cuerpo de números y $\mathfrak{p} \subset \mathcal{O}_K$ un ideal primo no nulo. En esta sección, vamos a dar las herramientas para poder estudiar la ramificación de $\mathfrak{p}$ mediante teoría de valoraciones. Se pueden consultar los conceptos y resultados básicos de esta teoría en el apéndice A.4.

La valoración $\mathfrak{p}$-ádica

Definimos la función $\mathrm{ord}_{\mathfrak{p}} \colon \mathcal{O}_K - \{0\} \to \mathbb{Z}$ como

$$\mathrm{ord}_{\mathfrak{p}}(x) = \mathrm{máx}\{r \in \mathbb{Z} : x\mathcal{O}_K \subset \mathfrak{p}^r\}.$$

De la proposición 1.4 se deduce que si $x, y \in \mathcal{O}_K - \{0\}$ entonces $\mathrm{ord}_{\mathfrak{p}}(xy) = \mathrm{ord}_{\mathfrak{p}}(x) + \mathrm{ord}_{\mathfrak{p}}(y)$, lo que nos permite extender $\mathrm{ord}_{\mathfrak{p}}$ a $K^\times$ como sigue:

$$\mathrm{ord}_{\mathfrak{p}}(z) = \mathrm{ord}_{\mathfrak{p}}(x) - \mathrm{ord}_{\mathfrak{p}}(y) \text{ para todo } z = \frac{x}{y} \in K^\times \text{ con } x, y \in \mathcal{O}_K - \{0\}.$$

Es directo comprobar que $\mathrm{ord}_{\mathfrak{p}}$ está bien definida, y que la función $v_{\mathfrak{p}} \colon K \to \mathbb{Z} \cup \{\infty\}$ dada por

$$v_{\mathfrak{p}}(x) = \begin{cases} \mathrm{ord}_{\mathfrak{p}}(x) & \text{si } x \neq 0, \\ \infty & \text{si } x = 0. \end{cases}$$

es una valoración discreta normalizada en K. La valoración $v_{\mathfrak{p}}$ se llama *valoración* $\mathfrak{p}$*-ádica*. Además, $v_{\mathfrak{p}}$ induce una familia de valores absolutos no arquimedianos discretos, como en la observación A.2. Tomando $c = N(\mathfrak{p})$ en dicha observación, obtenemos el *valor absoluto* $\mathfrak{p}$*-ádico* $|\cdot|_{\mathfrak{p}} \colon K \to \mathbb{Z}$, dado por

$$|x|_{\mathfrak{p}} = \begin{cases} N(\mathfrak{p})^{-v_{\mathfrak{p}}(x)} & \text{si } x \neq 0, \\ 0 & \text{si } x = 0. \end{cases}$$

La importancia del valor absoluto $\mathfrak{p}$-ádico se ve reflejada en el siguiente teorema.

Teorema 1.5 (de Ostroswki para cuerpos de números)**.** *Sea K un cuerpo de números. Todo valor absoluto no arquimediano no trivial en K es equivalente al valor absoluto $\mathfrak{p}$-ádico para un único ideal primo $\mathfrak{p} \subset \mathcal{O}_K$.*

Demostración. Ver [Con10]. □

Sea $K_{\mathfrak{p}}$ la completación de K respecto del valor absoluto $\mathfrak{p}$-ádico. También denotaremos $v_{\mathfrak{p}}$ (respectivamente, $|\cdot|_{\mathfrak{p}}$) a la extensión de la valoración $\mathfrak{p}$-ádica (respectivamente, del valor absoluto $\mathfrak{p}$-ádico) a $K_{\mathfrak{p}}$. Los conjuntos

$$\mathcal{O}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} : v_{\mathfrak{p}}(x) \geq 0\} = \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} \leq 1\}, \text{ y}$$
$$\mathfrak{M}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} : v_{\mathfrak{p}}(x) > 0\} = \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} < 1\}$$

son, respectivamente, el anillo e ideal de valoración de $K_{\mathfrak{p}}$.

Extensiones de $K_\mathfrak{p}$

Consideremos una extensión finita $F/K_\mathfrak{p}$ de grado n. Por el teorema A.3, el valor absoluto $\mathfrak{p}$-ádico se extiende a un único valor absoluto en F, dado por

$$|x|_F = \left|N_{F/K_\mathfrak{p}}(x)\right|_\mathfrak{p}^{\frac{1}{n}} \text{ para todo } x \in F^\times.$$

Además, F es un cuerpo completo respecto de $|\cdot|_F$. De manera similar, por el corolario A.3, la valoración $\mathfrak{p}$-ádica se extiende a una única valoración en F, dada por

$$w_F(x) = \frac{1}{n} v_\mathfrak{p}\left(N_{F/K_\mathfrak{p}}(x)\right) \text{ para todo } x \in F^\times.$$

Se verifica que $|\cdot|_F$ es un valor absoluto no arquimediano discreto, y que w_F es una valoración discreta. Tanto $|\cdot|_F$ como w_F se extienden de manera única a cualquier clausura algebraica $\overline{K}_\mathfrak{p}$, pero dichas extensiones no son discretas, en general (véase la observación A.3).

El anillo (respectivamente, ideal) de valoración de F es

$$\begin{aligned}\mathcal{O}_F &= \{x \in F : w_F(x) \geq 0\} = \{x \in F : |x|_F \leq 1\}, \text{ y}\\ \mathfrak{M}_F &= \{x \in F : w_F(x) > 0\} = \{x \in F : |x|_F < 1\}.\end{aligned}$$

Dado que w_F es una valoración discreta, se sigue de la proposición A.5 que $\mathcal{O}_F$ es un dominio de ideales principales, y su único ideal maximal es $\mathfrak{M}_F$. En particular, $\mathcal{O}_F$ es un dominio de Dedekind, y la proposición 1.4 implica que existe un único entero positivo e tal que

$$\mathfrak{M}_\mathfrak{p}\mathcal{O}_F = \mathfrak{M}_F^e.$$

Notemos que, en este caso, el exponente e depende únicamente de la extensión $F/K_\mathfrak{p}$. La siguiente proposición caracteriza a dicho exponente.

Proposición 1.8. Sea $F/K_\mathfrak{p}$ una extensión finita. Si v_F denota la valoración normalizada asociada a w_F, entonces

$$v_F = ew_F,$$

siendo e el único exponente que aparece en la factorización única de $\mathfrak{M}_\mathfrak{p}\mathcal{O}_F$.

Demostración. Veamos que ew_F está normalizada. Para ello, hay que probar que $ew_F(F^\times) = \mathbb{Z}$, o equivalentemente, $w_F(F^\times) = \frac{1}{e}\mathbb{Z}$. Por la proposición A.5, es suficiente probar que $w_F(\pi_F) = \frac{1}{e}$, siendo π_F un uniformizante en F.

Sea π un uniformizante en $K_\mathfrak{p}$. Entonces, π se expresa de manera única como $\pi = \varepsilon\pi_F^e$, con $\varepsilon \in \mathcal{O}_F^\times$. Por tanto, teniendo en cuenta que $v_\mathfrak{p}$ está normalizada y que $w_F|_{K_\mathfrak{p}} = v_\mathfrak{p}$, se sigue que

$$1 = v_\mathfrak{p}(\pi) = w_F(\pi) = w_F(\varepsilon\pi_F^e) = ew_F(\pi_F),$$

y concluimos que $w_F(\pi_F) = \frac{1}{e}$, como queríamos. □

Definición 1.10. Sea $F/K_\mathfrak{p}$ una extensión finita. Se definen:

- El *índice de ramificación de* $F/K_\mathfrak{p}$ como $e(F/K_\mathfrak{p}) = v_F(\pi)$, siendo v_F la valoración normalizada asociada a w_F, y π un uniformizante en $K_\mathfrak{p}$.
- El *grado de inercia de* $F/K_\mathfrak{p}$ como $f(F/K_\mathfrak{p}) = [\mathcal{O}_F/\mathfrak{M}_F : \mathcal{O}_\mathfrak{p}/\mathfrak{M}_\mathfrak{p}]$.

Observación. Sea $F/K_\mathfrak{p}$ una extensión finita. Notemos que el índice de ramificación coincide con el único exponente e que aparece en la factorización de $\mathfrak{M}_\mathfrak{p}\mathcal{O}_F$. En efecto, si π es un uniformizante en $K_\mathfrak{p}$, se sigue de la proposición anterior que

$$e(F/K_\mathfrak{p}) = v_F(\pi) = ew_F(\pi) = ev_\mathfrak{p}(\pi) = e.$$

Por otro lado, la inclusión $\mathcal{O}_\mathfrak{p} \subset \mathcal{O}_F$ induce una inclusión de cuerpos $\mathcal{O}_\mathfrak{p}/\mathfrak{M}_\mathfrak{p} \subset \mathcal{O}_F/\mathfrak{M}_F$, luego el grado de inercia $f(F/K_\mathfrak{p})$ está bien definido. Notemos que, por la proposición A.8, existe un isomorfismo $\mathcal{O}_\mathfrak{p}/\mathfrak{M}_\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p}$. Por ello, también denotaremos $k_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{M}_\mathfrak{p}$, ya que $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ es el único cuerpo de $N(\mathfrak{p})$ elementos (salvo isomorfismo), gracias al teorema de clasificación de cuerpos finitos. Por último, denotamos $k_F = \mathcal{O}_F/\mathfrak{M}_F$, que también es un cuerpo finito al ser una extensión finita de $k_\mathfrak{p}$.

Corolario 1.2. Sean $F/K_\mathfrak{p}$ y $F'/K_\mathfrak{p}$ dos extensiones finitas tales que $F \subset F'$. Entonces,

$$\begin{aligned} e(F'/K_\mathfrak{p}) &= e(F'/F)e(F/K_\mathfrak{p}), \text{ y} \\ f(F'/K_\mathfrak{p}) &= f(F'/F)f(F/K_\mathfrak{p}). \end{aligned}$$

Una vez más, el índice de ramificación y el grado de inercia se relacionan por la siguiente fórmula.

Proposición 1.9 (Identidad fundamental)**.** Si $F/K_\mathfrak{p}$ es una extensión finita, entonces

$$[F : K_\mathfrak{p}] = e(F/K_\mathfrak{p})f(F/K_\mathfrak{p}).$$

Demostración. Ver página 150, proposición (6.8) de [Neu13]. □

1.4. Extensiones no ramificadas y moderadas

Sea $K_\mathfrak{p}$ la completación de un cuerpo de números respecto del valor absoluto $\mathfrak{p}$-ádico, y fijemos una clausura algebraica $\overline{K}_\mathfrak{p}$. En esta sección, vamos a clasificar las extensiones de $K_\mathfrak{p}$ según la ramificación de las mismas. Utilizaremos la siguiente notación:

- $\mathcal{O}_\mathfrak{p}$, $\mathfrak{M}_\mathfrak{p}$ y $k_\mathfrak{p}$ denotan el anillo de valoración, el ideal de valoración y el cuerpo de residuos de $K_\mathfrak{p}$, respectivamente. La característica de $k_\mathfrak{p}$, denotada $\mathrm{char}(k_\mathfrak{p})$, es $p > 0$, con p un primo entero. El cardinal de $k_\mathfrak{p}$ es una potencia de p, que denotaremos q. Es decir, $k_\mathfrak{p} \cong \mathbb{F}_q$.
- Si $F/K_\mathfrak{p}$ es una extensión algebraica de $K_\mathfrak{p}$, siempre asumiremos que $F \subset \overline{K}_\mathfrak{p}$. Denotamos v_F a la valoración normalizada asociada a la extensión de $v_\mathfrak{p}$ a F. De manera similar, $\mathcal{O}_F$, $\mathfrak{M}_F$ y k_F denotan el anillo de valoración, el ideal de valoración y el cuerpo de residuos de F, respectivamente.

Extensiones no ramificadas de $K_\mathfrak{p}$

Definición 1.11. Una extensión finita $F/K_\mathfrak{p}$ se dice *no ramificada* si $e(F/K_\mathfrak{p}) = 1$. Se dice que una extensión algebraica de $K_\mathfrak{p}$ es *no ramificada* si puede expresarse como unión de extensiones finitas de $K_\mathfrak{p}$ no ramificadas.

Observación 1.1. Sea $F/K_\mathfrak{p}$ una extensión finita y no ramificada. Entonces, por la identidad fundamental,

$$[F : K_\mathfrak{p}] = [k_F : k_\mathfrak{p}] = f(F/K_\mathfrak{p}).$$

De hecho, dado que $k_\mathfrak{p} \cong \mathbb{F}_q$, se sigue que $k_F \cong \mathbb{F}_{q^f}$, siendo $f = f(F/K_\mathfrak{p})$. Además, si π es un uniformizante en $K_\mathfrak{p}$, también lo es en F, pues $e(F/K_\mathfrak{p}) = v_F(\pi) = 1$. Esto implica que

$$v_F(F^\times) = v_\mathfrak{p}(K_\mathfrak{p}^\times).$$

Proposición 1.10. Se verifican las siguientes propiedades:

- Sean $F/K_\mathfrak{p}$ y $F'/K_\mathfrak{p}$ dos extensiones algebraicas. Si $F/K_\mathfrak{p}$ es no ramificada, entonces FF'/F' es no ramificada.
- Toda subextensión de una extensión no ramificada de $K_\mathfrak{p}$ es no ramificada.
- El compositum dentro de $\overline{K}_\mathfrak{p}$ de un número finito de extensiones no ramificadas de $K_\mathfrak{p}$ es una extensión no ramificada de $K_\mathfrak{p}$.

Demostración. Ver página 153, proposición (7.2) y corolario (7.3) de [Neu13]. □

Definición 1.12. Sea $F/K_\mathfrak{p}$ una extensión algebraica. El cuerpo obtenido como la unión de todas las subextensiones no ramificadas de $F/K_\mathfrak{p}$ se llama *máxima subextensión no ramificada de* $F/K_\mathfrak{p}$. En particular, la máxima subextensión no ramificada de $\overline{K}_\mathfrak{p}/K_\mathfrak{p}$ se llama *máxima extensión no ramificada de* $K_\mathfrak{p}$, y se denota $K_\mathfrak{p}^{\mathrm{unr}}$.

En el resto de la sección, vamos a dar una serie de resultados cuya demostración se encuentra en el apéndice. Esto se ha decidido así para facilitar la lectura y por la cantidad de espacio que ocupan dichas demostraciones.

En primer lugar, vamos a hallar una expresión explícita de $K_\mathfrak{p}^{\mathrm{unr}}$.

Proposición 1.11. Sea $\zeta_n \in \overline{K}_\mathfrak{p}$ una raíz primitiva n-ésima de la unidad, con $\gcd(n, p) = 1$, y denotemos $F = K_\mathfrak{p}(\zeta_n)$. Entonces, la extensión $F/K_\mathfrak{p}$ es no ramificada de grado f, siendo f el menor entero positivo tal que $q^f \equiv 1 \bmod n$.

Demostración. Ver apéndice A.5. □

Teorema 1.6. *Sea $F/K_\mathfrak{p}$ una extensión finita. Entonces, $F/K_\mathfrak{p}$ es no ramificada de grado n si y sólo si $F \cong K_\mathfrak{p}(\zeta_{q^n-1})$, siendo $\zeta_{q^n-1} \in \overline{K}_\mathfrak{p}$ una raíz primitiva (q^n-1)-ésima de la unidad. En este caso, $F/K_\mathfrak{p}$ es una extensión de Galois tal que $\mathrm{Gal}(F/K_\mathfrak{p}) \cong \mathrm{Gal}(k_F/k_\mathfrak{p})$.*

Demostración. Ver apéndice A.5. □

Observemos que, para todo entero positivo m, los números de la forma $q^m - 1$ son enteros positivos coprimos con p. Esta observación junto con el teorema anterior nos da el siguiente corolario.

Corolario 1.3. La máxima extensión no ramificada de $K_\mathfrak{p}$ es

$$K_\mathfrak{p}^{\mathrm{unr}} = \bigcup_{\substack{n\geq 1,\\ \gcd(n,p)=1}} K_\mathfrak{p}(\zeta_n).$$

Observación 1.2. $K_\mathfrak{p}^{\mathrm{unr}}$ es un cuerpo henseliano (ver definicion A.20). Esto se debe al teorema A.5: si denotamos w a la extensión de $v_\mathfrak{p}$ a $K_\mathfrak{p}^{\mathrm{unr}}$, entonces $w(K_\mathfrak{p}^{\mathrm{unr}\times}) = v_\mathfrak{p}(K_\mathfrak{p}^\times)$. Además, w es discreta pues $v_\mathfrak{p}$ lo es. Por estos motivos, es habitual denotar $v_\mathfrak{p}$ a w, abusando la notación. Se puede probar[6] que para toda extensión finita $F/K_\mathfrak{p}^{\mathrm{unr}}$, se verifica la identidad fundamental:

$$[F : K_\mathfrak{p}^{\mathrm{unr}}] = e(F/K_\mathfrak{p}^{\mathrm{unr}})f(F/K_\mathfrak{p}^{\mathrm{unr}}).$$

Por otro lado, si $k_\mathfrak{p}^{\mathrm{unr}}$ denota al cuerpo de residuos de $K_\mathfrak{p}^{\mathrm{unr}}$, se verifica que $k_\mathfrak{p}^{\mathrm{unr}} \cong \overline{k}_\mathfrak{p} \cong \overline{\mathbb{F}}_q$, y de hecho, no es difícil comprobar a partir del teorema 1.6 y la proposición 1.10 que

$$\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{unr}}/K_\mathfrak{p}) \cong \mathrm{Gal}(\overline{k}_\mathfrak{p}/k_\mathfrak{p}) \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q).$$

En particular, si $F/K_\mathfrak{p}^{\mathrm{unr}}$ es una extensión finita, el cuerpo de residuos k_F es isomorfo a $k_\mathfrak{p}^{\mathrm{unr}}$, por ser una extensión finita de un cuerpo algebraicamente cerrado. Entonces, la identidad fundamental se reduce a

$$[F : K_\mathfrak{p}^{\mathrm{unr}}] = e(F/K_\mathfrak{p}^{\mathrm{unr}}).$$

Extensiones moderadas de $K_\mathfrak{p}$

Definición 1.13. Si $F/K_\mathfrak{p}$ es una extensión finita, se dice que $F/K_\mathfrak{p}$ es *moderada* si $e(F/K_\mathfrak{p})$ es coprimo con $p = \mathrm{char}(k_\mathfrak{p})$. Se dice que una extensión algebraica de $K_\mathfrak{p}$ es *moderada* si puede expresarse como unión de extensiones finitas de $K_\mathfrak{p}$ moderadas.

Observación 1.3. Sea $F/K_\mathfrak{p}$ una extensión finita. Notemos que $F/K_\mathfrak{p}$ es moderada si y sólo si $FK_\mathfrak{p}^{\mathrm{unr}}/K_\mathfrak{p}^{\mathrm{unr}}$ lo es, pues $e(FK_\mathfrak{p}^{\mathrm{unr}}/K_\mathfrak{p}^{\mathrm{unr}}) = e(F/K_\mathfrak{p})$.

Proposición 1.12. Se verifican las siguientes propiedades:

- Sean $F/K_\mathfrak{p}$ y $F'/K_\mathfrak{p}$ dos extensiones algebraicas. Si $F/K_\mathfrak{p}$ es moderada, entonces FF'/F' es moderada
- Toda subextensión de una extensión moderada de $K_\mathfrak{p}$ es moderada.
- El compositum dentro de $\overline{K}_\mathfrak{p}$ de un número finito de extensiones moderadas de $K_\mathfrak{p}$ es una extensión moderada de $K_\mathfrak{p}$.

Demostración. Ver página 156, corolario (7.8) de [Neu13]. □

Definición 1.14. Sea $F/K_\mathfrak{p}$ una extensión algebraica. El cuerpo obtenido como la unión de todas las subextensiones moderadas de $F/K_\mathfrak{p}$ se llama *máxima subextensión moderada de* $F/K_\mathfrak{p}$. En particular, la máxima subextensión moderada de $\overline{K}_\mathfrak{p}/K_\mathfrak{p}$ se llama *máxima extensión moderada de* $K_\mathfrak{p}$, y se denota $K_\mathfrak{p}^{\mathrm{tame}}$.

[6] Hemos enunciado la identidad fundamental para extensiones finitas de $K_\mathfrak{p}$, pero se puede generalizar cambiando $K_\mathfrak{p}$ por una extensión infinita Ω de $K_\mathfrak{p}$, siempre que Ω sea un cuerpo henseliano. La referencia dada en la proposición 1.9 lo demuestra en este caso.

Vamos a hallar una expresión explícita $K_{\mathfrak{p}}^{\text{tame}}$. Por la observación 1.3, basta hallar las extensiones finitas moderadas de $K_{\mathfrak{p}}^{\text{unr}}$. Para cada entero positivo n coprimo con p, definimos

$$F_n = K_{\mathfrak{p}}^{\text{unr}}(\sqrt[n]{\pi}),$$

siendo π un uniformizante en $K_{\mathfrak{p}}^{\text{unr}}$ y $\sqrt[n]{\pi}$ una raíz del polinomio $x^n - \pi$. Denotemos $\boldsymbol{\mu}_n$ al grupo de las raíces n-ésimas de la unidad en $\overline{K}_{\mathfrak{p}}$.

Proposición 1.13. Para todo entero positivo n coprimo con p, la extensión $F_n/K_{\mathfrak{p}}^{\text{unr}}$ es de Galois de grado n, con $\text{Gal}(F_n/K_{\mathfrak{p}}^{\text{unr}}) \cong \boldsymbol{\mu}_n$.

Demostración. El polinomio mínimo de $F_n/K_{\mathfrak{p}}^{\text{unr}}$ es $x^n - \pi$, que es irreducible por el criterio de Eisenstein (ver proposición A.6). Sea $\zeta_n \in \boldsymbol{\mu}_n$ una raíz primitiva n-ésima de la unidad. Entonces, las raíces de $x^n - \pi$ son

$$\zeta_n^i \sqrt[n]{\pi}, \text{ para } i = 0, \ldots, n-1.$$

Como $\gcd(n, p) = 1$, entonces $\zeta_n \in K_{\mathfrak{p}}^{\text{unr}}$, luego todas las raíces de $x^n - \pi$ están en F_n. Por tanto, la extensión $F_n/K_{\mathfrak{p}}^{\text{unr}}$ es de Galois y de grado n.

Además, $\text{Gal}(F_n/K_{\mathfrak{p}}^{\text{unr}})$ actúa en las raíces de $x^n - \pi$ permutándolas, luego podemos considerar un homomorfismo $\theta_n \colon \text{Gal}(F_n/K_{\mathfrak{p}}^{\text{unr}}) \to \boldsymbol{\mu}_n$ tal que

$$\sigma(\sqrt[n]{\pi}) = \theta_n(\sigma)\sqrt[n]{\pi}, \text{ con } \sigma \in \text{Gal}(F_n/K_{\mathfrak{p}}^{\text{unr}}).$$

Está claro que θ_n es inyectivo, y como $\text{Gal}(F_n/K_{\mathfrak{p}}^{\text{unr}})$ y $\boldsymbol{\mu}_n$ tienen el mismo cardinal (igual a n), entonces θ_n es un isomorfismo. □

Proposición 1.14. Para todo entero positivo n coprimo con p, la extensión $F_n/K_{\mathfrak{p}}^{\text{unr}}$ es moderada. Además, F_n no depende del uniformizante de $K_{\mathfrak{p}}^{\text{unr}}$ elegido.

Demostración. Sea n un entero positivo coprimo con p. Por la identidad fundamental,

$$n = [F_n : K_{\mathfrak{p}}^{\text{unr}}] = e(F_n/K_{\mathfrak{p}}^{\text{unr}})$$

y como $\gcd(n, p) = 1$, entonces $F_n/K_{\mathfrak{p}}^{\text{unr}}$ es moderada.

Veamos que $F_n/K_{\mathfrak{p}}^{\text{unr}}$ no depende de la elección de π. En efecto, si π' es otro uniformizante en $K_{\mathfrak{p}}^{\text{unr}}$, entonces existe una unidad ε en el anillo de valoración de $K_{\mathfrak{p}}^{\text{unr}}$ tal que $\pi' = \varepsilon\pi$, luego $\sqrt[n]{\pi'} = \sqrt[n]{\varepsilon}\sqrt[n]{\pi}$. Ahora bien, el cuerpo de residuos k_n de F_n es algebraicamente cerrado, luego la reducción del polinomio $\phi(x) = x^n - \varepsilon$ en k_n es un polinomio que se descompone en factores lineales. Además, como $p \nmid n$, entonces $\gcd(\phi, \phi') = 1$, luego dichos factores lineales son distintos. Esto implica que $\sqrt[n]{\varepsilon} \in K_{\mathfrak{p}}^{\text{unr}}$, por el lema de Hensel (ver observación 1.2). Concluimos que F_n no depende del uniformizante elegido, como queríamos. □

Teorema 1.7. *Sea $F/K_{\mathfrak{p}}^{\text{unr}}$ una extensión finita. Entonces, $F/K_{\mathfrak{p}}^{\text{unr}}$ es moderada de grado n si y sólo si $\gcd(n, p) = 1$ y $F \cong K_{\mathfrak{p}}^{\text{unr}}(\sqrt[n]{\pi})$ para algún uniformizante π de $K_{\mathfrak{p}}^{\text{unr}}$.*

Demostración. Ver apéndice A.5. □

Corolario 1.4. Sea π un uniformizante en $K_{\mathfrak{p}}^{\text{unr}}$. La máxima extensión moderada de $K_{\mathfrak{p}}$ es

$$K_{\mathfrak{p}}^{\text{tame}} = \bigcup_{\substack{n \geq 1, \\ \gcd(n,p)=1}} K_{\mathfrak{p}}^{\text{unr}}(\sqrt[n]{\pi}).$$

Grupos de inercia y de inercia salvaje

A continuación, daremos propiedades de ciertos subgrupos de $G_{K_\mathfrak{p}} = \mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p})$ relacionados con la máxima extensión no ramificada y moderada de $K_\mathfrak{p}$.

Definición 1.15. Dada una extensión de Galois $F/K_\mathfrak{p}$, se define el *grupo de inercia de* $\mathrm{Gal}(F/K_\mathfrak{p})$ como

$$I(F/K_\mathfrak{p}) = \mathrm{Gal}(F/F \cap K_\mathfrak{p}^{\mathrm{unr}}).$$

Si $F = \overline{K}_\mathfrak{p}$, se define el *grupo de inercia de* $G_{K_\mathfrak{p}}$ como

$$I_\mathfrak{p} = \mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p}^{\mathrm{unr}}).$$

Proposición 1.15. Existe un isomorfismo de grupos topológicos

$$I_\mathfrak{p} \cong \varprojlim I(F/K_\mathfrak{p}),$$

donde F recorre todas las extensiones finitas de Galois de $K_\mathfrak{p}$.

Demostración. Por el teorema 1.2, tenemos que

$$I_\mathfrak{p} = \mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p}^{\mathrm{unr}}) \cong \varprojlim \mathrm{Gal}(E/K_\mathfrak{p}^{\mathrm{unr}}),$$

donde E recorre las extensiones finitas de Galois de $K_\mathfrak{p}^{\mathrm{unr}}$. Ahora bien, para toda tal extensión $E/K_\mathfrak{p}^{\mathrm{unr}}$, existe una extensión $F/K_\mathfrak{p}$ finita de Galois tal que $E = FK_\mathfrak{p}^{\mathrm{unr}}$. Se sigue de esta observación y de la proposición 1.3 que

$$I_\mathfrak{p} \cong \varprojlim \mathrm{Gal}(FK_\mathfrak{p}^{\mathrm{unr}}/K_\mathfrak{p}^{\mathrm{unr}}) \cong \varprojlim \mathrm{Gal}(F/F \cap K_\mathfrak{p}^{\mathrm{unr}}) = \varprojlim I(F/K_\mathfrak{p}),$$

como queríamos. □

Definición 1.16. Dada una extensión de Galois $F/K_\mathfrak{p}$ una extensión finita de Galois, se define el *grupo de inercia salvaje de* $\mathrm{Gal}(F/K_\mathfrak{p})$ como

$$I^{\mathrm{wild}}(F/K_\mathfrak{p}) = \mathrm{Gal}(F/F \cap K_\mathfrak{p}^{\mathrm{tame}}).$$

Si $F = \overline{K}_\mathfrak{p}$, se define el *grupo de inercia salvaje de* $G_{K_\mathfrak{p}}$ como

$$I_\mathfrak{p}^{\mathrm{wild}} = \mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p}^{\mathrm{tame}}).$$

La siguiente proposición se demuestra de manera análoga a la proposición 1.15.

Proposición 1.16. Existe un isomorfismo de grupos topológicos

$$I_\mathfrak{p}^{\mathrm{wild}} \cong \varprojlim I^{\mathrm{wild}}(F/K_\mathfrak{p}),$$

donde F recorre todas las extensiones finitas de Galois de $K_\mathfrak{p}$.

Definición 1.17. Se define el *grupo de inercia moderada de* $G_{K_\mathfrak{p}}$ como $I_\mathfrak{p}^{\mathrm{tame}} = I_\mathfrak{p}/I_\mathfrak{p}^{\mathrm{wild}}$.

Vamos a dar una descripción explícita del grupo de inercia moderada I_p^{tame} de $G_{\mathbb{Q}_p} = \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, por simplicidad de la exposición. Denotemos $\boldsymbol{\mu}_d$ al grupo de las raíces d-ésimas de la unidad de $\overline{\mathbb{Q}}_p$. Si d y d' son enteros positivos coprimos con p tales que $d \mid d'$, consideramos el homomorfismo

$$\begin{aligned} f_{dd'} \colon \boldsymbol{\mu}_{d'} &\to \boldsymbol{\mu}_d \\ \zeta_{d'} &\mapsto \zeta_{d'}^{d'/d}. \end{aligned}$$

Entonces, $(\boldsymbol{\mu}_d, f_{dd'})$ es un sistema inverso indexado por los enteros positivos coprimos con p, con el orden parcial dado por la divisibilidad. Denotemos $\varprojlim_{(d,p)=1} \boldsymbol{\mu}_d$ al límite inverso de $(\boldsymbol{\mu}_d, f_{dd'})$. Por el teorema 1.2 y la proposición 1.13,

$$I_p^{\text{tame}} \cong \text{Gal}(\mathbb{Q}_p^{\text{tame}}/\mathbb{Q}_p^{\text{unr}}) \cong \varprojlim_{(d,p)=1} \text{Gal}(\mathbb{Q}_p^{\text{unr}}(\sqrt[d]{p})/\mathbb{Q}_p^{\text{unr}}) \cong \varprojlim_{(d,p)=1} \boldsymbol{\mu}_d. \tag{1.3}$$

Vamos a identificar I_p^{tame} con otro límite inverso. Para ello, si m y n son enteros positivos tales que $m \mid n$, consideramos el homomorfismo

$$\begin{aligned} N_{mn} \colon \mathbb{F}_{p^n}^\times &\to \mathbb{F}_{p^m}^\times \\ x &\mapsto x^{1+q+\cdots+q^{n-1}}, \end{aligned}$$

siendo $q = p^m$. Es decir, N_{mn} es el homomorfismo dado por la norma relativa a la extensión $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$. Entonces, $(\mathbb{F}_{p^n}^\times, N_{mn})$ es un sistema inverso indexado por los enteros positivos y con el orden parcial dado por la divisibilidad. Denotemos $\varprojlim_n \mathbb{F}_{p^n}^\times$ al límite inverso de $(\mathbb{F}_{p^n}^\times, N_{mn})$.

Proposición 1.17. Existe un isomorfismo $I_p^{\text{tame}} \cong \varprojlim_n \mathbb{F}_{p^n}^\times$.

Demostración. Por (1.3), basta probar que $\varprojlim_{(d,p)=1} \boldsymbol{\mu}_d \cong \varprojlim_n \mathbb{F}_{p^n}^\times$. Por un lado, está claro que $\mathbb{F}_{p^n}^\times \cong \boldsymbol{\mu}_{p^n-1}$, pues ambos grupos son cíclicos de orden $p^n - 1$. Por tanto, gracias al teorema A.1, basta comprobar que el conjunto formado por los números de la forma $p^n - 1$, para cada entero $n \geq 1$, es cofinal en el conjunto

$$S = \{d \in \mathbb{Z} : d \geq 1, \gcd(d, p) = 1\}.$$

Esto es cierto, pues para todo $d \in S$ existe un entero $n \geq 1$ tal que $p^n - 1 \equiv 0 \bmod d$. En efecto, basta tomar $n = \varphi(d)$, siendo φ la función de Euler. De este modo, d divide a $p^n - 1$, como queríamos. □

Para acabar esta sección, vamos a demostrar un resultado que será de gran utilidad a la hora de definir el peso de la conjetura de modularidad de Serre. Para ello, es necesario definir el concepto de *elemento de Frobenius en* $G_{\mathbb{Q}_p}$.

Observación. La extensión $\mathbb{Q}_p^{\text{unr}}/\mathbb{Q}_p$ es de Galois, luego por el teorema de correspondencia de Galois, la restricción $G_{\mathbb{Q}_p} \to \text{Gal}(\mathbb{Q}_p^{\text{unr}}/\mathbb{Q}_p)$ induce un isomorfismo de grupos topológicos

$$G_{\mathbb{Q}_p}/I_p \cong \text{Gal}(\mathbb{Q}_p^{\text{unr}}/\mathbb{Q}_p).$$

El grupo $G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ está topológicamente generado por el automorfismo de Frobenius $x \mapsto x^p$. Es decir, si denotamos σ_p al automorfismo de Frobenius, entonces $\langle \sigma_p \rangle$ es un subgrupo denso de $G_{\mathbb{F}_p}$. Por la observación 1.2, $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}/\mathbb{Q}_p) \cong G_{\mathbb{F}_p}$, luego podemos componer este isomorfismo con la restricción $G_{\mathbb{Q}_p} \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}/\mathbb{Q}_p)$ para obtener el homomorfismo reducción

$$G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}.$$

Definición 1.18. Se llama *elemento de Frobenius de* $G_{\mathbb{Q}_p}$ a cualquier automorfismo $\sigma \in G_{\mathbb{Q}_p}$ tal que su imagen por el homomorfismo reducción es el automorfismo de Frobenius $x \mapsto x^p$, y se denota $\mathrm{Frob}_p = \sigma$.

Proposición 1.18. Sea $s = \mathrm{Frob}_p \in G_{\mathbb{Q}_p}$. Para todo $u \in I_p$, se verifica

$$sus^{-1} \equiv u^p \text{ mód } I_p^{\mathrm{wild}}.$$

Demostración. Observemos la proposición equivale a probar

$$(sus^{-1})|_{\mathbb{Q}_p^{\mathrm{tame}}} = u^p|_{\mathbb{Q}_p^{\mathrm{tame}}}. \tag{1.4}$$

De hecho, basta probar (1.4) al aplicarlo a los elementos de la forma $\sqrt[n]{p}$ para todo entero n coprimo con p, pues cualquier elemento de $\mathbb{Q}_p^{\mathrm{tame}}$ pertenece a $\mathbb{Q}_p^{\mathrm{unr}}(\sqrt[n]{p})$ para algún entero n coprimo con p, por el corolario 1.4.

Como $\gcd(n,p) = 1$, entonces $\mathbb{Q}_p^{\mathrm{unr}}$ contiene todas las raíces n-ésimas de la unidad, por el corolario 1.3. Sea $\zeta_n \in \mathbb{Q}_p^{\mathrm{unr}}$ una raíz primitiva n-ésima de la unidad. El polinomio mínimo de la extensión $\mathbb{Q}_p^{\mathrm{unr}}(\sqrt[n]{p})/\mathbb{Q}_p^{\mathrm{unr}}$ es $x^n - p$, cuyas raíces son $\zeta_n^i \sqrt[n]{p}$ para $i = 1, \ldots, n$.

Sabemos que u deja fijas las raíces n-ésimas de la unidad, y $s = \mathrm{Frob}_p$ actúa en las raíces n-ésimas de la unidad elevando a p. Tanto s como u permutan las raíces de $x^n - p$. En particular,

$$s^{-1}(\sqrt[n]{p}) = \zeta_n^i \sqrt[n]{p}, \text{ y } u(\sqrt[n]{p}) = \zeta_n^j \sqrt[n]{p} \text{ para ciertos } i, j \in \{1, \ldots, n\}.$$

Teniendo en cuenta todas estas consideraciones, se sigue que

$$\begin{aligned} u^p(\sqrt[n]{p}) &= u^{p-1}u(\sqrt[n]{p}) = u^{p-1}(\zeta_n^j \sqrt[n]{p}) = \zeta_n^j u^{p-1}(\sqrt[n]{p}) \\ &= \zeta_n^j u^{p-2}u(\sqrt[n]{p}) = \zeta_n^j u^{p-2}(\zeta_n^j \sqrt[n]{p}) = (\zeta_n^j)^2 u^{p-2}(\sqrt[n]{p}) = \cdots = (\zeta_n^j)^p \sqrt[n]{p}. \end{aligned}$$

Por otro lado,

$$\begin{aligned} sus^{-1}(\sqrt[n]{p}) &= su(\zeta_n^i \sqrt[n]{p}) = s(u(\zeta_n^i)u(\sqrt[n]{p})) = s(\zeta_n^i \zeta_n^j (\sqrt[n]{p})) \\ &= s(\zeta_n^j \zeta_n^i \sqrt[n]{p}) = s(\zeta_n^j)s(\zeta_n^i \sqrt[n]{p}) = (\zeta_n^j)^p s(s^{-1}(\sqrt[n]{p})) = (\zeta_n^j)^p \sqrt[n]{p}. \end{aligned}$$

Concluimos que $sus^{-1}(\sqrt[n]{p}) = u^p(\sqrt[n]{p})$, como queríamos. □

1.5. Grupos de alta ramificación

Sea $K_\mathfrak{p}$ la completación de un cuerpo de números respecto del valor absoluto $\mathfrak{p}$-ádico, y fijemos una clausura algebraica $\overline{K}_\mathfrak{p}$. Sea $G = \mathrm{Gal}(F/K_\mathfrak{p})$, con $F/K_\mathfrak{p}$ una extensión finita de Galois. La notación de esta sección es la misma que la de la sección anterior.

Definición 1.19. Para todo real $u \geq -1$, se define el *u-ésimo grupo de ramificación de G con numeración baja* como

$$G_u = \{\sigma \in G : v_F(\sigma(x) - x) \geq u + 1 \text{ para todo } x \in \mathcal{O}_F\}.$$

Observación. Sean $n \geq -1$ un entero, y $x \in F$. Por la proposición A.5, $v_F(x) \geq n+1$ si y sólo si $x \in \mathfrak{M}_F^{n+1}$, pues v_F está normalizada. Por el lema A.2, $v_F(x) = v_F(\sigma x)$ para todo $\sigma \in G$, luego $v_F(x) \geq n+1$ si y sólo $v_F(\sigma x) \geq n+1$, y esto equivale a que $\sigma x \in \mathfrak{M}_F^{n+1}$ por la proposición A.5 de nuevo. En otras palabras,

$$\sigma\left(\mathfrak{M}_F^{n+1}\right) = \mathfrak{M}_F^{n+1} \text{ para todo entero } n \geq -1 \text{ y para todo } \sigma \in G.$$

Esto implica que todo automorfismo $\sigma \in G$ induce un automorfismo $\sigma \bmod \mathfrak{M}_F$ en el anillo $\mathcal{O}_F/\mathfrak{M}_F^{n+1}$, y podemos considerar el homomorfismo sobreyectivo $G \to \mathrm{Aut}(\mathcal{O}_F/\mathfrak{M}_F^{n+1})$ dado por $\sigma \mapsto \sigma \bmod \mathfrak{M}_F^{n+1}$ para todo entero $n \geq -1$. Entonces, está claro que el n-ésimo grupo de ramificación G_n es el núcleo de dicho homomorfismo, pues

$$v_F(\sigma(x) - x) \geq n+1 \iff \sigma(x) - x \in \mathfrak{M}_F^{n+1} \iff \sigma(x) \equiv x \bmod \mathfrak{M}_F^{n+1}.$$

Proposición 1.19. Se verifican las siguientes igualdades:

$$G_{-1} = G, \;\; G_0 = I(F/K_\mathfrak{p}) \;\text{ y }\; G_1 = I^{\mathrm{wild}}(F/K_\mathfrak{p}).$$

Demostración. Ver apéndice A.5. □

Proposición 1.20. G_1 es el único p-subgrupo de Sylow[7] de G_0.

Demostración. Ver página 174, proposición (9.12) de [Neu13]. □

En general, los grupos de alta ramificación forman una cadena decreciente de subgrupos

$$G_0 \supset G_1 \supset \cdots \supset G_u \supset \ldots$$

de manera que G_u es trivial a partir de un cierto real u. Además, para todo real $u \geq -1$, G_u es un subgrupo normal de G. En efecto, sean $\sigma \in G_u$, $\tau \in G$ y $x \in \mathcal{O}_F$. Entonces,

$$v_F(\tau^{-1}\sigma\tau x - x) = v_F(\tau^{-1}(\sigma\tau x - \tau x)) = v_F(\sigma(\tau x) - \tau x),$$

y se concluye el resultado pues $\tau\mathcal{O}_F = \mathcal{O}_F$ por el lema A.2. También se verifica que $G_u = G_{\lceil u \rceil}$ para todo real $u \geq -1$.

[7] Un p-subgrupo de Sylow de un grupo G es cualquier subgrupo de G de orden p^m, siendo m un entero tal que p^m es la mayor potencia de p que divide al orden de G.

Definición 1.20. Se define la *función de Herbrand* $\varphi_{F/K_\mathfrak{p}}\colon [-1,\infty) \to [-1,\infty)$ *asociada a* G como

$$\varphi_{F/K_\mathfrak{p}}(u) = \int_{-1}^{u} \frac{dt}{[G_0 : G_t]}.$$

Por convenio, $[G_0 : G_t]^{-1} = [G_{-1} : G_0]^{-1}$ si $t = -1$, y $[G_0 : G_t]^{-1} = [G_0 : G_0]^{-1} = 1$ si $-1 < t \leq 0$. Es decir, $\varphi_{F/K_\mathfrak{p}}(u) = u$ para todo $u \in [-1, 0]$.

Observación 1.4. Denotemos g_u al orden de G_u para todo real $u \geq -1$. Es inmediato comprobar que $\varphi_{F/K_\mathfrak{p}}(0) = 0$ y que $\varphi_{F/K_\mathfrak{p}}$ es continua, lineal a trozos y estrictamente creciente. De hecho,

$$\varphi_{F/K_\mathfrak{p}}(u) = \frac{1}{g_0}(g_1 + \cdots + g_{\lfloor u \rfloor} + (u - \lfloor u \rfloor) g_{\lceil u \rceil}) \quad \text{para todo } u > 0, \text{ y}$$
$$\varphi'_{F/K_\mathfrak{p}}(u) = \frac{1}{[G_0 : G_u]} = \frac{g_u}{g_0} = \frac{g_{\lceil u \rceil}}{g_0} \quad \text{para todo } u \notin \mathbb{Z},\ u > -1.$$

Además, $\varphi'_{F/K_\mathfrak{p}}(u)$ es constante para todo $i \leq u < i + 1$ con $i \geq -1$ entero, pues

$$[G_0 : G_u]^{-1} = [G_0 : G_{i+1}]^{-1} \text{ para todo } i \leq u < i + 1 \text{ con } i \in \mathbb{Z},\ i \geq -1.$$

En particular, $\varphi_{F/K_\mathfrak{p}}$ es un homeomorfismo del intervalo $[-1,\infty)$ en sí mismo. A la función inversa $\varphi^{-1}_{F/K_\mathfrak{p}}$ la denotamos $\psi_{F/K_\mathfrak{p}}$.

Definición 1.21. Para todo real $r \geq -1$, se define el *r-ésimo grupo de ramificación de G con numeración alta* como $G^r = G_{\psi_{F/K_\mathfrak{p}}(r)}$.

Teorema 1.8 (Teorema de Herbrand)**.** *Sean $F'/K_\mathfrak{p}$ una subextensión de Galois de $F/K_\mathfrak{p}$, y $H = \mathrm{Gal}(F/F') \subset G$. Si $t = \varphi_{F/F'}(u)$ para algún $u \geq -1$ entonces $G_u H/H = (G/H)_t$.*

Demostración. Ver capítulo IV, sección 3, lema 5 de [Ser13]. □

Corolario 1.5. Sea $F'/K_\mathfrak{p}$ una subextensión de Galois de $F/K_\mathfrak{p}$. Entonces,

$$\varphi_{F/K_\mathfrak{p}} = \varphi_{F'/K_\mathfrak{p}} \circ \varphi_{F/F'} \text{ y } \psi_{F/K_\mathfrak{p}} = \psi_{F/F'} \circ \psi_{F'/K_\mathfrak{p}}.$$

Demostración. Ver capítulo IV, sección 3, proposición 15 de [Ser13]. □

Corolario 1.6. Sean $F'/K_\mathfrak{p}$ una subextensión de Galois de $F/K_\mathfrak{p}$, y $H = \mathrm{Gal}(F/F') \subset G$. Entonces,

$$(G/H)^r = G^r H/H \text{ para todo } r \geq -1.$$

Demostración. Sea $r \geq -1$ real. Por definición y por el teorema de Herbrand, sabemos que

$$G^r H/H = G_{\psi_{F/K_\mathfrak{p}}(r)} H/H = (G/H)_t,$$

donde $t = \varphi_{F/F'}(\psi_{F/K_\mathfrak{p}}(r))$. Por el corolario anterior, sabemos que

$$\psi_{F/K_\mathfrak{p}} = \psi_{F/F'} \circ \psi_{F'/K_\mathfrak{p}},$$

luego $t = \varphi_{F/F'}(\psi_{F/F'} \circ \psi_{F'/K_\mathfrak{p}}(r)) = \varphi_{F/F'} \circ \psi_{F/F'} \circ \psi_{F'/K_\mathfrak{p}}(r) = \psi_{F'/K_\mathfrak{p}}(r)$, pues $\varphi_{F/F'}$ es la inversa de $\psi_{F/F'}$. Por tanto,

$$G^r H/H = (G/H)_t = (G/H)_{\psi_{F'/K_\mathfrak{p}}(r)} = (G/H)^r,$$

como queríamos. □

2 Representaciones de Galois

"Groups, as men, will be known by their actions."

— Guillermo Moreno.

El grupo absoluto de Galois $G_{\mathbb{Q}}$ es un objeto central en la teoría algebraica de números, pues contiene información sobre todas las extensiones de Galois de $\mathbb{Q}$. En efecto, si $K/\mathbb{Q}$ es una extensión de Galois, entonces podemos expresar $\mathrm{Gal}(K/\mathbb{Q})$ como un cociente de $G_{\mathbb{Q}}$ gracias al teorema de correspondencia de Galois.

La forma estándar de estudiar estos cocientes es tratar de identificarlos con un subgrupo de un grupo de matrices bien conocido. Esto se consigue a través de las *representaciones* de $G_{\mathbb{Q}}$. Por ello, comenzamos este capítulo con una introducción sobre las representaciones de grupos en general, para luego centrarnos en las representaciones de $G_{\mathbb{Q}}$ y sus propiedades.

2.1. Representaciones de grupos

El contenido de esta sección se basa en la parte I de [Ser+77]. De ahora en adelante, si F es un cuerpo, $\mathrm{Aut}_F(V)$ denota el grupo de automorfismos de un F-espacio vectorial V.

Definición 2.1. Sean G un grupo y V un espacio vectorial de dimensión finita sobre un cuerpo F. Una *representación de G en V* es un homomorfismo de grupos $\rho\colon G \to \mathrm{Aut}_F(V)$.

Si ρ es una representación de G en V, también se dice que G *actúa en* V. Además, se define la *dimensión de* ρ como $\dim \rho = \dim_F(V)$. Por último, se dice que ρ es un *carácter de* G si $\dim \rho = 1$.

Definición 2.2. Dos representaciones $\rho, \rho'\colon G \to \mathrm{Aut}_F(V)$ se dicen *equivalentes* o *isomorfas*, y se denota $\rho \cong \rho'$, si existe $\tau \in \mathrm{Aut}_F(V)$ tal que

$$\rho(\sigma) = \tau\rho'(\sigma)\tau^{-1} \text{ para todo } \sigma \in G.$$

Sea $n = \dim_F(V)$. Eligiendo una base de V como F-espacio vectorial, podemos identificar $\mathrm{Aut}_F(V) \cong \mathrm{GL}_n(F)$ y trabajar con representaciones con codominio en $\mathrm{GL}_n(F)$.

Observación (Notación). Sea $\rho\colon G \to \mathrm{Aut}_F(V)$ una representación de dimensión 2. Después de elegir una base de V como F-espacio vectorial, la imagen por ρ de todo $\sigma \in G$ se expresa como

$$\rho(\sigma) = \begin{pmatrix} \alpha(\sigma) & \beta(\sigma) \\ \gamma(\sigma) & \delta(\sigma) \end{pmatrix}, \text{ siendo } \alpha, \beta, \gamma, \delta : G \to F \text{ funciones.}$$

En este caso, denotaremos

$$\rho = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

y si algún $\alpha, \beta, \gamma, \delta$ no es relevante, escribiremos $*$ en la entrada correspondiente de la matriz.

Definición 2.3. Sean $\rho\colon G \to \mathrm{Aut}_F(V)$ una representación y $W \subset V$ un subespacio. Se dice que W *es invariante por la acción de* G si

$$\rho(\sigma)w \in W \text{ para todo } w \in W \text{ y para todo } \sigma \in G.$$

En este caso, se dice que $\rho^W\colon G \to \mathrm{Aut}_F(W)$ es una *subrepresentación de* ρ.

Proposición 2.1. Sea $\rho\colon G \to \mathrm{Aut}_F(V)$ una representación. Si H es un subgrupo normal de G, entonces

$$V^H = \{v \in V : \rho(\tau)v = v \text{ para todo } \tau \in H\}$$

es un subespacio de V invariante por la acción de G.

Demostración. Sean $\sigma \in G$ y $v \in V^H$. Como H es un subgrupo normal de G, entonces $\sigma^{-1}\tau\sigma \in H$ para todo $\tau \in H$. Dado que ρ es un homomorfismo de grupos, se sigue que

$$v = \rho(\sigma^{-1}\tau\sigma)v = \rho(\sigma)^{-1}\rho(\tau)\rho(\sigma)v \text{ para todo } \tau \in H,$$

luego $\rho(\sigma)v = \rho(\tau)\rho(\sigma)v$ para todo $\tau \in H$. Concluimos que $\rho(\sigma)v \in V^H$, como queríamos. □

Definición 2.4. Sea $\rho\colon G \to \mathrm{Aut}_F(V)$ una representación. Se dice que ρ es *simple* o *irreducible* si los únicos subespacios de V invariantes por la acción de G son $\{\mathbf{0}\}$ y V. Se dice que ρ es *semisimple* si V admite una descomposición

$$V = \bigoplus_{i=1}^{r} V_i,$$

donde cada V_i es un subespacio de V invariante por la acción de G, y las subrepresentaciones $\rho^{V_i}\colon G \to \mathrm{Aut}_F(V_i)$ son irreducibles para todo $i \in \{1, \ldots, r\}$.

Definición 2.5. Dada una representación $\rho\colon G \to \mathrm{Aut}_F(V)$ de dimensión 2, se define la *semisimplificación de* ρ como la representación

$$\rho^{ss}\colon G \to \mathrm{Aut}(V^{ss}),$$

donde V^{ss} se define como sigue:

- Si ρ es irreducible, entonces $V^{ss} = V$.
- Si ρ es reducible, entonces $V^{ss} = W \oplus V/W$, siendo $W \subset V$ el subespacio maximal invariante por la acción de G.

Observación. Sea $\rho\colon G \to \mathrm{Aut}_F(V)$ una representación de dimensión 2. Si ρ es irreducible, está claro que ρ^{ss} es semisimple. Supongamos que ρ es reducible, y sea $W \subset V$ el subespacio maximal de dimensión 1 invariante por la acción de G. Si $W = \langle w \rangle$, entonces podemos tomar $\{w, v\}$ como base de V, para un cierto $v \in V - W$. Por tanto,

$$\rho = \begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix},$$

siendo ϕ_1 y ϕ_2 dos caracteres de G, y ρ actúa en W como el carácter ϕ_1. Entonces, $\{w, v+W\}$ es una base de V^{ss}, y por tanto,

$$\rho^{ss} = \begin{pmatrix} \phi_1 & 0 \\ 0 & \phi_2 \end{pmatrix},$$

luego ρ^{ss} es semisimple.

Definición 2.6. Sea $\rho\colon G \to \mathrm{Aut}_F(V)$ una representación de dimensión 2, dada por

$$\rho = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \text{ con } \alpha, \beta, \gamma, \delta\colon G \to F \text{ funciones.}$$

Si $\varepsilon\colon G \to F^\times$ es un carácter, la representación $\varepsilon \otimes \rho\colon G \to \mathrm{Aut}_F(V)$ dada por

$$\varepsilon \otimes \rho = \varepsilon \otimes \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \varepsilon\alpha & \varepsilon\beta \\ \varepsilon\gamma & \varepsilon\delta \end{pmatrix}$$

se llama *twist de ρ por ε*.

2.2. Representaciones de Galois

Ya estamos listos para poder definir el concepto de representación de Galois y sus características. Las principales referencias utilizadas para escribir el resto del capítulo son [Wie08] y el capítulo 9 de [DS05].

Definición 2.7. Sean K un cuerpo perfecto, F un cuerpo dotado de una topología, y V un F-espacio vectorial de dimensión finita. Una *representación de Galois* es un homomorfismo continuo

$$\rho\colon G_K \to \mathrm{Aut}_F(V),$$

de modo que la topología de G_K es la topología de Krull, y la topología de $\mathrm{Aut}_F(V)$ es la inducida por la topología usual de F.

Sea $\rho\colon G_K \to \mathrm{Aut}_F(V)$ una representación de Galois. La acción de G_K en V se puede restringir a la acción de cualquier subgrupo normal de G_K, y por el teorema de correspondencia de Galois, estos subgrupos son exactamente $\mathrm{Gal}(\overline{K}/L)$ con L/K una extensión de Galois. Será habitual considerar representaciones de $\mathrm{Gal}(\overline{K}/L)$ en estas condiciones, y también las llamaremos *representaciones de Galois*.

Hay distintos tipos de representaciones de Galois, dependiendo del cuerpo F y de su topología. Por ejemplo:

- ρ es una *representación módulo p* si $F = \overline{\mathbb{F}}_p$ con la topología discreta,
- ρ es una *representación ℓ-ádica* si $F = \overline{\mathbb{Q}}_\ell$ con la topología ℓ-ádica,
- ρ es una *representación de Artin* si $F = \mathbb{C}$ con la topología euclídea.

En este proyecto, nos centraremos en estudiar en las representaciones de Galois módulo p de los grupos de Galois $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ y $G_{\mathbb{Q}_\ell} = \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$, para algún primo entero ℓ.

Definición 2.8. Sea $\rho\colon G_K \to \mathrm{Aut}_F(V)$ una representación de Galois. Se dice que ρ *factoriza por una extensión finita* si existe una extensión finita L/K tal que $\mathrm{Gal}(\overline{K}/L) \subset \ker\rho$. En este caso, obtenemos un diagrama conmutativo

$$\begin{array}{ccc} G_K & \xrightarrow{\quad\rho\quad} & \mathrm{Aut}_F(V) \\ & {\scriptstyle\pi_L}\searrow \quad \nearrow{\scriptstyle\tilde{\rho}} & \\ & \mathrm{Gal}(L/K) & \end{array}$$

donde π_L es la restricción a L.

Proposición 2.2. Sea $\rho\colon G_K \to \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ una representación de Galois. Entonces, existe una extensión L/K finita de Galois tal que

$$\ker\rho = \mathrm{Gal}(\overline{K}/L) \text{ y } \rho(G_K) \cong \mathrm{Gal}(L/K).$$

Demostración. Sabemos que $\{\mathrm{id}\} \subset \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ es abierto en la topología discreta, luego $\ker\rho = \rho^{-1}(\{\mathrm{id}\})$ es abierto en la topología de Krull, por continuidad de ρ. Por tanto, existe una extensión finita de Galois L/K tal que $\ker\rho = \mathrm{Gal}(\overline{K}/L)$. De hecho, L es el subcuerpo de $\overline{K}$ fijo por $\ker\rho$.

Finalmente, por el primer teorema de isomorfía de Noether y por el teorema de correspondencia de Galois,

$$\rho(G_K) \cong G_K/\ker\rho = \mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/L) \cong \mathrm{Gal}(L/K),$$

como queríamos. □

Corolario 2.1. Sea $\rho\colon G_K \to \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ una representación de Galois de dimensión 1. Entonces, $\rho(G_K)$ es un grupo cíclico de orden coprimo con p.

Demostración. Basta observar que $\rho(G_K) \subset \mathbb{F}_{p^r}^\times$ para algún entero $r \geq 1$, pues $\rho(G_K)$ es un grupo finito por la proposición anterior. Como $\mathbb{F}_{p^r}^\times$ es un grupo cíclico de orden $p^r - 1$, entonces $\rho(G_K)$ es un subgrupo cíclico cuyo orden divide a $p^r - 1$, por el teorema de Lagrange. Concluimos que $\rho(G_K)$ es un grupo cíclico de orden coprimo con p. □

2.3. Ramificación

En esta sección, vamos a enunciar y demostrar propiedades de las representaciones de $G_{\mathbb{Q}}$ módulo p, relacionadas con la ramificación de un primo ℓ en extensiones finitas de $\mathbb{Q}$. Para ello, veamos en primer lugar cómo se puede relacionar la ramificación de ℓ en una extensión finita de Galois de $\mathbb{Q}$ con la ramificación de extensiones finitas de Galois de $\mathbb{Q}_\ell$.

Para cada primo ℓ, sea $\overline{v}_\ell$ la extensión de v_ℓ a $\overline{\mathbb{Q}}_\ell$. Dada una extensión finita de Galois $K/\mathbb{Q}$, fijemos una $\mathbb{Q}$-inclusión[1] $\iota_\ell\colon K \hookrightarrow \overline{\mathbb{Q}}_\ell$. Entonces, ι_ℓ induce una valoración en K, dada por

$$w_K(x) = \overline{v}_\ell \circ \iota_\ell(x) \text{ para todo } x \in K^\times.$$

[1]Sea K un cuerpo, y consideremos dos extensiones algebraicas F/K y F'/K. Una *K-inclusión* es una inclusión de cuerpos $\iota\colon F \hookrightarrow F'$ tal que $\iota(x) = x$ para todo $x \in K$.

La valoración w_K extiende v_ℓ a K, pues $\overline{v}_\ell$ es compatible en extensiones finitas de $\mathbb{Q}$ por la observación A.3, y es invariante por conjugación por el lema A.2. En particular, w_K es discreta, luego w_K es equivalente a la valoración $\mathfrak{l}$-ádica para un único ideal primo $\mathfrak{l} \subset \mathcal{O}_K$ tal que $\mathfrak{l} \mid \ell$, por el teorema de Ostrowski. De hecho, $\mathfrak{l} = \iota_\ell^{-1}(\overline{\mathfrak{M}}_\ell)$, y $\mathfrak{l}$ se llama *ideal primo inducido por* ι_ℓ.

Sea $K_\mathfrak{l}$ la completación de K respecto del valor absoluto $\mathfrak{l}$-ádico. Entonces, la inclusión $\mathbb{Q} \hookrightarrow K$ induce una inclusión $\mathbb{Q}_\ell \hookrightarrow K_\mathfrak{l}$. En efecto, si $\{x_n\}_{n\in\mathbb{N}} \subset \mathbb{Q}$ es una sucesión de Cauchy respecto de $|\cdot|_\ell$, también lo es respecto de $|\cdot|_\mathfrak{l}$, por ser valores absolutos equivalentes en $\mathbb{Q}$. Por tanto, $\mathbb{Q}_\ell \subset K_\mathfrak{l}$.

Dado que $K \subset K_\mathfrak{l} \subset \overline{\mathbb{Q}}_\ell$, podemos considerar el compositum $K\mathbb{Q}_\ell$ dentro de $\overline{\mathbb{Q}}_\ell$, y se verifica que $K_\mathfrak{l} = K\mathbb{Q}_\ell$. En efecto, $K\mathbb{Q}_\ell \subset K_\mathfrak{l}$ por definición de compositum. Recíprocamente, como $K\mathbb{Q}_\ell/\mathbb{Q}_\ell$ es una extensión finita, entonces $K\mathbb{Q}_\ell$ es un cuerpo completo por el teorema A.3 y contiene a K, por lo que debe ser su completación. Es decir, $K_\mathfrak{l} = K\mathbb{Q}_\ell$, y la extensión $K_\mathfrak{l}/\mathbb{Q}_\ell$ es de Galois por la proposición 1.3. Así, ι_ℓ induce un diagrama conmutativo

$$\begin{array}{ccc} K & \xhookrightarrow{\iota_\ell} & K_\mathfrak{l} \\ \uparrow & & \uparrow \\ \mathbb{Q} & \hookrightarrow & \mathbb{Q}_\ell \end{array}$$

que induce un homomorfismo inyectivo y continuo $\iota_\ell^*\colon \mathrm{Gal}(K_\mathfrak{l}/\mathbb{Q}_\ell) \to \mathrm{Gal}(K/\mathbb{Q})$, dado por

$$\sigma \mapsto \iota_\ell^{-1} \circ \sigma \circ \iota_\ell = \sigma|_K.$$

La composición con ι_ℓ^{-1} tiene sentido: $K/\mathbb{Q}$ es de Galois, luego $\iota_\ell(K)/\iota_\ell(\mathbb{Q})$ también, y por tanto, $\sigma(\iota_\ell(K)) \subset \iota_\ell(K)$ para todo $\sigma \in \mathrm{Gal}(K_\mathfrak{l}/\mathbb{Q}_\ell)$.

Proposición 2.3. Sea $K/\mathbb{Q}$ una extensión finita de Galois. Para todo primo ℓ, fijemos una $\mathbb{Q}$-inclusión $\iota_\ell\colon K \hookrightarrow \overline{\mathbb{Q}}_\ell$, y denotemos $\mathfrak{l} \subset \mathcal{O}_K$ al ideal primo inducido por ι_ℓ. Entonces, el homomorfismo ι_ℓ^* induce isomorfismos de grupos topológicos

$$\mathrm{Gal}(K_\mathfrak{l}/\mathbb{Q}_\ell) \cong D(\mathfrak{l}/\ell) \ \text{ e } \ I(K_\mathfrak{l}/\mathbb{Q}_\ell) \cong I(\mathfrak{l}/\ell).$$

Demostración. Sea $\sigma \in D(\mathfrak{l}/\ell)$, es decir, $\sigma(\mathfrak{l}) = \mathfrak{l}$. Entonces, σ preserva la valoración $\mathfrak{l}$-ádica y se puede extender a un automorfismo $\overline{\sigma} \in \mathrm{Gal}(K_\mathfrak{l}/\mathbb{Q}_\ell)$ definiéndolo como

$$\overline{\sigma}\left(\lim_{n\to\infty} x_n\right) = \lim_{n\to\infty} \sigma x_n,$$

para toda sucesión de Cauchy $\{x_n\}_{n\in\mathbb{N}}$ respecto del valor absoluto $\mathfrak{l}$-ádico. Dado que $\iota_\ell^*(\overline{\sigma}) = \sigma|_K = \sigma$, entonces $D(\mathfrak{l}/\ell) \subset \iota_\ell^*\left(\mathrm{Gal}(K_\mathfrak{l}/\mathbb{Q}_\ell)\right)$.

Recíprocamente, sea $\sigma \in \mathrm{Gal}(K_\mathfrak{l}/\mathbb{Q}_\ell)$. Entonces, por el lema A.2,

$$x \in \mathfrak{l} \iff v_\mathfrak{l}(x) = v_\mathfrak{l}(\sigma x) \geq 1 \iff \sigma x \in \mathfrak{l},$$

luego, $\sigma(\mathfrak{l}) = \mathfrak{l}$. Por tanto, $\iota_\ell^*\left(\mathrm{Gal}(K_\mathfrak{l}/\mathbb{Q}_\ell)\right) \subset D(\mathfrak{l}/\ell)$, concluyendo el primer isomorfismo.

Por otro lado, sea $\pi_{\mathfrak{l}/\ell}\colon D(\mathfrak{l}/\ell) \to \mathrm{Gal}(k_{\mathfrak{l}}/\mathbb{F}_\ell)$ el homomorfismo reducción. La composición $\pi_{\mathfrak{l}/\ell} \circ \iota_\ell^*$ coincide con el homomorfismo reducción $\pi_{K_{\mathfrak{l}}/\mathbb{Q}_\ell}\colon \mathrm{Gal}(K_{\mathfrak{l}}/\mathbb{Q}_\ell) \to \mathrm{Gal}(k_{\mathfrak{l}}/\mathbb{F}_\ell)$. Por tanto,

$$I(K_{\mathfrak{l}}/\mathbb{Q}_\ell) = \ker \pi_{K_{\mathfrak{l}}/\mathbb{Q}_\ell} = \ker(\pi_{\mathfrak{l}/\ell} \circ \iota_\ell^*) = \iota_\ell^{*-1}(\ker \pi_{\mathfrak{l}/\ell}) = \iota_\ell^{*-1}\left(I(\mathfrak{l}/\ell)\right),$$

concluyendo el resultado. □

Para el resto del capítulo, fijemos una $\mathbb{Q}$-inclusión $\iota_\ell\colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ para cada primo ℓ, y denotemos $\mathfrak{L} \subset \overline{\mathbb{Z}}$ al ideal primo inducido por ι_ℓ. Entonces, para toda extensión finita de Galois $K/\mathbb{Q}$, el homomorfismo ι_ℓ^* induce un diagrama conmutativo

$$\begin{array}{ccc} G_{\mathbb{Q}_\ell} & \xhookrightarrow{\iota_\ell^*} & G_{\mathbb{Q}} \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K_{\mathfrak{L}_K}/\mathbb{Q}_\ell) & \xhookrightarrow{\iota_\ell^*} & \mathrm{Gal}(K/\mathbb{Q}), \end{array}$$

siendo $\mathfrak{L}_K = \mathfrak{L} \cap \mathcal{O}_K$, que es un ideal primo de $\mathcal{O}_K$ tal que $\mathfrak{L}_K \mid \ell$.

Corolario 2.2. Para todo primo ℓ, fijemos una $\mathbb{Q}$-inclusión $\iota_\ell : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$, y denotemos $\mathfrak{L} \subset \overline{\mathbb{Z}}$ al ideal primo inducido por ι_ℓ. Entonces, el homomorfismo ι_ℓ^* induce isomorfismos de grupos topológicos

$$G_{\mathbb{Q}_\ell} \cong D(\mathfrak{L}/\ell) \text{ e } I_\ell \cong I(\mathfrak{L}/\ell).$$

Demostración. Para toda extensión finita de Galois $K/\mathbb{Q}$, denotemos $\mathfrak{L}_K = \mathfrak{L} \cap \mathcal{O}_K$. La restricción de ι_ℓ^* al grupo de Galois de cada tal extensión $K/\mathbb{Q}$ induce isomorfismos de grupos topológicos

$$\begin{aligned} D(\mathfrak{L}/\ell) &= \varprojlim D(\mathfrak{L}_K/\ell) \cong \varprojlim \mathrm{Gal}(K_{\mathfrak{L}_K}/\mathbb{Q}_\ell), \text{ e} \\ I(\mathfrak{L}/\ell) &= \varprojlim I(\mathfrak{L}_K/\ell) \cong \varprojlim I(K_{\mathfrak{L}_K}/\mathbb{Q}_\ell). \end{aligned}$$

Por el teorema 1.1, $D(\mathfrak{L}/\ell) \cong G_{\mathbb{Q}_\ell}$, y por la proposición 1.15, $I(\mathfrak{L}/\ell) \cong I_\ell$, como queríamos. □

Definición 2.9. Sea $\rho\colon G_{\mathbb{Q}} \to \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ una representación de Galois.

- La representación de Galois $\rho_\ell\colon G_{\mathbb{Q}_\ell} \to \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ dada por $\rho_\ell = \rho \circ \iota_\ell^*$ se llama *representación local de ρ en ℓ.*
- Si $\rho_\ell(I_\ell) = \{\mathrm{id}\}$, se dice que ρ_ℓ es *no ramificada* y que ρ es *no ramificada en ℓ.*
- Si $\rho_\ell(I_\ell^{\mathrm{wild}}) = \{\mathrm{id}\}$, se dice que ρ_ℓ es *moderada* y que ρ es *moderada en ℓ* .

Proposición 2.4. Sea $\rho\colon G_{\mathbb{Q}} \to \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ una representación de Galois, y denotemos K al subcuerpo de $\overline{\mathbb{Q}}$ fijo por $\ker \rho$. Entonces, ρ es no ramificada en un primo ℓ si y sólo si ℓ es no ramificado en $K/\mathbb{Q}$.

Demostración. Sea ℓ un primo. Por el primer teorema de isomorfía de Noether,

$$\rho_\ell(I_\ell) \cong I_\ell/\ker \rho_\ell \cap I_\ell,$$

luego ρ es no ramificada en ℓ si y sólo si $I_\ell \subset \ker \rho_\ell$. Por la proposición 2.2, sabemos que $K/\mathbb{Q}$ es una extensión finita de Galois, y que $\ker \rho = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Además,

$$\ker \rho_\ell = \ker(\rho \circ \iota_\ell^*) = \iota_\ell^{*-1}(\ker \rho) = \iota_\ell^{*-1}\left(\mathrm{Gal}(\overline{\mathbb{Q}}/K)\right) = \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/K_\mathfrak{l}),$$

siendo $\mathfrak{l} = \mathfrak{L} \cap \mathcal{O}_K$. Por tanto, $I_\ell \subset \ker \rho_\ell$ si y sólo si $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell^{\mathrm{unr}}) \subset \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/K_\mathfrak{l})$. Por el teorema de correspondencia de Galois, esto equivale a que $K_\mathfrak{l} \subset \mathbb{Q}_\ell^{\mathrm{unr}}$, que a su vez equivale a que

$$I(K_\mathfrak{l}/\mathbb{Q}_\ell) = \mathrm{Gal}(K_\mathfrak{l}/K_\mathfrak{l} \cap \mathbb{Q}_\ell^{\mathrm{unr}}) = \{\mathrm{id}\}.$$

Por la proposición 2.3, $I(K_\mathfrak{l}/\mathbb{Q}_\ell) = \{\mathrm{id}\}$ si y sólo si $I(\mathfrak{L}/\ell) = \{\mathrm{id}\}$. Por el teorema 1.3, esto equivale a que ℓ sea no ramificado en $K/\mathbb{Q}$, como queríamos. □

Corolario 2.3. Toda representación de Galois $\rho\colon G_\mathbb{Q} \to \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ es no ramificada salvo en una cantidad finita de primos.

Lema 2.1. Si $\rho_p\colon G_{\mathbb{Q}_p} \to \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ es una representación de Galois, entonces $V^{I_p^{\mathrm{wild}}} \neq \{\mathbf{0}\}$.

Demostración. En primer lugar, $\rho_p(I_p^{\mathrm{wild}})$ es un grupo finito por la proposición 2.2 y de hecho es un p-grupo por la proposición 1.20.

La acción de I_p^{wild} en V nos permite expresar V como unión disjunta de las órbitas inducidas por dicha acción. El orden de cada órbita divide al orden de $\rho_p(I_p^{\mathrm{wild}})$, que es una potencia de p. Dado que V es un $\overline{\mathbb{F}}_p$-espacio vectorial finito, el cardinal de V también es una potencia de p. Ahora bien, la órbita de $\mathbf{0} \in V$ tiene orden 1, luego debe de haber al menos otras $p-1$ órbitas distintas de orden 1. Cada una de estas órbitas nos da un elemento no nulo de $V^{I_p^{\mathrm{wild}}}$, concluyendo que $V^{I_p^{\mathrm{wild}}} \neq \{\mathbf{0}\}$. □

Proposición 2.5. Si $\rho_p\colon G_{\mathbb{Q}_p} \to \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ es una representación de Galois semisimple, entonces ρ_p es moderada.

Demostración. Notemos que si el resultado se verifica para dos representaciones ρ_p y ρ_p' entonces se verifica para $\rho_p \oplus \rho_p'$, luego podemos asumir sin pérdida de generalidad que ρ_p es simple.

Dado que $I_p^{\mathrm{wild}} \lhd G_{\mathbb{Q}_p}$, se sigue de la proposición 2.1 que $V^{I_p^{\mathrm{wild}}}$ es un subespacio de V invariante por la acción de $G_{\mathbb{Q}_p}$. Como ρ_p es simple, o bien $V^{I_p^{\mathrm{wild}}} = \{\mathbf{0}\}$ o bien $V^{I_p^{\mathrm{wild}}} = V$, y por el lema anterior sólo puede ocurrir $V^{I_p^{\mathrm{wild}}} = V$. Concluimos que $\rho_p(I_p^{\mathrm{wild}}) = \{\mathrm{id}\}$, como queríamos. □

De esta proposición se sigue que todo carácter $G_\mathbb{Q} \to \overline{\mathbb{F}}_p^\times$ es moderado en p, pues todo carácter es irreducible.

Teorema 2.1. *Sean $\rho_1, \rho_2\colon G_\mathbb{Q} \to \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ dos representaciones de Galois, y S un conjunto finito de primos enteros. Si $\rho_1(\mathrm{Frob}_\ell) = \rho_2(\mathrm{Frob}_\ell)$ para todo primo $\ell \notin S$, entonces $\rho_1 = \rho_2$.*

Demostración. Por la proposición 1.7, las representaciones ρ_1 y ρ_2 coinciden en un conjunto denso. Como ρ_1 y ρ_2 son continuas, entonces son iguales. □

Teorema 2.2 (Brauer-Nesbitt). *Sean $\rho_1, \rho_2 \colon G_{\mathbb{Q}} \to \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ dos representaciones de Galois bidimensionales y semisimples, y S un conjunto finito de primos enteros. Si*

$$\operatorname{tr}\rho_1(\mathrm{Frob}_\ell) = \operatorname{tr}\rho_2(\mathrm{Frob}_\ell) \;\; y \;\; \det\rho_1(\mathrm{Frob}_\ell) = \det\rho_2(\mathrm{Frob}_\ell)$$

para todo primo $\ell \notin S$, entonces $\rho_1 \cong \rho_2$.

Demostración. Ver página 215, teorema 30.16 de [CR66]. □

Definición 2.10. Sea $\rho \colon G_{\mathbb{Q}} \to \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ una representación de Galois tal que $\dim\rho \leq 2$. Después de fijar una $\mathbb{Q}$-inclusión $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, se dice que ρ es *impar* si $\det\rho(c) = -1$, siendo $c \in G_{\mathbb{Q}}$ la conjugación compleja.

2.4. Representaciones de Galois de dimensión 1

Comenzamos esta sección clasificando las representaciones de Galois de la forma

$$\rho \colon G_{\mathbb{Q}} \to \mathrm{GL}_1(\overline{\mathbb{F}}_p) \cong \overline{\mathbb{F}}_p^{\times}.$$

Vamos a probar que se corresponden con unos caracteres particulares, que definimos a continuación.

Definición 2.11. Sea N un entero positivo. Un *carácter de Dirichlet módulo N* es un homomorfismo de grupos multiplicativos

$$\varepsilon \colon (\mathbb{Z}/N\mathbb{Z})^{\times} \to \mathbb{C}^{\times}.$$

El entero N se llama *módulo de ε*. Si el módulo de ε está especificado, se dice que ε es un *carácter de Dirichlet*.

Observación. Sea $\varepsilon \colon (\mathbb{Z}/N\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$ un carácter de Dirichlet. Dado que ε es un homomorfismo de grupos, entonces ε es completamente multiplicativo. Es decir, $\varepsilon(mn) = \varepsilon(m)\varepsilon(n)$ para todo $m, n \in (\mathbb{Z}/N\mathbb{Z})^{\times}$.

Sea N un entero positivo. Para todo entero positivo d tal que $d \mid N$, podemos considerar la proyección natural $\pi_{N,d} \colon (\mathbb{Z}/N\mathbb{Z})^{\times} \to (\mathbb{Z}/d\mathbb{Z})^{\times}$. Así, si ε_d es un carácter de Dirichlet módulo d, podemos obtener un carácter de Dirichlet ε_N módulo N, dado por la composición $\varepsilon_N = \varepsilon_d \circ \pi_{N,d}$.

Definición 2.12. Sea ε un carácter de Dirichlet módulo N. Se define el *conductor de ε* como el menor entero positivo d que divide a N tal que existe un carácter de Dirichlet módulo d verificando $\varepsilon = \varepsilon_d \circ \pi_{N,d}$. Si el conductor de ε coincide con N, se dice que ε es un carácter de Dirichlet *primitivo*.

Observación. Sea $\varepsilon \colon (\mathbb{Z}/N\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$ un carácter de Dirichlet.

- Podemos extender ε a una aplicación $\mathbb{Z} \to \mathbb{C}$ definiéndola como

$$n \mapsto \begin{cases} \varepsilon(n \bmod N) & \text{si } \gcd(n, N) = 1, \\ 0 & \text{si no.} \end{cases}$$

A esta aplicación también la denotamos ε, abusando de la notación. Observemos que la aplicación extendida ya no es un homomorfismo de grupos, pero sigue siendo completamente multiplicativa.

- Sea φ la función de Euler. Para todo $n \in (\mathbb{Z}/N\mathbb{Z})^\times$, se verifica que $\varepsilon(n)$ es una raíz $\varphi(N)$-ésima de la unidad. En efecto, por ser ε una función completamente multiplicativa y por el teorema de Euler-Fermat,

$$\varepsilon(n)^{\varphi(N)} = \varepsilon(n^{\varphi(N)}) = \varepsilon(1) = 1.$$

- En general, dado un anillo R, se puede definir un *carácter de Dirichlet módulo* N como un homomorfismo de grupos de multiplicativos $(\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$, y verifica las propiedades mencionadas anteriormente. El caso $R = \overline{\mathbb{F}}_p$ será de importancia en el siguiente teorema.

Teorema 2.3. *Existe una correspondencia biunívoca*

$$\left\{ \begin{array}{c} \textit{caracteres primitivos de Dirichlet} \\ \varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{representaciones de Galois} \\ \rho\colon G_{\mathbb{Q}} \to \overline{\mathbb{F}}_p^\times \end{array} \right\}.$$

Además, N es el menor entero tal que ρ factoriza por la extensión $\mathbb{Q}(\zeta_N)/\mathbb{Q}$.

Demostración. Sea $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$ un carácter de Dirichlet primitivo. No es difícil comprobar que el homomorfismo

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) &\to (\mathbb{Z}/N\mathbb{Z})^\times \\ (\zeta_N \mapsto \zeta_N^n) &\mapsto n \bmod N \end{aligned} \tag{2.1}$$

es un isomorfismo de grupos. Si denotamos π_N a la restricción de $G_{\mathbb{Q}}$ a $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, obtenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} G_{\mathbb{Q}} & & \\ \downarrow{\scriptstyle \pi_N} & & \\ \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) & \xrightarrow{\cong} & (\mathbb{Z}/N\mathbb{Z})^\times \\ & {\scriptstyle \rho_{\varepsilon,N}} \searrow \quad \swarrow {\scriptstyle \varepsilon} & \\ & \overline{\mathbb{F}}_p^\times & \end{array}$$

De este modo, obtenemos un homomorfismo $\rho_\varepsilon = \rho_{\varepsilon,N} \circ \pi_N\colon G_{\mathbb{Q}} \to \overline{\mathbb{F}}^\times$. Veamos que ρ_ε es continua para concluir que es una representación de Galois. Para ello, basta ver que $\rho_\varepsilon^{-1}(\{\mathrm{id}\})$ es abierto. Esto es cierto, pues $\ker \rho_\varepsilon = \rho_\varepsilon^{-1}(\{\mathrm{id}\}) \cong \mathrm{Gal}(K/\mathbb{Q})$, siendo $K/\mathbb{Q}$ una extensión finita de Galois tal que $K \subset \mathbb{Q}(\zeta_N)$.

Recíprocamente, sea $\rho\colon G_{\mathbb{Q}} \to \overline{\mathbb{F}}_p^\times$ una representación de Galois de dimensión 1. Por el corolario 2.1, existe una extensión $K/\mathbb{Q}$ finita de Galois tal que $\rho(G_{\mathbb{Q}}) \cong \mathrm{Gal}(K/\mathbb{Q})$ y $\mathrm{Gal}(K/\mathbb{Q})$ es un grupo abeliano. Ahora bien, el teorema de Kronecker-Weber afirma que

toda extensión abeliana de $\mathbb{Q}$ está contenida en $\mathbb{Q}(\zeta_N)$ para algún entero N. Así, sea N un entero tal que $K \subset \mathbb{Q}(\zeta_N)$. Entonces $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_N)) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/K) = \ker \rho$, por lo que ρ factoriza por la extensión $\mathbb{Q}(\zeta_N)/\mathbb{Q}$. Por tanto, el diagrama anterior muestra que

$$\rho = \rho_{\varepsilon_\rho, N} \circ \pi_N$$

para algún carácter de Dirichlet ε_ρ de módulo N. Para que ε_ρ sea primitivo, basta tomar N como el menor entero que divide a N tal que ρ factoriza por $\mathbb{Q}(\zeta_N)/\mathbb{Q}$. □

El carácter ciclotómico

Sean p un primo entero y ζ_p una raíz p-ésima primitiva de la unidad en $\overline{\mathbb{Q}}$. Sabemos que las raíces del polinomio $x^p - 1$ son las raíces p-ésimas de la unidad, y forman un grupo cíclico $\boldsymbol{\mu}_p$ de orden p, generado por ζ_p. El grupo absoluto $G_\mathbb{Q}$ actúa en $\boldsymbol{\mu}_p$ permutando sus elementos. Teniendo en cuenta que $\mathrm{Aut}(\boldsymbol{\mu}_p) \cong \mathbb{F}_p^\times$, esta acción da lugar a un carácter $\chi_p \colon G_\mathbb{Q} \to \mathbb{F}_p^\times$ definido por

$$\sigma(\zeta_p) = \zeta_p^{\chi_p(\sigma)}, \text{ con } \sigma \in G_\mathbb{Q}.$$

Definición 2.13. El carácter $\chi_p \colon G_\mathbb{Q} \to \mathbb{F}_p^\times$ definido anteriormente se llama *carácter ciclotómico módulo* p. La representación local de χ_p en cualquier primo ℓ también se llama *carácter ciclotómico módulo* p, y también se denota χ_p.

Observación. El carácter χ_p no depende de la raíz p-ésima de la unidad elegida. En efecto, sea $\zeta_p' \in \boldsymbol{\mu}_p$ una raíz p-ésima primitiva de la unidad distinta de ζ_p. Entonces, existe un entero r coprimo con p tal que $\zeta_p' = \zeta_p^r$. Sea $\sigma \in G_\mathbb{Q}$ tal que $\sigma(\zeta_p) = \zeta_p^{\chi_p(\sigma)}$. Concluimos que

$$\sigma(\zeta_p') = \sigma(\zeta_p^r) = \sigma(\zeta_p)^r = \left(\zeta_p^{\chi_p(\sigma)}\right)^r = \left(\zeta_p^r\right)^{\chi_p(\sigma)} = \left(\zeta_p'\right)^{\chi_p(\sigma)},$$

como queríamos.

Observación. Si ℓ es un primo distinto de p, entonces Frob_ℓ actúa en ζ_p elevando a ℓ. Es decir, $\chi_p(\mathrm{Frob}_\ell) = \ell$, para todo primo ℓ distinto de p.

Caracteres fundamentales

Fijemos un entero $n \geq 1$ y una $\mathbb{F}_p$-inclusión $\tau \colon \mathbb{F}_{p^n} \hookrightarrow \overline{\mathbb{F}}_p$. Sea σ_p el automorfismo de Frobenius $x \mapsto x^p$, que es generador topológico de $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Podemos obtener $n-1$ inclusiones más, dadas por

$$\begin{aligned} \tau_j \colon \mathbb{F}_{p^n} &\hookrightarrow \overline{\mathbb{F}}_p \\ x &\mapsto (\sigma_p^j \circ \iota)(x) = \iota(x)^{p^j}, \text{ para todo } j = 1, \ldots, n-1. \end{aligned}$$

Por otro lado, consideramos el siguiente homomorfismo

$$\psi \colon I_p^{\mathrm{tame}} \overset{t}{\cong} \varprojlim_n \mathbb{F}_{p^n}^\times \overset{\pi_n}{\twoheadrightarrow} \mathbb{F}_{p^n}^\times \overset{\tau_j}{\hookrightarrow} \overline{\mathbb{F}}_p^\times,$$

siendo τ_j alguna de las n inclusiones $\tau_j\colon \mathbb{F}_{p^n} \hookrightarrow \overline{\mathbb{F}}_p$ con $j = 1, \dots, n$, π_n la proyección canónica del límite inverso en $\mathbb{F}_{p^n}^\times$, y t el isomorfismo de la proposición 1.17.

Definición 2.14. Sea n un entero positivo. Si $\psi\colon I_p^{\text{tame}} \to \overline{\mathbb{F}}_p^\times$ es un carácter definido por la composición $\psi = \tau_j \circ \pi_n \circ t$ para algún $j = 1, \dots, n$, se dice que ψ es un *carácter fundamental de nivel* n.

Definición 2.15. Sea $\phi\colon I_p^{\text{tame}} \to \overline{\mathbb{F}}_p^\times$ un carácter. Se dice que ϕ es *de nivel* n si n es el menor entero positivo tal que $\phi(I_p^{\text{tame}}) \subseteq \mathbb{F}_{p^n}^\times$.

Observación. Sea ψ un carácter fundamental de nivel n.

- Por definición, $\psi = \tau_j \circ \pi_n \circ t$ para algún $j = 1, \dots, n$. Observemos que $\psi(I_p^{\text{tame}}) = \mathbb{F}_{p^n}^\times$. En efecto, t es un isomorfismo, y en particular, es sobreyectivo. Como π_n es la proyección del límite inverso en $\mathbb{F}_{p^n}^\times$, entonces π_n es sobreyectivo, y por tanto, $\pi_n \circ t$ también. La imagen de $\pi_n \circ t$ tiene cardinal $p^n - 1$, luego la inclusión τ_j la lleva en un subgrupo de cardinal $p^n - 1$, que es justamente el subgrupo multiplicativo $\mathbb{F}_{p^n}^\times$ de $\overline{\mathbb{F}}_p^\times$.
- Dado que cada inclusión τ_j se corresponde con la j-ésima potencia del automorfismo de Frobenius $x \mapsto x^p$ para $j = 1, \dots, n$, los n caracteres fundamentales de nivel n son
$$\psi, \psi^p, \psi^{p^2}, \dots, \psi^{p^{n-1}}.$$
- Sea $\phi\colon I_p^{\text{tame}} \to \overline{\mathbb{F}}_p^\times$ un carácter de nivel, a lo más, n. Entonces, podemos expresar ϕ como
$$\phi = \alpha \circ \pi_n \circ t,$$
para algún homomorfismo de grupos $\alpha\colon \mathbb{F}_{p^n}^\times \to \overline{\mathbb{F}}_p^\times$. Es decir, ϕ y ψ se diferencian en que α es un homomorfismo de grupos que no necesariamente proviene de un homomorfismo de cuerpos. Dado que $\mathbb{F}_{p^n}^\times$ es cíclico, dicho homomorfismo está determinado por la imagen de un generador de $\mathbb{F}_{p^n}^\times$, que tiene orden $p^n - 1$. Esto nos permite expresar
$$\phi = \psi^a \text{ con } a \in \mathbb{Z}/(p^n - 1)\mathbb{Z}.$$
Tomando a como un entero tal que $0 \leq a < p^n - 1$, la expresión anterior es única.

Observación 2.1. Consideremos la restricción a I_p del carácter ciclotómico módulo p, es decir,
$$\chi_p|_{I_p}\colon I_p \to \mathbb{F}_p^\times.$$

Este carácter es moderado por la proposición 2.5, es decir, $\chi_p(I_p^{\text{wild}}) = \{\text{id}\}$. Por tanto, χ_p induce un carácter $\chi\colon I_p^{\text{tame}} \to \mathbb{F}_p^\times$ de modo que el siguiente diagrama

$$\begin{array}{ccc} I_p & \xrightarrow{\chi_p|_{I_p}} & \mathbb{F}_p^\times \\ & \searrow \quad \nearrow_{\chi} & \\ & I_p^{\text{tame}} & \end{array}$$

es conmutativo, y por tanto, $\chi(I_p^{\text{tame}}) = \chi_p(I_p) = \mathbb{F}_p^\times$. Se puede comprobar[2] que χ es el único carácter fundamental de nivel 1.

[2]Ver ejercicio 16 del capítulo 4 de [RS99]. Se incluye la solución al final del capítulo.

Proposición 2.6. Sea n un entero positivo. Sean $\psi_1, \ldots, \psi_n$ los n caracteres fundamentales de nivel n, y χ el único carácter fundamental de nivel 1. Entonces,

$$\prod_{j=1}^{n} \psi_j = \chi.$$

Demostración. Por definición de carácter fundamental de nivel n, sabemos que

$$\psi_j = \tau_j \circ \pi_n \circ t \text{ para todo } j = 1, \ldots, n,$$

siendo $\tau_1, \ldots, \tau_n$ las $\mathbb{F}_p$-inclusiones de cuerpos $\mathbb{F}_{p^n} \hookrightarrow \overline{\mathbb{F}}_p$, π_n la proyección canónica del límite inverso en $\mathbb{F}_{p^n}^{\times}$, y t el isomorfismo de la proposición 1.17. Análogamente,

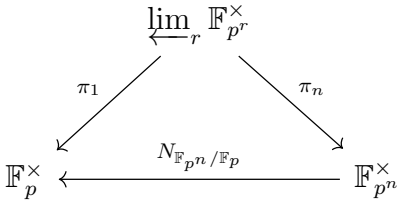
$$\chi = i \circ \pi_1 \circ t, \tag{2.2}$$

siendo i la única $\mathbb{F}_p$-inclusión de cuerpos $i\colon \mathbb{F}_p \hookrightarrow \overline{\mathbb{F}}_p$.

Consideremos la aplicación $N\colon \mathbb{F}_{p^n}^{\times} \to \overline{\mathbb{F}}_p^{\times}$ dada por $N(x) = \prod_{j=1}^{n} \tau_j(x)$, y observemos que $N = i \circ N_{\mathbb{F}_{p^n}/\mathbb{F}_p}$. Entonces, para todo $\sigma \in I_p^{\text{tame}}$,

$$\prod_{j=1}^{n} \psi_j(\sigma) = \prod_{j=1}^{n} \tau_j(\pi_n(t(\sigma))) = N(\pi_n(t(\sigma))). \tag{2.3}$$

Por tanto, basta comprobar que $N \circ \pi_n = i \circ \pi_1$. Sabemos que $\varprojlim_r \mathbb{F}_{p^r}^{\times}$ es el límite inverso respecto del sistema inverso cuyos morfismos son las aplicaciones $N_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}$ para todo par de enteros positivos (n, m) tales que $m \mid n$. Tomando $m = 1$, el diagrama



es conmutativo, luego $\pi_1 = N_{\mathbb{F}_{p^n}/\mathbb{F}_p} \circ \pi_n$, y por tanto, $i \circ \pi_1 = i \circ N_{\mathbb{F}_{p^n}/\mathbb{F}_p} \circ \pi_n = N \circ \pi_n$. Se sigue de (2.2) que $\chi = i \circ \pi_1 \circ t = N \circ \pi_n \circ t$, y se concluye el resultado por (2.3). □

3 Curvas elípticas

"It is possible to write endlessly about elliptic curves. (This is not a threat.)"

— Serge Lang.

Este capítulo consiste en una pequeña introducción a la teoría de curvas elípticas, que son variedades algebraicas estrechamente relacionadas con las formas modulares. En este trabajo, tienen relevancia a la hora de demostrar el último teorema de Fermat. La principal referencia utilizada para escribir este capítulo es [Sil09].

3.1. Ecuación de Weierstrass

Definición 3.1. Sea K un cuerpo. Una *curva elíptica sobre* K es un par (E, O_E) tal que:

- E es una curva[1] no singular de género 1.
- $O_E \in E(K)$, donde $E(K)$ denota el conjunto de puntos K-racionales de E.

Gracias al teorema de Riemann-Roch (ver teorema II.5.4 de [Sil09]), toda curva elíptica (E, O_E) sobre K puede expresarse de manera que E esté definida por una ecuación homogénea de la forma

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{3.1}$$

con $a_1, \ldots, a_6 \in K$, y O_E se corresponda con el punto del infinito $[0 : 1 : 0]$. Para ver una demostración, se puede consultar la proposición III.3.1 de [Sil09]. Observemos que $[0 : 1 : 0]$ es el único punto de E que está en el hiperplano del infinito $\{Z = 0\}$, por lo que es usual trabajar con la deshomogenización de (3.1) respecto de Z:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.2}$$

También es habitual denotar E/K a una curva elíptica sobre un cuerpo K, quedando implícito el punto O_E.

Definición 3.2. Tanto la ecuación (3.1) como (3.2) se llaman *ecuación de Weierstrass*. Si una curva algebraica C está definida por una ecuación de Weierstrass, se dice que dicha ecuación es un *modelo de Weierstrass para* C.

Observación 3.1. Sea E/K una curva elíptica. Entonces, E admite un modelo de Weierstrass, pero no es único. Si E está definida por (3.2), podemos obtener otro modelo de Weierstrass para E mediante el cambio de variables

$$(x, y) \mapsto (u^2x + r,\ u^3y + u^2sx + t),$$

con $r, s, t, u \in \overline{K}$ y $u \neq 0$. Para ver una demostración de este hecho, se puede consultar la proposición III.3.1 de [Sil09].

[1] Es decir, una variedad algebraica proyectiva de dimensión 1.

Veamos cómo simplificar la ecuación (3.2). Si $\mathrm{char}(K) \neq 2$, el cambio de variable

$$y \mapsto \frac{1}{2}(y - a_1x - a_3).$$

transforma la ecuación (3.2) en

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{3.3}$$

donde

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

También definimos las siguientes cantidades

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

Además, si $\mathrm{char}(K) \notin \{2, 3\}$, podemos simplificar (3.3) con el cambio de variables

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right).$$

De esta manera, podemos expresar (3.3) como

$$y^2 = x^3 + Ax + B, \tag{3.4}$$

donde $A = -27c_4$ y $B = -54c_6$.

Definición 3.3. Sea C una curva algebraica. Si $\mathrm{char}(K) \notin \{2, 3\}$ y si C está definida por una ecuación de la forma (3.4), se dice que C está en *forma corta de Weierstrass*.

Hay dos parámetros de interés asociados a una ecuación de Weierstrass, que definimos a continuación.

Definición 3.4. Sea C una curva algebraica tal que (3.2) es un modelo de Weierstrass para C. Se definen:

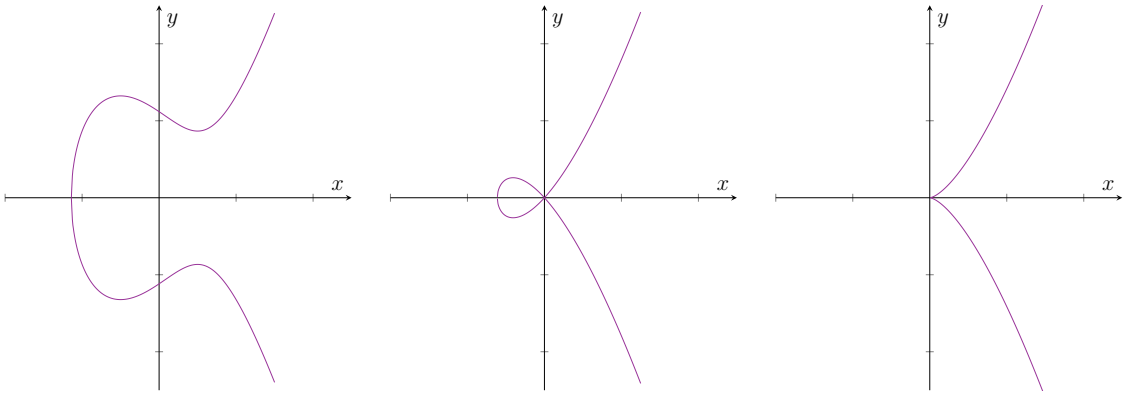
- El *discriminante* de C como $\Delta_C = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$.
- El *j-invariante* de C como $j_C = \dfrac{c_4^3}{\Delta}$.

Proposición 3.1. Sea C una curva algebraica tal que (3.2) es un modelo de Weierstrass para C. Entonces:

1. C es no singular si y sólo si $\Delta_C \neq 0$.
2. C tiene un nodo si y sólo si $\Delta_C = 0$ y $c_4 \neq 0$.
3. C tiene una cúspide si y sólo si $\Delta_C = c_4 = 0$.

En los dos últimos casos, el nodo o la cúspide es el único punto singular de C.

Demostración. Ver proposición III.1.4 de [Sil09]. □



(a) Cúbica no singular (b) Cúbica con un nodo (c) Cúbica con una cúspide

Figura 3.1: Tipos de cúbicas según sus singularidades

3.2. Puntos racionales y estructura de grupo

Sea E/K una curva elíptica sobre un cuerpo K. De ahora en adelante, denotaremos

$$E(K) = \{(x, y) \in E : x, y \in K\} \cup \{O_E\}$$

al conjunto de puntos K-racionales de E. Una de las propiedades más importantes de las curvas elípticas es que se puede definir una operación en el conjunto de sus puntos K-racionales que lo dotan de estructura de grupo abeliano. Vamos a describir geométricamente esta operación, que denotaremos $\oplus$. Para ello, utilizaremos el siguiente teorema.

Teorema 3.1 (Bézout)**.** *Sean C y C' dos curvas algebraicas proyectivas distintas de grados d y d', respectivamente. Si C y C' no tienen componentes irreducibles en común, entonces C y C' se cortan en dd' puntos contados con multiplicidad.*

Demostración. Ver corolario I.7.8 de [Har13]. □

Sean $P, Q \in E(K)$ dos puntos K-racionales de E. Sea $\mathscr{L} = \overline{PQ}$ la recta que pasa por P y Q (si $P = Q$, definimos $\mathscr{L}$ como la recta tangente a E en P). Por el teorema de Bézout, existe otro punto $R \in E(K)$ tal que $E \cap \mathscr{L} = \{P, Q, R\}$, y consideramos la recta $\mathscr{L}' = \overline{RO_E}$. De nuevo, el teorema de Bezout asegura que existe un punto de E que corta a $\mathscr{L}'$. Dicho punto es el que definimos como $P \oplus Q$.

Proposición 3.2. Dada una curva elíptica E/K, se verifican las siguientes propiedades:

1. $P \oplus O_E = P$ para todo $P \in E(K)$.
2. $P \oplus Q = Q \oplus P$ para todo $P, Q \in E(K)$.
3. Para todo $P \in E(K)$, existe un punto $P' \in E(K)$ tal que $P \oplus P' = O_E$.
4. $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ para todo $P, Q, R \in E(K)$.

Demostración. Las 3 primeras propiedades son fáciles de verificar por la definición de $\oplus$. Para ver una demostración de la última propiedad, se puede consultar el capítulo 5 de [Ful08]. □

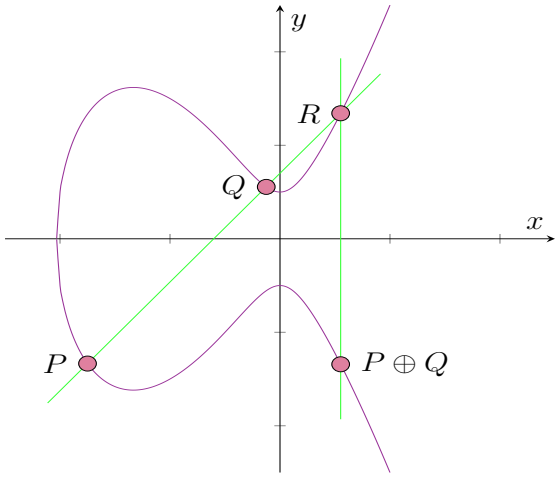


Figura 3.2: Suma de puntos racionales en una curva elíptica

Corolario 3.1. Dada una curva elíptica E/K, el grupo $E(K)$ con la operación $\oplus$ tiene estructura de grupo abeliano, siendo O_E el elemento identidad.

De ahora en adelante, dada una curva elíptica E/K y dados $P, Q \in E(K)$, utilizaremos la siguiente notación:

- $P + Q = P \oplus Q$.
- $-P$ denota al elemento inverso de P.
- $[m]P = P \underbrace{+ \cdots +}_{m \text{ veces}} P$, para todo entero $m \geq 1$.

3.3. Isogenias

Sea K un cuerpo de característica 0, y fijemos una clausura algebraica $\overline{K}$.

Definición 3.5. Sean E_1/K y E_2/K curvas elípticas. Una *isogenia entre* E_1 *y* E_2 es un morfismo de variedades algebraicas $\phi\colon E_1 \to E_2$ definido sobre $\overline{K}$ tal que $\phi(O_{E_1}) = O_{E_2}$. Se dice que E_1 y E_2 son *isógenas* si existe una isogenia $\phi\colon E_1 \to E_2$ tal que $\phi(E_1) \neq \{O_{E_2}\}$. Además, si ϕ está definida sobre K, se dice que E_1 y E_2 son K*-isógenas*.

El teorema II.2.3 de [Sil09] prueba que si $\phi\colon E_1 \to E_2$ es una isogenia, entonces sólo existen dos posibilidades: $\phi(E_1) = \{O_{E_2}\}$ o $\phi(E_1) = E_2$. Además, el teorema III.4.8 del mismo libro demuestra que las isogenias son homomorfismos de grupos.

Proposición 3.3. Sea E/K una curva elíptica. Dado un subgrupo finito $H \subset E(\overline{K})$, existe una única curva elíptica $E' = E/H$ y una única isogenia no constante $\phi\colon E \to E'$ tal que $\ker \phi = H$.

Demostración. Ver proposición III.4.12 de [Sil09]. □

3.4. Curvas elípticas sobre extensiones de $\mathbb{Q}_\ell$

A lo largo de esta sección, utilizaremos la siguiente notación:

- ℓ es un primo y $K/\mathbb{Q}_\ell$ es una extensión finita.
- v denota a la valoración normalizada asociada a la extensión de v_ℓ a K.
- $\mathcal{O}_v$, $\mathfrak{M}_v$ y k_v denotan el anillo de valoración, el ideal de valoración y el cuerpo de residuos de K.
- π es un uniformizante en K. Es decir, $v(\pi) = 1$ y $\mathfrak{M}_v = \pi\mathcal{O}_v$.

Modelo minimal local

Sea E/K una curva elíptica con modelo de Weierstrass

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

El cambio de variables $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ con $u \in K^\times$ produce un nuevo modelo de Weierstrass para E, y es posible elegir u de modo que $a_1, \ldots, a_6 \in \mathcal{O}_v$. Una vez hecho esto, el discriminante Δ_E verifica $v(\Delta_E) \geq 0$, y como v es discreta, es posible elegir un modelo de Weierstrass para E con coeficientes en $\mathcal{O}_v$ tal que $v(\Delta_E)$ sea mínimo.

Definición 3.6. Sea E/K una curva elíptica. Un modelo de Weierstrass para E se llama *modelo minimal para* E si tiene coeficientes en $\mathcal{O}_v$ y si $v(\Delta_E)$ es mínimo entre todos los modelos de Weierstrass para E con coeficientes en $\mathcal{O}_v$. El discriminante de un modelo minimal para E se llama *discriminante minimal de* E.

Observación. Sea E/K una curva elíptica con modelo de Weierstrass

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

y denotemos Δ al discriminante asociado a este modelo. Veamos cómo determinar si el modelo es minimal para E. Supongamos que $a_1, \ldots, a_6 \in \mathcal{O}_v$ y que el modelo no es minimal para E. Cualquier cambio de variables que proporcione otro modelo de Weierstrass para E es de la forma descrita en la observación 3.1. Por tanto, si denotamos Δ' al discriminante del nuevo modelo para E, se verifica que $\Delta' = u^{-12}\Delta$. Concluimos que

$$a_1, \ldots, a_6 \in \mathcal{O}_v \text{ y } v(\Delta) < 12 \implies \text{el modelo es minimal.}$$

De manera similar, $c_4' = u^{-4}c_4$ y $c_6' = u^{-6}c_6$, luego

$$a_1, \ldots, a_6 \in \mathcal{O}_v \text{ y } v(c_4) < 4 \implies \text{el modelo es minimal.}$$
$$a_1, \ldots, a_6 \in \mathcal{O}_v \text{ y } v(c_6) < 6 \implies \text{el modelo es minimal.}$$

Además, si $\ell \notin \{2, 3\}$, podemos dar un resultado recíproco: si el modelo es minimal, entonces $v(\Delta) < 12$ o $v(c_4) < 4$.

La proposición VII.1.3 de [Sil09] asegura que toda curva elíptica E/K admite un modelo minimal, y es único salvo cambio de variables

$$(x, y) \mapsto (u^2x + r,\ u^3y + u^2sx + t),$$

con $u \in \mathcal{O}_v^\times$ y $r, s, t \in \mathcal{O}_v$.

Reducción módulo π

Sea E/K una curva elíptica definida por un modelo minimal

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

y consideremos el homomorfismo reducción $\mathcal{O}_v \to \mathcal{O}_v/\pi\mathcal{O}_v$, denotado $x \mapsto \widetilde{x}$. Como el modelo es minimal, entonces $a_1, \ldots, a_6 \in \mathcal{O}_v$, podemos reducir estos coeficientes módulo π, de modo que obtenemos una curva algebraica $\widetilde{E}$ definida sobre $k_v = \mathcal{O}_v/\pi\mathcal{O}_v$ por el modelo

$$\widetilde{E} : y^2 + \widetilde{a_1}xy + \widetilde{a_3}y = x^3 + \widetilde{a_2}x^2 + \widetilde{a_4}x + \widetilde{a_6}.$$

La curva $\widetilde{E}/k_v$ se llama *reducción de E módulo π*. Ahora bien, aunque E es una curva no singular, $\widetilde{E}$ podría tener un punto singular. Por ello, damos la siguiente clasificación.

Definición 3.7. Sea E/K una curva elíptica definida por un modelo minimal, y sea $\widetilde{E}/k_v$ la reducción de E módulo π.

(i) Si $\widetilde{E}$ es no singular, se dice que E *tiene buena reducción*.

(ii) Si $\widetilde{E}$ tiene un punto singular $P \in \widetilde{E}(k_v)$, se dice que E *tiene mala reducción*. Existen dos tipos de mala reducción:

  (a) Si P es un nodo, se dice que E *tiene reducción multiplicativa.*

  - Si las pendientes de las rectas tangentes en P están en k_v, se dice que E *tiene reducción split*.
  - Si las pendientes de las rectas tangentes en P no están en k_v, se dice que E *tiene reducción non-split*.

  (b) Si P es una cúspide, se dice que E *tiene reducción aditiva*.

De la proposición 3.1, se deduce el siguiente resultado.

Proposición 3.4. Sea E/K una curva elíptica definida por un modelo minimal

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

con discriminante Δ_E. Entonces:

1. E tiene buena reducción si y sólo si $v(\Delta_E) = 0$.
2. E tiene reducción multiplicativa si y sólo si $v(\Delta_E) > 0$ y $v(c_4) = 0$.
3. E tiene reducción aditiva si y sólo si $v(\Delta_E) > 0$ y $v(c_4) > 0$.

3.5. Curvas elípticas sobre cuerpos de números

Teorema de Mordell-Weil

Sea K un cuerpo de números, y sea E/K una curva elíptica. Por el corolario 3.1, $E(K)$ tiene estructura de grupo abeliano. El celebrado teorema de Mordell-Weil, que enunciamos a continuación, da más información sobre la estructura de $E(K)$ en este caso.

Teorema 3.2 (Mordell-Weil)**.** *Sea E/K una curva elíptica con K un cuerpo de números. Entonces, $E(K)$ es un grupo finitamente generado.*

Demostración. Ver capítulo VIII de [Sil09]. □

Este teorema, junto con el teorema de estructura de grupos abelianos finitamente generados, implican que

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

donde $E(K)_{\text{tors}}$ es el subgrupo de $E(K)$ formado por todos los elementos de torsión, y r es un entero no negativo, llamado *rango de* E. Si $K = \mathbb{Q}$, entonces $E(\mathbb{Q})_{\text{tors}}$ está explícitamente determinado por el siguiente teorema, que fue demostrado por Barry Mazur en los artículos [Maz77] y [MG78].

Teorema 3.3 (de torsión de Mazur)**.** *Sea $E/\mathbb{Q}$ una curva elíptica. Entonces $E(\mathbb{Q})_{\text{tors}}$ es isomorfo a uno de los siguientes grupos:*

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

Además, si G es cualquiera de estos grupos, existe una curva elíptica $E/\mathbb{Q}$ tal que

$$E(\mathbb{Q})_{\text{tors}} \cong G.$$

Modelo minimal global

En esta subsección, utilizaremos la siguiente notación:

- K es un cuerpo de números.
- M_K^0 es el conjunto de valoraciones en K.
- Si $v \in M_K^0$, denotaremos K_v a la completación de K respecto de cualquier valor absoluto (necesariamente, no arquimediano) definido a partir de v.

Como $K \subset K_v$ para toda $v \in M_K^0$, cualquier curva elíptica E/K puede verse como una curva elíptica definida sobre K_v. Esto nos permite dar la siguiente definición.

Definición 3.8. Sea E/K una curva elíptica definida por un modelo de Weierstrass

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

Dada $v \in M_K^0$, se dice que el modelo es *minimal en* v si es minimal para E/K_v. Se dice que el modelo es *minimal* si es minimal en v para toda $v \in M_K^0$.

En este caso, no siempre es posible encontrar un modelo minimal para una curva elíptica E/K. El corolario VIII.8.3 de [Sil09] da una caracterización de los cuerpos de números sobre los que una curva elíptica admite un modelo minimal. En particular, si $K = \mathbb{Q}$, entonces toda curva elíptica $E/\mathbb{Q}$ admite un modelo minimal. Esto nos permite dar la siguiente definición.

Definición 3.9. Sea $E/\mathbb{Q}$ una curva elíptica dada por un modelo minimal. Dado un primo ℓ, se dice que E *tiene buena* (respectivamente, *mala) reducción en* ℓ si $E/\mathbb{Q}_\ell$ tiene buena (respectivamente, mala) reducción. En particular, si $E/\mathbb{Q}$ no tiene mala reducción aditiva en ℓ para todo primo ℓ, se dice que E es *semiestable*.

3.6. Representaciones de Galois asociadas a curvas elípticas

Definición 3.10. Sea $E/\mathbb{Q}$ una curva elíptica. Para todo entero $m \geq 1$, se define el *subgrupo de m-torsión de $E(\overline{\mathbb{Q}})$* como

$$E[m] = \{P \in E(\overline{\mathbb{Q}}) : [m]P = O_E\},$$

y todo $P \in E[m]$ se llama *punto de m-torsión de E*. Además, denotamos $\mathbb{Q}(E[m])$ al cuerpo generado por las coordenadas de los puntos de m-torsión de E sobre $\mathbb{Q}$.

Proposición 3.5. Sea $E/\mathbb{Q}$ una curva elíptica. Para todo entero $m \geq 1$, existe un isomorfismo de grupos

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

Demostración. Ver corolario III.6.4. de [Sil09]. □

Dada una curva elíptica $E/\mathbb{Q}$, veamos cómo obtener una representación de Galois a partir del subgrupo de p-torsión de E, siendo p un primo. El grupo absoluto de Galois $G_{\mathbb{Q}}$ actúa en los puntos de $E(\overline{\mathbb{Q}})$ como sigue: para todo $\sigma \in G_{\mathbb{Q}}$ y para todo $P \in E(\overline{\mathbb{Q}})$, se define

$$\sigma(P) = \begin{cases} (\sigma(x), \sigma(y)) & \text{si } P = (x, y), \\ O_E & \text{si } P = O_E. \end{cases}$$

Se puede comprobar[2] que para todo $P, Q \in E(\overline{\mathbb{Q}})$ y para todo $\sigma \in G_{\mathbb{Q}}$, se verifica:

1. $\sigma(P + Q) = \sigma(P) + \sigma(Q)$,
2. $\sigma(-P) = -\sigma(P)$,
3. Si $P \in E[m]$ para un entero $m \geq 1$, entonces $\sigma(P) \in E[m]$.

Por tanto, todo $\sigma \in G_{\mathbb{Q}}$ induce un automorfismo en $E[p]$. Por la proposición 3.5,

$$E[p] \cong \mathbb{F}_p \times \mathbb{F}_p,$$

luego $E[p]$ es un $\mathbb{F}_p$-espacio vectorial de dimensión 2. Si fijamos una base $\{P, Q\}$ de este espacio vectorial, todo automorfismo de $E[p]$ inducido por un elemento $\sigma \in G_{\mathbb{Q}}$ viene dado por una matriz

$$M_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ con } a, b, c, d \in \mathbb{F}_p.$$

Por tanto, podemos considerar la representación de Galois

$$\begin{aligned} \overline{\rho}_{E,p} \colon G_{\mathbb{Q}} &\to \mathrm{Aut}_{\mathbb{F}_p}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p) \\ \sigma &\mapsto M_\sigma. \end{aligned}$$

[2] Ver proposición 6.3 del capítulo 6 de [ST92].

La acción de $\overline{\rho}_{E,p}(\sigma)$ en $E[p]$ viene dada como sigue: si $R = x_1P + x_2Q \in E[p]$ con $x_1, x_2 \in \mathbb{F}_p$, entonces,

$$\overline{\rho}_{E,p}(\sigma)(R) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Observemos que $\sigma \in \ker \overline{\rho}_{E,p}$ si y sólo si $\sigma(R) = R$ para todo $R \in E[p]$, y esto ocurre si y sólo si σ actúa trivialmente en $\mathbb{Q}(E[p])$. Por tanto,

$$\ker \overline{\rho}_{E,p} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[p])),$$

y la extensión $\mathbb{Q}(E[p])/\mathbb{Q}$ es de Galois. Veamos algunas propiedades $\overline{\rho}_{E,p}$.

Proposición 3.6. Sea $E/\mathbb{Q}$ una curva elíptica con buena reducción en ℓ. Si $\ell \neq p$, entonces la representación $\overline{\rho}_{E,p}$ es no ramificada en ℓ.

Demostración. Ver proposición VII.4.1 de [Sil09]. □

Proposición 3.7. Sea $E/\mathbb{Q}$ una curva elíptica. Para todo primo p, se verifica $\det \overline{\rho}_{E,p} = \chi_p$.

Demostración. Se puede definir un operador

$$e_p(\cdot,\cdot)\colon E[p] \times E[p] \to \boldsymbol{\mu}_p,$$

llamado *Weil pairing*. La proposición III.8.1 [Sil09] asegura que $e_p(\cdot,\cdot)$ satisface las siguientes propiedades:

1. Es bilineal.
2. Es alternado, es decir, $e_p(P,P) = 1$ para todo $P \in E[p]$. En particular, $e_p(P,Q) = e_p(Q,P)^{-1}$ para todo $P, Q \in E[p]$.
3. Es compatible con la acción de $G_{\mathbb{Q}}$, es decir, $e_p(\sigma(P), \sigma(Q)) = \sigma(e_p(P,Q))$ para todo $\sigma \in G_{\mathbb{Q}}$ y para todo $P, Q \in E[p]$.

Fijemos una base $\{P, Q\}$ de $E[p]$, y sea $\sigma \in G_{\mathbb{Q}}$ tal que

$$\overline{\rho}_{E,p}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ con } a, b, c, d \in \mathbb{F}_p.$$

Es decir, $\sigma(P) = aP + cQ$ y $\sigma(Q) = bP + dQ$. Las propiedades de $e_p(\cdot,\cdot)$ implican que es sobreyectivo, luego $e_p(P,Q) = \zeta_p$, siendo ζ_p una raíz primitiva p-ésima de la unidad. Por tanto,

$$\begin{aligned}
\sigma(\zeta_p) &= \sigma(e_p(P,Q)) \\
&= e_p(\sigma(P), \sigma(Q)) && \text{Por la propiedad 3} \\
&= e_p(aP + cQ, bP + dQ) \\
&= e_p(aP, bP)e_p(aP, dQ)e_p(cQ, bP)e_p(cQ, dQ) && \text{Por la propiedad 1} \\
&= e_p(P,P)^{ab}e_p(P,Q)^{ad}e_p(Q,P)^{cd}e_p(Q,Q)^{cd} && \text{Por la propiedad 1} \\
&= e_p(P,Q)^{ad}e_p(Q,P)^{bc} && \text{Por la propiedad 2} \\
&= e_p(P,Q)^{ad}e_p(P,Q)^{-bc} && \text{Por la propiedad 2} \\
&= e(P,Q)^{ad-bc} = \zeta_p^{ad-bc}.
\end{aligned}$$

Por definición de carácter ciclotómico, tenemos que $\sigma(\zeta_p) = \zeta_p^{\chi_p(\sigma)}$. Como $ad - bc = \det \overline{\rho}_{E,p}(\sigma)$, el cálculo anterior implica que $\chi_p = \det \overline{\rho}_{E,p}$, como queríamos. □

Teorema 3.4. *Sea $E/\mathbb{Q}$ una curva elíptica semiestable. Dado un primo $p \geq 3$, supongamos que $\overline{\rho}_{E,p}$ es reducible. Entonces, E es $\mathbb{Q}$-isógena a una curva elíptica $E'/\mathbb{Q}$. Además, existe un punto de p-torsión racional no trivial de E o de E'.*

Demostración. Como $\overline{\rho}_{E,p}$ es reducible, existe un subespacio $H \subset E[p]$ de dimensión 1 invariante por la acción de $G_{\mathbb{Q}}$. Por la proposición 3.3, existe una única curva elíptica $E' = E/H$ y una única isogenia no constante $\Phi\colon E \to E'$ tal que $\ker \Phi = H$. Además, como H es invariante por la acción de $G_{\mathbb{Q}}$, entonces E' es una curva elíptica definida sobre $\mathbb{Q}$, y E y E' son $\mathbb{Q}$-isógenas.

En particular, $H = \langle P \rangle$, con $P \in E[p]$. Si tomamos una base $\{P, Q\}$ de $E[p]$, podemos expresar $\overline{\rho}_{E,p}$ como

$$\overline{\rho}_{E,p} = \begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix}, \text{ con } \phi_1, \phi_2 \text{ dos caracteres de } G_{\mathbb{Q}}.$$

De hecho, $\phi_1\colon G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{F}_p}(H)$. Ahora bien, el lema 6 de la página 307 de [Ser72] asegura que si $p \geq 3$ y E es semiestable, uno de estos caracteres es el trivial, y el otro es χ_p.

- Si $\phi_1 = 1$ y $\phi_2 = \chi_p$, entonces $\sigma(P) = P$ para todo $\sigma \in G_{\mathbb{Q}}$, luego P es un punto racional de p-torsión no trivial de E.
- Supongamos que $\phi_1 = \chi_p$ y $\phi_2 = 1$. Entonces, $\Phi(Q)$ es un punto de p-torsión de E', pues
$$O_{E'} = \Phi(O_E) = \Phi([p]Q) = [p]\Phi(Q),$$
y es no trivial ya que $\ker \Phi = \langle P \rangle$ y Q es linealmente independiente de P. Sea $\sigma \in G_{\mathbb{Q}}$ tal que $\sigma(Q) = bP + dQ$, con $b \in \mathbb{F}_p$ y $d = \phi_2(\sigma) = 1$. Concluimos que $\Phi(Q)$ es un punto de p-torsión racional no trivial de E', pues
$$\sigma(\Phi(Q)) = \Phi(\sigma(Q)) = \Phi(bP + Q) = \Phi(Q),$$
como queríamos. □

Uniformización ℓ-ádica y curva de Tate

Sea ℓ un primo y fijemos una clausura algebraica $\mathbb{Q}_\ell$. Dado $q \in \mathbb{Q}_\ell^\times$ tal que $v_\ell(q) > 0$, definimos el subgrupo
$$q^{\mathbb{Z}} = \{q^n : n \in \mathbb{Z}\} \subset K^\times.$$

Sea $E/\mathbb{Q}$ una curva elíptica con mala reducción multiplicativa en ℓ. Es decir, $E/\mathbb{Q}_\ell$ tiene mala reducción multiplicativa, y podemos suponer que es split salvo una extensión cuadrática no ramificada de $\mathbb{Q}_\ell$, gracias al teorema C.14.1.d de [Sil09]. El objetivo de esta subsección es construir un isomorfismo $E(\overline{\mathbb{Q}}_\ell) \cong \overline{\mathbb{Q}}_\ell^\times / q^{\mathbb{Z}}$ que nos permitirá caracterizar la ramificación en ℓ de la representación $\overline{\rho}_{E,p}$ en términos del discriminante minimal Δ_E, siempre que $\ell \neq p$.

Las principales referencias para esta subsección son el capítulo V de [Sil13], el apéndice C de [Sil09] y el apéndice A.1.1 y A.1.2 de [Ser97].

Dado $q \in \mathbb{Q}_\ell^\times$ tal que $v_\ell(q) > 0$, definimos las siguientes siguientes series:

$$s_k(q) = \sum_{n=1}^{\infty} \frac{n^k q^n}{1-q^n}, \quad a_4(q) = -5s_3(q) \text{ y } a_6(q) = -\frac{5s_3(q)+7s_5(q)}{12}.$$

Entonces, las series $a_4(q)$ y $a_6(q)$ convergen en $\mathbb{Z}_\ell$, y podemos considerar la ecuación de Weierstrass

$$y^2 + xy = x^3 + a_4(q)x + a_6(q), \tag{3.5}$$

que tiene discriminante

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24}.$$

Como $v_\ell(\Delta(q)) = v_\ell(q) > 0$, el producto anterior converge a un elemento no nulo de $\mathbb{Q}_\ell$. Por tanto, la ecuación de Weierstrass (3.5) es un modelo para una curva elíptica $E_q/\mathbb{Q}_\ell$, llamada *curva de Tate asociada a* q. El j-invariante de E_q es

$$j(q) = \frac{(1+48a_4(q))^3}{\Delta(q)} = \frac{1}{q}\left(1+744q+196884q^2+\dots\right).$$

En particular, como $v_\ell(q) > 0$,

$$v_\ell(j(q)) = v_\ell\left(\frac{1}{q}+744+196884q+\dots\right) = -v_\ell(q) < 0. \tag{3.6}$$

Teorema 3.5 (Tate)**.** *Dado $q \in \mathbb{Q}_\ell^\times$ tal que $v_\ell(q) > 0$, las series*

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q) \text{ y } Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q).$$

convergen para todo $u \in \overline{\mathbb{Q}}_\ell^\times$ tal que $u \notin q^{\mathbb{Z}}$, y definen un homomorfismo sobreyectivo

$$\Phi\colon \overline{\mathbb{Q}}_\ell^\times \to E_q(\overline{\mathbb{Q}}_\ell)$$
$$u \mapsto \begin{cases} (X(u,q), Y(u,q)) & \text{si } u \notin q^{\mathbb{Z}}, \\ O_{E_q} & \text{si } u \in q^{\mathbb{Z}}. \end{cases}$$

cuyo núcleo es $q^{\mathbb{Z}}$. Además, Φ es compatible con la acción de $G_{\mathbb{Q}_\ell}$, es decir,

$$\Phi(\sigma(u)) = \sigma(\Phi(u)) \text{ para todo } u \in \overline{\mathbb{Q}}_\ell^\times \text{ y para todo } \sigma \in G_{\mathbb{Q}_\ell}.$$

En particular, para toda extensión finita $K/\mathbb{Q}_\ell$, Φ induce un isomorfismo $K^\times/q^{\mathbb{Z}} \cong E_q(K)$ que es compatible con la acción de $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/K)$.

Demostración. Ver teorema V.3.1 de [Sil13]. □

Teorema 3.6 (Tate)**.** *Sea $E/\mathbb{Q}_\ell$ una curva elíptica tal que $v_\ell(j_E) < 0$. Entonces, existe un único $q \in \mathbb{Q}_\ell^\times$ con $v_\ell(q) > 0$ tal que E es $\overline{\mathbb{Q}}_\ell$-isomorfa a la curva de Tate E_q asociada a q. En particular, $j_E = j(q)$. Es más, E es $\mathbb{Q}_\ell$-isomorfa a E_q si y sólo si E tiene mala reducción multiplicativa split.*

Demostración. Ver teorema V.5.3 de [Sil13]. □

Teorema 3.7. *Sea $E/\mathbb{Q}$ una curva elíptica semiestable. Supongamos que E tiene reducción multiplicativa en $\ell \neq p$. Entonces, $\overline{\rho}_{E,p}$ es no ramificada en ℓ si y sólo si $v_\ell(\Delta_E) \equiv 0 \mod p$, siendo Δ_E el discriminante minimal de E.*

Demostración. Como E tiene mala reducción multiplicativa en ℓ, entonoces $v_\ell(\Delta_E) > 0$ y $v_\ell(c_4) = 0$, por la proposición 3.4. Por tanto,

$$v_\ell(j_E) = v_\ell\left(\frac{c_4}{\Delta_E}\right) = -v_\ell(\Delta_E) < 0.$$

Por el teorema 3.6, existe un único $q \in \mathbb{Q}_\ell^\times$ con $v_\ell(q) > 0$ tal que $E/\mathbb{Q}_\ell$ es $\mathbb{Q}_\ell$-isomorfa a la curva de Tate E_q asociada a q. En particular, $j_E = j(q)$, luego se sigue de (3.6) que

$$v_\ell(\Delta_E) = -v_\ell(j_E) = -v_\ell(j(q)) = v_\ell(q). \tag{3.7}$$

Supongamos que $E/\mathbb{Q}_\ell$ tiene reducción non-split. Entonces, por el teorema C.14.1.d de [Sil09], existe una única extensión $K/\mathbb{Q}_\ell$ cuadrática y no ramificada tal que E/K tiene reducción split. Por el teorema 3.5, existe un isomorfismo

$$E(\overline{\mathbb{Q}}_\ell) \cong \overline{\mathbb{Q}}_\ell^\times / q^{\mathbb{Z}}$$

compatible con la acción de $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/K)$. La imagen del subgrupo de p-torsión $E(\overline{\mathbb{Q}}_\ell)[p]$ bajo este isomorfismo es el subgrupo

$$\langle \zeta_p, q^{1/p} \rangle = \{\zeta_p^a (q^{1/p})^b : 0 \leq a, b, < p\},$$

donde $q^{1/p}$ es una raíz del polinomio $x^p - q$. Por tanto, después de fijar una $\mathbb{Q}$-inclusión $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$, basta probar que la extensión $K(\zeta_p, q^{1/p})/K$ es no ramificada si y sólo si $v_\ell(q) \equiv 0 \mod p$, por (3.7).

Si $K(\zeta_p, q^{1/p})/K$ es no ramificada, entonces ℓ es uniformizante en $K(\zeta_p, q^{1/p})$, pues $K/\mathbb{Q}_\ell$ es no ramificada. Luego,

$$q^{1/p} = \varepsilon \ell^m \text{ con } v_\ell(\varepsilon) = 0 \text{ y } m > 0,$$

y por tanto $q = \varepsilon^p \ell^{pm}$. Concluimos que $v_\ell(q) = pm \equiv 0 \mod p$.

Recíprocamente, supongamos que $K(\zeta_p, q^{1/p})/K$ es ramificada. Sea $L = K(\zeta_p)$. Como $p \neq \ell$, la extensión L/K es no ramificada, luego $L(q^{1/p})/L$ es ramificada. No es difícil comprobar que esto sólo es posible si $v_\ell(q) \not\equiv 0 \mod p$.

Finalmente, si $E/\mathbb{Q}_\ell$ tiene reducción split, se razona de manera análoga con $K = \mathbb{Q}_\ell$, concluyendo el resultado. □

4 Formas modulares

"There are five fundamental operations in mathematics: addition, subtraction, multiplication, division, and modular forms."

— Martin Eichler.

En este capítulo introduciremos la teoría básica de formas modulares, centrándonos en la reducción módulo p de las mismas y sus representaciones asociadas. Las principales referencias utilizadas en este capítulo son [DS05] y [Loz11].

4.1. Formas modulares y formas cuspidales

Definición 4.1. Se define *grupo modular* como el grupo de matrices

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

Denotemos $\Im(z)$ la parte imaginaria de un número complejo z, y denotemos $\mathcal{H}$ al semiplano superior complejo, es decir,

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

El grupo modular actúa en $\mathcal{H}$ mediante *transformaciones lineales fraccionarias*, también llamadas *transformaciones de Möbius*. Esta acción se define como

$$M(z) = \frac{az+b}{cz+d}, \text{ para toda } M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ y para todo } z \in \mathcal{H}.$$

Veamos que la acción está bien definida. Dado $z \in \mathcal{H}$, tenemos que

$$\Im(M(z)) = \Im\left(\frac{az+b}{cz+d}\right) = \Im\left(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}\right) = \frac{\Im(adz+bc\bar{z})}{|cz+d|^2},$$

y como $ad - bc = 1$, entonces $\Im(adz + bc\bar{z}) = \Im(z)$. Finalmente,

$$\Im(M(z)) = \frac{\Im(z)}{|cz+d|^2} > 0,$$

pues $\Im(z) > 0$. Concluimos que $M(z) \in \mathcal{H}$, luego la acción está bien definida. Además, se puede comprobar[1] que el grupo modular está generado por las matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

[1] Ver corolario 3.3.5 de [Loz11]

Po tanto, el grupo de transformaciones de Möbius definido por la acción de $\mathrm{SL}_2(\mathbb{Z})$ en el $\mathcal{H}$ está generado por las funciones

$$z \mapsto z+1 \quad \text{y} \quad z \mapsto \frac{-1}{z}.$$

También será de interés la acción de ciertos subgrupos de $\mathrm{SL}_2(\mathbb{Z})$ en el semiplano superior complejo. Dado $N \geq 1$ entero, estos subgrupos son

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

Definición 4.2. Sea k un entero positivo. Para toda matriz $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, se define el operador $[M]_k \colon \{f \colon \mathcal{H} \to \mathbb{C}\} \to \{f \colon \mathcal{H} \to \mathbb{C}\}$ como

$$(f[M]_k)(z) = (cz+d)^{-k} f(M(z)) \text{ para todo } z \in \mathcal{H}.$$

Observación. Sea k un entero positivo. Si $f \colon \mathcal{H} \to \mathbb{C}$ es una función meromorfa, entonces $f[M]_k$ también es meromorfa y tiene los mismos ceros y polos que f para toda matriz $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, pues $cz + d \notin \{0, \infty\}$ para todo $z \in \mathcal{H}$.

Definición 4.3. Sean N y k enteros positivos. Una función $f \colon \mathcal{H} \to \mathbb{C}$ se dice *débilmente modular de peso k y nivel N* si f es meromorfa en $\mathcal{H}$ y verifica

$$(f[M]_k) = f \text{ para toda } M \in \Gamma_1(N).$$

Observación. Sean N y k enteros positivos. Si f es una función débilmente modular de peso k y nivel N, entonces verifica

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \text{ para toda } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) \text{ y para todo } z \in \mathcal{H}.$$

Esta condición para $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ se traduce en

$$f(z+1) = f(z) \text{ para todo } z \in \mathcal{H}.$$

Es decir, si $f \colon \mathcal{H} \to \mathbb{C}$ es débilmente modular de peso k y nivel N entonces f es periódica de periodo 1 y admite una expansión de Fourier de la forma

$$f(q) = \sum_{n \in \mathbb{Z}} a_n(f) q^n, \text{ con } q = e^{2\pi i z},\ z \in \mathcal{H} \text{ y } a_n(f) \in \mathbb{C},$$

también llamada *q-expansión de f.*

Definición 4.4. Sea $f \colon \mathcal{H} \to \mathbb{C}$ una función débilmente modular de peso k y nivel N. Los coeficientes $a_n(f)$ se llaman *coeficientes de Fourier de f*. Además, se dice que

- f *es holomorfa en* ∞ si $a_n(f) = 0$ para todo $n < 0$.
- f *se anula en* ∞ si $a_n(f) = 0$ para todo $n \leq 0$.
- f *está normalizada* si se anula en ∞ y $a_1(f) = 1$.

Definición 4.5. Sean N y k enteros positivos. Se dice que $f\colon \mathcal{H} \to \mathbb{C}$ es una *forma modular de peso* k *y nivel* N si

1. f es débilmente modular de peso k,
2. f es holomorfa en $\mathcal{H}$,
3. $f[M]_k$ es holomorfa en ∞ para toda matriz $M \in \mathrm{SL}_2(\mathbb{Z})$.

Si además $f[M]_k$ se anula en ∞ para toda $M \in \mathrm{SL}_2(\mathbb{Z})$, se dice que f es una *forma cuspidal de peso* k *y nivel* N. Al conjunto de formas modulares (respectivamente, cuspidales) de peso k y nivel N lo denotamos $\mathcal{M}_k(N)$ (respectivamente, $\mathcal{S}_k(N)$).

Es directo comprobar que $\mathcal{M}_k(N)$ y $\mathcal{S}_k(N)$ son espacios vectoriales sobre $\mathbb{C}$ y que $\mathcal{S}_k(N)$ es subespacio de $\mathcal{M}_k(N)$. Además, son de dimensión finita (se puede encontrar la fórmula de la dimensión en el teorema 3.5.1 y en el teorema 3.6.1 de [DS05]) y admiten una descomposición como suma directa de subespacios que dependen de caracteres de Dirichlet módulo N.

Definición 4.6. Sean N y k enteros positivos, y ε un carácter de Dirichlet módulo N. Se dice que f es una *forma modular de peso* k*, nivel* N *y carácter* ε si $f \in \mathcal{M}_k(N)$ y verifica

$$f\left(\frac{az+b}{cz+d}\right) = \varepsilon(d)(cz+d)^k f(z) \text{ para toda } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \text{ y para todo } z \in \mathcal{H}.$$

Si además $f \in \mathcal{S}_k(N)$, se dice que f es una *forma cuspidal de peso* k*, nivel* N *y carácter* ε. El conjunto de formas modulares (respectivamente, cuspidales) de peso k, nivel N y carácter ε se denota $\mathcal{M}_k(N, \varepsilon)$ (respectivamente, $\mathcal{S}_k(N, \varepsilon)$).

Observación 4.1. La matriz $M = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ pertenece a $\Gamma_0(N)$ para todo entero $N \geq 1$. Por tanto, dados enteros positivos N y k y un carácter de Dirichlet ε módulo N, toda forma modular $f \in \mathcal{M}_k(N, \varepsilon)$ verifica que

$$f(z) = f(M(z)) = \varepsilon(-1)(-1)^k f(z) \text{ para todo } z \in \mathcal{H}.$$

Esto implica que el espacio $\mathcal{M}_k(N, \varepsilon)$ es trivial a no ser que

$$\varepsilon(-1) = (-1)^k,$$

y lo mismo ocurre para $\mathcal{S}_k(N, \varepsilon)$, al ser un subespacio de $\mathcal{M}_k(N, \varepsilon)$.

Además, se puede probar[2] que los espacios definidos anteriormente admiten una descomposición

$$\mathcal{M}_k(N) = \bigoplus_{\varepsilon} \mathcal{M}_k(N, \varepsilon) \text{ y } \mathcal{S}_k(N) = \bigoplus_{\varepsilon} \mathcal{S}_k(N, \varepsilon), \tag{4.1}$$

donde ε recorre los carácteres de Dirichlet módulo N.

[2] Ver capitulo 4, sección 3 de [DS05].

4.2. Operadores de Hecke

Fijemos enteros positivos N y k y un carácter de Dirichlet $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. Vamos a definir unos operadores en el espacio de formas cuspidales que preservan la descomposición (4.1). Esta sección se basa en el capítulo 5 de [DS05] y la sección 4 del capítulo 4 de [Loz11].

Definición 4.7. Dado $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$, se define el *operador diamante* $\langle\delta\rangle\colon \mathcal{S}_k(N) \to \mathcal{S}_k(N)$ como

$$(\langle\delta\rangle(f))(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

para alguna matriz $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ tal que $d \equiv \delta \bmod N$.

Se puede comprobar que el operador diamante no depende de la matriz elegida, luego sólo depende de $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$. Además, no es difícil comprobar de la definición que

$$\mathcal{S}_k(N,\varepsilon) = \{f \in \mathcal{S}_k(N) : \langle\delta\rangle(f) = \varepsilon(\delta)(f) \text{ para todo } \delta \in (\mathbb{Z}/N\mathbb{Z})^\times\}.$$

Definición 4.8. Para cada primo ℓ, se define un operador $T_\ell\colon \mathcal{S}_k(N,\varepsilon) \to \mathcal{S}_k(N,\varepsilon)$, llamado *$\ell$-ésimo operador de Hecke*, como sigue: para toda forma cuspidal $f \in \mathcal{S}_k(N,\varepsilon)$ con q-expansión

$$f(q) = \sum_{n=1}^{\infty} a_n(f) q^n, \text{ con } q = e^{2\pi i z} \text{ y } z \in \mathcal{H},$$

se define el operador T_ℓ como

$$T_\ell(f)(q) = \begin{cases} \displaystyle\sum_{n=1}^{\infty} a_{n\ell}(f) q^n + \varepsilon(\ell)\ell^{k-1} \sum_{n=1}^{\infty} a_n(f) q^{n\ell} & \text{si } \ell \nmid N, \\ \displaystyle\sum_{n=1}^{\infty} a_{n\ell}(f) q^n & \text{si } \ell \mid N. \end{cases}$$

Definición 4.9. Una forma cuspidal $f \in \mathcal{S}_k(N,\varepsilon)$ se dice *autoforma* si f es un autovector para todos los operadores de Hecke T_ℓ, simultáneamente.

Observación. Se puede probar que si $f \in \mathcal{S}_k(N,\varepsilon)$ es una autoforma normalizada, entonces sus coeficientes de Fourier son enteros algebraicos. Se recomienda ver el teorema 6.5.1 de [DS05] para el caso $k = 2$ y la observación 3.5.3 de [DI95] para el caso general.

4.3. Formas cuspidales con coeficientes en $\overline{\mathbb{F}}_p$

Fijemos un primo p. En esta sección, definiremos el concepto de *forma cuspidal con coeficientes en $\overline{\mathbb{F}}_p$*, o *forma cuspidal módulo p*. La idea es, como bien indica el nombre, definirlas a partir de la reducción módulo p de las formas cuspidales clásicas, siempre que tengan coeficientes de Fourier en $\overline{\mathbb{Z}}$. Utilizaremos la siguiente notación:

- N es un entero positivo coprimo con p, y k es un entero tal que $k \geq 2$.
- $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$ es un carácter verificando $\varepsilon(-1) = (-1)^k$ si $p \neq 2$. De lo contrario, suponemos que k es par.

- Fijamos un par de $\mathbb{Q}$-inclusiones $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ y $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. La primera inclusión induce un homomorfismo $\overline{\mathbb{Z}} \to \overline{\mathbb{F}}_p$, que denotaremos $x \mapsto \tilde{x}$.

Sabemos que ε tiene imagen finita y toma valores en las raíces de la unidad de orden $\varphi(N)$. Consideramos el único homomorfismo

$$\varepsilon_0 \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Z}}^\times$$

tal que $\widetilde{\varepsilon_0(x)} = \varepsilon(x)$ para todo $x \in (\mathbb{Z}/N\mathbb{Z})^\times$. Este homomorfismo es un carácter que verifica $\varepsilon_0(-1) = (-1)^k$.

Definición 4.10. Una *forma cuspidal con coeficientes en $\overline{\mathbb{F}}_p$ de peso k, nivel N y carácter ε* es una serie formal

$$f = \sum_{n=1}^{\infty} a_n(f) q^n, \text{ con } a_n \in \overline{\mathbb{F}}_p,$$

tal que existe una forma cuspidal $F \in \mathcal{S}_k(N, \varepsilon_0)$ con coeficientes en $\overline{\mathbb{Z}}$ verificando $\widetilde{F} = f$. Es decir, si $A_n(F)$ son los coeficientes de Fourier de F, entonces $\widetilde{A_n(F)} = a_n(f)$ para todo entero $n \geq 1$. El conjunto de formas cuspidales con coeficientes en $\overline{\mathbb{F}}_p$ de peso k, nivel N y carácter ε se denota $\widetilde{\mathcal{S}}_k(N, \varepsilon)$.

Se puede comprobar que[3] que el conjunto $\widetilde{\mathcal{S}}_k(N, \varepsilon)$ verifica las siguientes propiedades:

- $\widetilde{\mathcal{S}}_k(N, \varepsilon)$ es un $\overline{\mathbb{F}}_p$-espacio vectorial. La definición de $\widetilde{\mathcal{S}}_k(N, \varepsilon)$ no depende de la elección de la inclusión $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, luego la dimensión de $\widetilde{\mathcal{S}}_k(N, \varepsilon)$ como $\overline{\mathbb{F}}_p$-espacio vectorial coincide con la dimensión de $\mathcal{S}_k(N, \varepsilon_0)$ como $\mathbb{C}$-espacio vectorial. Esto se sigue de la proposición 2.7 de [DS74].
- Para todo primo ℓ, el espacio $\widetilde{\mathcal{S}}_k(N, \varepsilon)$ es invariante por la acción de los operadores de Hecke $T_\ell \colon \widetilde{\mathcal{S}}_k(N, \varepsilon) \to \widetilde{\mathcal{S}}_k(N, \varepsilon)$, definidos como

$$T_\ell \colon \sum_{n=1}^{\infty} a_n q^n \mapsto \begin{cases} \displaystyle\sum_{n=1}^{\infty} a_{n\ell}(f) q^n + \varepsilon(\ell)\ell^{k-1} \sum_{n=1}^{\infty} a_n(f) q^{n\ell} & \text{si } \ell \nmid pN, \\ \displaystyle\sum_{n=1}^{\infty} a_{n\ell}(f) q^n & \text{si } \ell \mid pN. \end{cases}$$

- Si $f \in \widetilde{\mathcal{S}}_k(N, \varepsilon)$ es una autoforma normalizada, entonces la forma cuspidal asociada $F \in \mathcal{S}_k(N, \varepsilon_0)$ también es una autoforma normalizada para todo T_ℓ con ℓ primo.

Twists de formas cuspidales módulo p

Katz demuestra lo siguiente en [Kat06]:

Proposición 4.1. Existe un operador $\theta \colon \widetilde{\mathcal{S}}_k(N, \varepsilon) \to \widetilde{\mathcal{S}}_{k+p+1}(N, \varepsilon)$ cuya acción en las q-expansiones viene dada por

$$\theta \colon \sum_{n=1}^{\infty} a_n(f) q^n \mapsto \sum_{n=1}^{\infty} n a_n(f) q^n.$$

[3] Ver sección 3.1 de [Ser87].

Observación 4.2. Si $f \in \widetilde{\mathcal{S}}_k(N,\varepsilon)$, entonces $T_\ell(\theta f) = \ell\theta(T_\ell(f))$ para todo primo ℓ. Por tanto, si $f \in \widetilde{\mathcal{S}}_k(N,\varepsilon)$ es una autoforma cuspidal normalizada con coeficientes de Fourier $a_\ell(f)$, entonces $\theta f \in \widetilde{\mathcal{S}}_{k+p+1}(N,\varepsilon)$ es una autoforma cuspidal normalizada con coeficientes de Fourier $\ell a_\ell(f)$, para todo primo ℓ.

4.4. Representaciones de Galois asociadas a formas modulares

En el capítulo 3, construimos una representación de Galois módulo p a partir de los puntos de p-torsión una curva elíptica. Otra forma de obtener representaciones de Galois módulo p es a partir de autoformas cuspidales módulo p. Esto se debe al siguiente teorema:

Teorema 4.1 (Deligne). *Sean N un entero positivo coprimo con p, $k \geq 2$ un entero, y $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$ un carácter. Sea $f \in \widetilde{\mathcal{S}}_k(N,\varepsilon)$ una autoforma normalizada con coeficientes de Fourier $a_n(f)$ para todo $n \geq 1$. Entonces, existe una representación de Galois semisimple*

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

tal que para todo primo ℓ con $\ell \nmid Np$, se verifica

1. *ρ_f es no ramificada en ℓ,*
2. *$\operatorname{tr}\rho_f(\mathrm{Frob}_\ell) = a_\ell(f)$, y*
3. *$\det\rho_f(\mathrm{Frob}_\ell) = \varepsilon(\ell)\ell^{k-1}$.*

Como ρ_f es semisimple, las dos últimas propiedades aseguran que ρ_f es única salvo conjugación, gracias al teorema de Brauer-Nesbitt. Por ello, en las condiciones del teorema anterior, se dice que *ρ_f es la representación asociada a f*, o que *ρ_f proviene de f*.

El teorema 4.1 fue demostrado por Shimura en el caso $k = 2$. Se puede encontrar una construcción explícita de ρ_f para este caso en la sección 9.5 de [DS05]. El caso general fue demostrado por Deligne en [Del06].

Observación 4.3. Supongamos las condiciones del teorema anterior.

- Por el teorema 2.3, podemos extender $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$ a un carácter $\varepsilon\colon G_{\mathbb{Q}} \to \overline{\mathbb{F}}_p^\times$. Por tanto, teniendo en cuenta que $\chi_p(\mathrm{Frob}_\ell) = \ell$ para todo primo $\ell \neq p$, la propiedad 3 del teorema anterior equivale a

  $$\det\rho_f(\mathrm{Frob}_\ell) = \varepsilon(\mathrm{Frob}_\ell)\chi_p^{k-1}(\mathrm{Frob}_\ell) \text{ para todo } \ell \nmid Np.$$

  Por el teorema 2.1, esto equivale a $\det\rho_f = \varepsilon\chi_p^{k-1}$.

- El punto anterior implica que ρ_f es impar. En efecto, viendo ε como un carácter $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$, tenemos que $\varepsilon(-1) = (-1)^k$, por la observación 4.1. Viendo ε como $\varepsilon\colon G_{\mathbb{Q}} \to \overline{\mathbb{F}}_p^\times$, tenemos que $\varepsilon(c) = (-1)^k$, donde c denota la conjugación compleja. En efecto, como $\zeta_N \overset{c}{\mapsto} \zeta_N^{-1}$, la imagen de c bajo el isomorfismo (2.1) es -1. De manera similar, $\zeta_p \overset{c}{\mapsto} \zeta_p^{-1}$, luego $\chi_p(c) = -1$. Concluimos que ρ_f es impar, pues

  $$\det\rho_f(c) = \varepsilon(c)\chi_p^{k-1}(c) = (-1)^k(-1)^{k-1} = -1.$$

Fijemos para el resto de la sección una autoforma normalizada $f \in \widetilde{\mathcal{S}}_k(N, \varepsilon)$ en las condiciones del teorema 4.1, y denotemos $\rho_{f,p}$ a la representación local de ρ_f en p, después de fijar una $\mathbb{Q}$-inclusión $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Los siguientes resultados serán de gran utilidad para motivar la definición del peso en la conjetura de modularidad de Serre.

Teorema 4.2 (Fontaine)**.** *Supongamos que* $2 \leq k \leq p+1$*. Si* $a_p(f) = 0$*, entonces* $\rho_{f,p}$ *es irreducible, y*

$$\rho_{f,p}|_{I_p} \cong \begin{pmatrix} \psi'^{k-1} & 0 \\ 0 & \psi^{k-1} \end{pmatrix},$$

siendo ψ, ψ' *los caracteres fundamentales de nivel 2.*

Este teorema fue demostrado por Fontaine en dos cartas enviadas a Serre en 1979, pero la demostración nunca llegó a publicarse. Se puede encontrar una demostración en la sección 6 de [Edi92].

Proposición 4.2. Sea $\rho_{\theta f}$ la representación de Galois de módulo p asociada a la autoforma normalizada $\theta f \in \widetilde{\mathcal{S}}_{k+p+1}(N, \varepsilon)$. Entonces, $\rho_{\theta f} \cong \chi_p \otimes \rho_f$.

Demostración. Sea ℓ un primo tal que $\ell \nmid Np$. Por el teorema 4.1 y por la observación 4.2, $\rho_{\theta f}$ es una representación de Galois semisimple tal que

$$\operatorname{tr} \rho_{\theta f}(\mathrm{Frob}_\ell) = \ell a_\ell(f) \text{ y } \det \rho_{\theta f}(\mathrm{Frob}_\ell) = \varepsilon(\ell)\ell^{k+p}.$$

Por otro lado, teniendo en cuenta que $\chi_p(\mathrm{Frob}_\ell) = \ell$ para todo primo $\ell \neq p$, tenemos que

$$\begin{aligned} \operatorname{tr}(\chi_p \otimes \rho_f)(\mathrm{Frob}_\ell) &= \chi_p(\mathrm{Frob}_\ell) a_\ell(f) = \ell a_\ell(f), \\ \det(\chi_p \otimes \rho_f)(\mathrm{Frob}_\ell) &= \varepsilon(\ell)\chi_p^2(\mathrm{Frob}_\ell)\ell^{k-1} = \varepsilon(\ell)\ell^2\ell^{k-1} = \varepsilon(\ell)\ell^{k+p}. \end{aligned}$$

Por el teorema 4.1, ρ_f es semisimple y por tanto $\chi_p \otimes \rho_f$ también. Como $\rho_{\theta f}$ es semisimple, concluimos por el teorema 2.2 que $\rho_{\theta f} \cong \chi_p \otimes \rho_f$, como queríamos. □

Teorema 4.3 (Deligne)**.** *Supongamos que* $2 \leq k \leq p+1$*. Si* $a_p(f) \neq 0$*, entonces* $\rho_{f,p}$ *es reducible, y*

$$\rho_{f,p}|_{I_p} \cong \begin{pmatrix} \chi_p^{k-1} & * \\ 0 & 1 \end{pmatrix}.$$

Demostración. Ver [Gro90]. □

En todos estos teoremas, hemos supuesto que $2 \leq k \leq p+1$. Esto no es restrictivo gracias al siguiente resultado:

Proposición 4.3. Sea $f \in \widetilde{\mathcal{S}}_k(N, \varepsilon)$ una autoforma. Existen enteros i y k' tales que

$$0 \leq i \leq p-1 \quad \text{y} \quad 2 \leq k' \leq p+1,$$

y existe una autoforma $g \in \widetilde{\mathcal{S}}_{k'}(N, \varepsilon)$ de modo que f y $\theta^i g$ tienen los mismos autovalores para todo T_ℓ, con ℓ primo distinto de p.

Demostración. Ver teorema 3.4 de [Edi92]. □

5 La conjetura de modularidad de Serre

Hemos visto en el capítulo anterior que gracias al teorema de Deligne podemos obtener una representación de Galois $G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ a partir de una autoforma cuspidal con coeficientes en $\overline{\mathbb{F}}_p$. Recíprocamente, dada una representación de Galois $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$, es natural preguntarse bajo qué condiciones ρ está asociada a una autoforma cuspidal con coeficientes en $\overline{\mathbb{F}}_p$. Esta cuestión la resuelve la *conjetura de modularidad de Serre* en su versión débil:

Teorema 5.1 (Conjetura de modularidad de Serre, versión débil)**.** *Dada una representación de Galois impar e irreducible*

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p),$$

existe una autoforma cuspidal normalizada f con coeficientes en $\overline{\mathbb{F}}_p$ tal que $\rho \cong \rho_f$, siendo ρ_f la representación de Galois asociada a f.

Ahora bien, si ρ es una representación de Galois en las condiciones de este teorema, no se puede garantizar la unicidad de la autoforma de la que proviene ρ. Sin embargo, en [Ser87], Serre define un nivel $N(\rho)$, un peso $k(\rho)$ y un carácter $\varepsilon(\rho)$ asociados a ρ, de modo que $N(\rho)$ y $k(\rho)$ son óptimos en el siguiente sentido: para toda autoforma cuspidal normalizada $g \in \widetilde{\mathcal{S}}_k(N, \varepsilon)$ tal que $p \nmid N$, $k \geq 2$ y $\rho \cong \rho_g$, se verifica

$$N(\rho) \mid N \ \text{ y } \ k \geq k(\rho).$$

Con estos parámetros, podemos dar una versión más fuerte del teorema 5.1:

Teorema 5.2 (Conjetura de modularidad de Serre, versión fuerte)**.** *Dada una representación de Galois impar e irreducible*

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p),$$

existe una autoforma cuspidal normalizada f de nivel $N(\rho)$, peso $k(\rho)$ y carácter $\varepsilon(\rho)$ con coeficientes en $\overline{\mathbb{F}}_p$ tal que $\rho \cong \rho_f$, siendo ρ_f la representación de Galois asociada a f.

La conjetura de modularidad de Serre fue demostrada para el caso de $N(\rho) = 1$ y para pesos pequeños por Chandrashekhar Khare y Jean-Pierre Wintenberger en [KW04], y de manera independiente por Luis Dieulefait en [Die07]. En [Kha06], Khare la demostró para el caso $N(\rho) = 1$, y finalmente fue demostrada en su totalidad por Khare y Wintenberger en [KW09a] y [KW09b].

Este capítulo lo dedicamos a la construcción del nivel $N(\rho)$, el peso $k(\rho)$ y el carácter $\varepsilon(\rho)$, siguiendo el artículo original de Serre [Ser87] y el artículo de Bas Edixhoven [Edi92]. Para el resto del capítulo, denotamos $\mathrm{Aut}(V) = \mathrm{Aut}_{\overline{\mathbb{F}}_p}(V)$ y fijamos:

- Una representación de Galois $\rho\colon G_{\mathbb{Q}} \to \mathrm{Aut}(V) \cong \mathrm{GL}_2(\overline{\mathbb{F}}_p)$, siendo V un $\overline{\mathbb{F}}_p$-espacio vectorial de dimensión 2.
- Para todo primo entero ℓ, una $\mathbb{Q}$-inclusión $\iota_\ell\colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. Así, cada ι_ℓ induce una inclusión $\iota_\ell^*\colon G_{\mathbb{Q}_\ell} \hookrightarrow G_{\mathbb{Q}}$ dada por $\sigma \mapsto \sigma|_{\overline{\mathbb{Q}}}$.

5.1. El nivel $N(\rho)$

En esta sección, definiremos el nivel $N(\rho)$ inspirándonos en la siguiente observación: si ρ proviene de una autoforma cuspidal de nivel N, siendo N coprimo con p, el teorema de Deligne asegura que ρ es no ramificada en un primo ℓ siempre que $\ell \nmid pN$. Esto nos indica que la definición de $N(\rho)$ debería depender únicamente de la ramificación de ρ en todo primo distinto de p.

Así, para cualquier primo ℓ, consideramos la representación $\rho_\ell \colon G_{\mathbb{Q}_\ell} \to \mathrm{Aut}(V)$ dada por la restricción de ρ a $G_{\mathbb{Q}_\ell}$. Por la proposición 2.2, existe una extensión finita de Galois $L/\mathbb{Q}_\ell$ tal que

$$\ker \rho_\ell = \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/L) \text{ y } \rho_\ell(G_{\mathbb{Q}_\ell}) \cong \mathrm{Gal}(L/\mathbb{Q}_\ell).$$

Denotemos $G_\ell = \mathrm{Gal}(L/\mathbb{Q}_\ell)$. Para todo real $u \geq -1$ y para todo primo ℓ, sean $G_{\ell,u}$ el u-ésimo grupo de ramificación de G_ℓ con numeración baja, y $V_{\ell,u}$ el subespacio de V fijo por $G_{\ell,u}$.

Definición 5.1. Dado un primo ℓ, se define el *exponente del conductor de ρ en ℓ* como

$$n(\ell,\rho) = \sum_{u=0}^{\infty} \frac{\dim(V/V_{\ell,u})}{[G_{\ell,0} : G_{\ell,u}]}.$$

Dado un primo ℓ, está claro que $n(\ell,\rho)$ es finito, pues la filtración $\{G_{\ell,u}\}_{u\geq -1}$ es trivial a partir de un real $u \geq -1$ suficientemente grande. Más que eso, el teorema 1' de la sección 2 del capítulo VI de [Ser13] asegura que $n(\ell,\rho)$ es un entero no negativo, pero la demostración queda fuera del alcance de este trabajo. Además,

- $n(\ell,\rho) = 0 \iff G_{\ell,0} = \{\mathrm{id}\} \iff \rho$ es no ramificada en ℓ.
- $n(\ell,\rho) = \dim(V/V_{\ell,0}) \iff G_{\ell,1} = \{\mathrm{id}\} \iff \rho$ es moderada en ℓ.

Definición 5.2. Se define el *nivel de Serre asociado a ρ* como

$$N(\rho) = \prod_{\substack{\ell \neq p \\ \ell \text{ primo}}} \ell^{n(\ell,\rho)}.$$

Comprobemos que el nivel $N(\rho)$ es un número entero. En efecto, $n(\ell,\rho) = 0$ si y sólo si ρ es no ramificada en ℓ, y sabemos que ρ es no ramificada salvo en una cantidad finita de primos por el corolario 2.3. Concluimos que $N(\rho)$ es un número entero, y es coprimo con p por construcción.

Además, $N(\rho)$ sólo es divisible por los primos distintos de p en los que ρ es ramificada. En otras palabras, $\ell \nmid pN(\rho)$ si y sólo si ρ es no ramificada en $\ell \neq p$, que es lo que buscábamos. El hecho de que $N(\rho)$ sea óptimo se demuestra en los artículos [Car86] y [Liv89].

Por último, cabe destacar que $N(\rho)$ no es más que la parte coprima con p del *conductor de Artin de ρ*, denotado $\mathfrak{f}(\rho)$. Se recomienda consultar el capítulo VI de [Ser13] para ver algunas propiedades del conductor de Artin de una representación y resultados relacionados con el mismo.

5.2. El carácter $\varepsilon(\rho)$

Para construir el carácter $\varepsilon(\rho)$, consideramos la representación de Galois

$$\det\rho\colon G_{\mathbb{Q}} \to \mathrm{Aut}(\overline{\mathbb{F}}_p) \cong \overline{\mathbb{F}}_p^{\times}.$$

y su restricción $\det\rho_\ell\colon G_{\mathbb{Q}_\ell} \to \overline{\mathbb{F}}_p^{\times}$ a $G_{\mathbb{Q}_\ell}$ para cualquier primo ℓ. De nuevo, por la proposición 2.2, existe una extensión finita de Galois $M/\mathbb{Q}_\ell$ tal que

$$\ker(\det\rho_\ell) = \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/M) \quad \text{y} \quad \det\rho_\ell(G_{\mathbb{Q}_\ell}) \cong \mathrm{Gal}(M/\mathbb{Q}_\ell).$$

Mantenemos la notación utilizada en la sección 5.1, y fijamos la siguiente notación:

- Para todo real $r \geq -1$, sean G_ℓ^r el r-ésimo grupo de ramificación de G_ℓ con numeración alta, y V_ℓ^r el subespacio de V fijo por G_ℓ^r. Recordemos que $G_\ell = \mathrm{Gal}(L/\mathbb{Q}) \cong \rho_\ell(G_{\mathbb{Q}_\ell})$.
- Denotemos $H_\ell = \mathrm{Gal}(M/\mathbb{Q}_\ell)$. Para todo real $r \geq -1$, sean H_ℓ^r (respectivamente, $H_{\ell,r}$) el r-ésimo grupo de ramificación de H_ℓ con numeración alta (respectivamente, baja), y sea U_ℓ^r (respectivamente $U_{\ell,r}$) el subespacio de $U = \overline{\mathbb{F}}_p$ fijo por H_ℓ^r (respectivamente, $H_{\ell,r}$).

Gracias al teorema 2.3, podemos identificar $\det\rho$ con un carácter de Dirichlet. Para hallar su conductor, utilizaremos un resultado que afirma que el conductor de un carácter de Dirichlet coincide con su conductor de Artin.[1] El exponente del conductor y el conductor de Artin de $\det\rho$ son, respectivamente,

$$n(\ell,\det\rho) = \sum_{r=0}^{\infty} \frac{\dim(U/U_{\ell,r})}{[H_{\ell,0} : H_{\ell,r}]} \quad \text{y} \quad \mathfrak{f}(\det\rho) = \prod_{\ell \text{ primo}} \ell^{n(\ell,\det\rho)} = N(\det\rho)p^{n(p,\det\rho)}. \tag{5.1}$$

Así, podemos identificar $\det\rho$ con un carácter de Dirichlet primitivo módulo $\mathfrak{f}(\det\rho)$, pero también podemos identificarlo con otro carácter de Dirichlet cuyo módulo sea divisible por $\mathfrak{f}(\det\rho)$.

Vamos a probar que $\mathfrak{f}(\det\rho)$ divide a $pN(\rho)$. Observemos que, por la expresión (5.1), es suficiente demostrar que $n(p,\det\rho) \leq 1$ y que $n(\ell,\det\rho) \leq n(\ell,\rho)$ para todo primo ℓ. Para demostrar la segunda desigualdad, primero daremos una expresión del exponente del conductor de ρ y $\det\rho$ en términos de grupos de ramificación con numeración alta. Nos basamos en [Ulm15] para demostrar el siguiente lema.

Lema 5.1. Para todo primo ℓ, se verifica

$$n(\ell,\rho) = \int_{-1}^{\infty} \dim(V/V_\ell^r)\,dr \quad \text{y} \quad n(\ell,\det\rho) = \int_{-1}^{\infty} \dim(U/U_\ell^r)\,dr.$$

[1] Esto es una consecuencia de resultados de teoría de cuerpos de clases en dimensión 1, y la demostración queda fuera del alcance de este trabajo. Se recomienda consultar el comentario después del corolario 2 de la página 228 de [Ser13], así como la sección 3 del capítulo VI del mismo libro.

Demostración. Probaremos sólo la primera igualdad, la segunda se demuestra exactamente igual. Fijemos un primo ℓ. Para cada entero $i \geq -1$, consideramos la función real

$$u \mapsto \frac{\dim(V/V_{\ell,u})}{[G_{\ell,0} : G_{\ell,u}]}, \text{ con } i \leq u < i+1,$$

que es constante en cada intervalo $[i, i+1)$. Por tanto,

$$n(\ell,\rho) = \sum_{u=0}^{\infty} \frac{\dim(V/V_{\ell,u})}{[G_{\ell,0} : G_{\ell,u}]} = \lim_{m\to\infty} \sum_{i=0}^{m} \int_{i-1}^{i} \frac{\dim(V/V_{\ell,u})}{[G_{\ell,0} : G_{\ell,u}]}\, du = \int_{-1}^{\infty} \frac{\dim(V/V_{\ell,u})}{[G_{\ell,0} : G_{\ell,u}]}\, du. \quad (5.2)$$

Hacemos el cambio de variable $r = \varphi_L(u)$, siendo φ_L la función de Herbrand asociada a $G_\ell = \mathrm{Gal}(L/\mathbb{Q}_\ell)$. Así, para todo real $u \in [i, i+1)$ con $i \geq -1$ entero, se sigue de la observación 1.4 que

$$dr = \varphi_L'(u)\, du = \frac{du}{[G_{\ell,0} : G_{\ell,u}]} \text{ y } V_\ell^r = V_{\ell,\varphi_L^{-1}(r)} = V_{\ell,u}.$$

Basta sustituir estas expresiones en la última integral de (5.2) para concluir el resultado. □

Proposición 5.1. Para todo primo ℓ, se verifica $n(\ell, \det\rho) \leq n(\ell,\rho)$.

Demostración. Fijemos un primo ℓ. Por el lema anterior, el enunciado equivale a probar que

$$\int_{-1}^{\infty} \dim(U/U_\ell^r)\, dr \leq \int_{-1}^{\infty} \dim(V/V_\ell^r)\, dr,$$

Como los integrandos anteriores son funciones monótonas no negativas, basta probar que

$$\dim(U/U_\ell^r) \leq \dim(V/V_\ell^r) \text{ para todo } r \in [-1,\infty).$$

Para todo real $r \geq -1$, se tiene $\dim(U/U_\ell^r) = 1 - \dim(U_\ell^r)$ y $\dim(V/V_\ell^r) = 2 - \dim(V_\ell^r)$, luego basta probar que

$$\dim(V_\ell^r) - 1 \leq \dim(U_\ell^r) \text{ para todo } r \in [-1,\infty). \quad (5.3)$$

Sea $r \geq -1$ real. Como $\dim U_\ell^r \in \{0,1\}$ y $\dim V_\ell^r \in \{0,1,2\}$, claramente se tiene la desigualdad (5.3) siempre que $\dim(V_\ell^r) \in \{0,1\}$. Veamos qué ocurre si $\dim(V_\ell^r) = 2$, o equivalentemente, si $G_\ell^r = \{\mathrm{id}\}$.

Denotemos $N_\ell = \mathrm{Gal}(L/M)$. Del teorema de correspondencia de Galois, se sigue que $H_\ell \cong G_\ell/N_\ell$. Por el corolario 1.6,

$$H_\ell^r \cong (G_\ell/N_\ell)^r = G_\ell^r N_\ell/N_\ell$$

y como $G_\ell^r = \{\mathrm{id}\}$, entonces $H_\ell^r = \{\mathrm{id}\}$. Por tanto, $\dim(U_\ell^r) = 1$ y concluimos que se verifica la desigualdad (5.3), como queríamos. □

Proposición 5.2. Se verifica $n(p, \det\rho) \leq 1$.

Demostración. Sabemos por el corolario 2.1 que $\det\rho_p(G_{\mathbb{Q}_p})$ es un subgrupo cíclico finito de $\overline{\mathbb{F}}_p^\times$ de orden coprimo con p. Como $H_p \cong \det\rho_p(G_{\mathbb{Q}_p})$, entonces todo subgrupo de H_p es cíclico de orden coprimo con p. Sin embargo, $H_{p,1}$ es un subgrupo de H_p de orden una potencia de p, por la proposición 1.20. Por tanto, $H_{p,1} = \{\mathrm{id}\}$ necesariamente, luego $H_{p,u} = \{\mathrm{id}\}$ para todo $u \geq 1$. Concluimos que

$$n(p, \det\rho) = \frac{\dim(U/U_{p,0})}{[H_{p,0} : H_{p,0}]} = 1 - \dim(U_{p,0}) \leq 1,$$

como queríamos. □

Estas dos últimas proposiciones implican que $\mathfrak{f}(\det\rho)$ divide a $pN(\rho)$ y por tanto podemos identificar $\det\rho$ con un carácter de Dirichlet $\det\rho\colon (\mathbb{Z}/pN(\rho)\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$. Como $N(\rho)$ es coprimo con p, entonces $(\mathbb{Z}/pN(\rho)\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/N(\rho)\mathbb{Z})^\times$ por el teorema chino del resto. Así, obtenemos dos caracteres

$$\eta\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times \text{ y } \varepsilon\colon (\mathbb{Z}/N(\rho)\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times,$$

que verifican $\det\rho = \varepsilon\,\eta$. Es más, el carácter η es moderado por la proposición 2.5, y podemos verlo como un carácter de I_p^{tame} de nivel 1. Por tanto, $\eta = \chi_p^h$, siendo χ_p el carácter ciclotómico de módulo p, y $h \in \mathbb{Z}/(p-1)\mathbb{Z}$. Concluimos que

$$\det\rho = \varepsilon\chi_p^h, \text{ con } h \in \mathbb{Z}/(p-1)\mathbb{Z}. \tag{5.4}$$

Recordemos la observación 4.3: si ρ proviene de una autoforma de peso $k \geq 2$ y carácter ε entonces $\det\rho = \varepsilon\chi_p^{k-1}$. Comparando esta expresión con (5.4), estamos motivados a dar la siguiente definición.

Definición 5.3. Se define el *carácter de Serre asociado a* ρ como el carácter $\varepsilon(\rho)$ dado por la restricción de $\det\rho$ a $(\mathbb{Z}/N(\rho)\mathbb{Z})^\times$.

5.3. El peso $k(\rho)$

Finalmente, dedicamos esta sección a definir el peso $k(\rho)$. Mientras que $N(\rho)$ depende de la ramificación de ρ fuera de p, el peso $k(\rho)$ depende de la ramificación de $\rho_p\colon G_{\mathbb{Q}_p} \to \mathrm{Aut}(V)$.

Sea ρ_p^{ss} la semisimplificación de ρ_p. La representación ρ_p^{ss} es moderada por la proposición 2.5, es decir, $\rho_p^{ss}(I_p^{\mathrm{wild}}) = \{\mathrm{id}\}$. Como $I_p^{\mathrm{tame}} = I_p/I_p^{\mathrm{wild}}$ entonces la representación $\rho_p^{ss}|_{I_p}$ induce una representación

$$\rho_{\mathrm{t}}^{ss}\colon I_p^{\mathrm{tame}} \to \mathrm{Aut}(V^{ss}),$$

de modo que el siguiente diagrama

$$\begin{array}{ccc} I_p & \xrightarrow{\rho_p^{ss}|_{I_p}} & \mathrm{Aut}(V^{ss}) \\ & \searrow \quad \nearrow_{\rho_{\mathrm{t}}^{ss}} & \\ & I_p^{\mathrm{tame}} & \end{array}$$

es conmutativo, y por tanto, $\rho_{\mathrm{t}}^{ss}(I_p^{\mathrm{tame}}) = \rho_p^{ss}(I_p)$. Por la proposición 1.17, $I_p^{\mathrm{tame}} \cong \varprojlim_n \mathbb{F}_{p^n}^{\times}$, luego ρ_{t}^{ss} factoriza por un subgrupo cíclico de I_p^{tame} de orden coprimo con p. Por tanto, ρ_{t}^{ss} es semisimple por el teorema de ver Maschke[2], y es reducible por el teorema de descomposición de Jordan-Chevalley[3]. Se sigue que, después de elegir una base adecuada, podemos expresar

$$\rho_p^{ss}|_{I_p} = \rho_{\mathrm{t}}^{ss} = \begin{pmatrix} \phi_1 & 0 \\ 0 & \phi_2 \end{pmatrix}, \tag{5.5}$$

siendo $\phi_1, \phi_2 \colon I_p^{\mathrm{tame}} \to \overline{\mathbb{F}}_p^{\times}$ dos caracteres.

Proposición 5.3. Los caracteres ϕ_1 y ϕ_2 son de nivel 1 o de nivel 2, simultáneamente.

Demostración. Sea $s = \mathrm{Frob}_p \in G_{\mathbb{Q}_p}$, y denotemos $M = \rho_{\mathrm{t}}^{ss}(s)$. Por la proposición 1.18 y por ser $\rho_{\mathrm{t}}^{ss}(I_p^{\mathrm{tame}})$ abeliano, se sigue que

$$M\rho_{\mathrm{t}}^{ss}(u)M^{-1} = \rho_{\mathrm{t}}^{ss}(sus^{-1}) = \rho_{\mathrm{t}}^{ss}(u^p) = (\rho_{\mathrm{t}}^{ss})^p(u) \text{ para todo } u \in I_p^{\mathrm{tame}}.$$

Es decir, $\rho_{\mathrm{t}}^{ss} \cong (\rho_{\mathrm{t}}^{ss})^p$. Como ρ_{t}^{ss} viene dada por una matriz diagonal y al conjugarla por M obtenemos una matriz diagonal, entonces sólo se dan dos casos:

- $(\rho_{\mathrm{t}}^{ss})^p = \begin{pmatrix} \phi_1^p & 0 \\ 0 & \phi_2^p \end{pmatrix}$. Tenemos $\phi_1^p = \phi_1$ y $\phi_2 = \phi_2^p$, luego los caracteres son de nivel 1.
- $(\rho_{\mathrm{t}}^{ss})^p = \begin{pmatrix} \phi_2^p & 0 \\ 0 & \phi_1^p \end{pmatrix}$. Ahora, $\phi_1^p = \phi_2$ y $\phi_2^p = \phi_1$, luego los caracteres son de nivel 2 ya que $\phi_1 = \phi_2^p = (\phi_1^p)^p = \phi_1^{p^2}$ y $\phi_2 = \phi_1^p = (\phi_2^p)^p = \phi_2^{p^2}$. □

En el resto de la sección, definiremos $k(\rho)$ en función de la acción de I_p^{wild} en V y del nivel de los caracteres ϕ_1 y ϕ_2. Denotemos ψ y ψ' a los caracteres fundamentales de nivel 2, siendo $\psi' = \psi^p$, y denotemos χ al único carácter fundamental de nivel 1, es decir, al carácter de I_p^{tame} inducido por el carácter ciclotómico χ_p (ver observación 2.1).

5.3.1. Caso supersingular

Supongamos que ϕ_1 y ϕ_2 son de nivel 2. Entonces podemos expresar ϕ_1 como

$$\phi_1 = \psi^{a+pb} = \psi^a\,(\psi^p)^b = \psi^a\,\psi'^b, \text{ con } 0 \le a, b \le p-1.$$

Observemos que $a \neq b$. De lo contrario, $\phi_1 = (\psi\,\psi^p)^a = \chi^a$ por la proposición 2.6. Esto es absurdo pues χ es de nivel 1, pero ϕ_1 es de nivel 2. Por tanto, podemos suponer sin pérdida de generalidad que $a < b$. Volviendo a utilizar la proposición 2.6, tenemos que

$$\phi_1 = \psi^a\,\psi'^b = \psi^a\,\psi'^{b-a+a} = \psi^a\,\psi'^a\,\psi'^{b-a} = \chi^a\,\psi'^{b-a}.$$

Teniendo en cuenta que $\chi^p = \chi$ y que $\psi'^{p^2} = \psi$, se sigue que ϕ_2 es de la forma

$$\phi_2 = \phi_1^p = (\chi^a\,\psi'^{b-a})^p = \chi^a\,\psi^{b-a}.$$

[2]Ver teorema 2.1.6 de [Wie08].
[3]Ver página 17, sección 4.2 de [Hum12].

Así, de (5.5) se sigue que

$$\rho_p^{ss}|_{I_p} = \rho_{\mathrm{t}}^{ss} = \begin{pmatrix} \chi^a\,\psi'^{b-a} & 0 \\ 0 & \chi^a\,\psi^{b-a} \end{pmatrix}. \tag{5.6}$$

Lema 5.2. La representación $\rho_p\colon G_{\mathbb{Q}_p} \to \mathrm{Aut}(V)$ es irreducible.

Demostración. Por reducción al absurdo, supongamos que existe un subespacio $W \subset V$ de dimensión 1 invariante por la acción de $G_{\mathbb{Q}_p}$. Es decir, ρ_p actúa en W como un carácter

$$\Phi\colon G_{\mathbb{Q}_p} \to \mathrm{Aut}(W).$$

Como Φ es irreducible, entonces es moderado por la proposición 2.5, e induce un carácter

$$\Phi_{\mathrm{t}}\colon I_p^{\mathrm{tame}} \to \mathrm{Aut}(W) \cong \overline{\mathbb{F}}_p^{\times}$$

que debe coincidir con ϕ_1 o con ϕ_2. Sea $s = \mathrm{Frob}_p \in G_{\mathbb{Q}_p}$. Como la imagen de Φ_{t} es un grupo abeliano, se sigue de la proposición 1.18 que

$$\Phi_{\mathrm{t}}(u) = \Phi_{\mathrm{t}}(sus^{-1}) = \Phi_{\mathrm{t}}(u^p) = \Phi_{\mathrm{t}}^p(u) \text{ para todo } u \in I_p^{\mathrm{tame}}.$$

Es decir, Φ_{t} es un carácter de nivel 1. Esto es absurdo, pues ϕ_1 y ϕ_2 son de nivel 2. □

De este lema, deducimos que $\rho_p|_{I_p} = \rho_p^{ss}|_{I_p}$. Por tanto, de (5.6) se sigue que

$$\rho_p|_{I_p} = \begin{pmatrix} \chi^a\,\psi'^{b-a} & 0 \\ 0 & \chi^a\,\psi^{b-a} \end{pmatrix} = \chi^a \otimes \begin{pmatrix} \psi'^{b-a} & 0 \\ 0 & \psi^{b-a} \end{pmatrix}.$$

Observemos que esta representación es similar a un twist por χ^a de una representación irreducible asociada a una autoforma cuspidal con coeficientes en $\overline{\mathbb{F}}_p$, como en el teorema de Fontaine. Recordando la proposición 4.2 y teniendo en cuenta que cada twist por χ añadiría $p+1$ al peso de la autoforma, estamos motivados a dar la siguiente definición.

Definición 5.4. Si los caracteres ϕ_1 y ϕ_2 son de nivel 2, se define el *peso de Serre asociado a* ρ como

$$k(\rho) = 1 + b - a + a(p+1) = 1 + pa + b.$$

5.3.2. Caso ordinario moderado

Supongamos que ϕ_1 y ϕ_2 son de nivel 1 y que $\rho_p(I_p^{\mathrm{wild}}) = \{\mathrm{id}\}$. Razonando como en el inicio de la sección, $\rho_p(I_p^{\mathrm{wild}}) = \{\mathrm{id}\}$ implica que $\rho_p|_{I_p} = \rho_{\mathrm{t}}^{ss}$. Por otro lado, como ϕ_1 y ϕ_2 son de nivel 1, podemos expresar

$$\phi_1 = \chi^a \;\text{ y }\; \phi_2 = \chi^b, \text{ con } 0 \le a, b \le p-2.$$

Reordenando si es necesario, podemos suponer que $a \le b$. Por tanto,

$$\rho_p|_{I_p} = \begin{pmatrix} \chi^b & 0 \\ 0 & \chi^a \end{pmatrix} = \chi^a \otimes \begin{pmatrix} \chi^{b-a} & 0 \\ 0 & 1 \end{pmatrix}.$$

Comparando este resultado con el teorema de Deligne y razonando igual que en el caso supersingular, estamos motivados a dar la siguiente definición.

Definición 5.5. Si los caracteres ϕ_1 y ϕ_2 son de nivel 1 y ρ_p es moderada, se define el *peso de Serre asociado a* ρ como

$$k(\rho) = \begin{cases} 1 + pa + b & \text{si } (a,b) \neq (0,0), \\ p & \text{si } (a,b) = (0,0). \end{cases}$$

Observación. Notemos que si $a = b = 0$ entonces $k(\rho)$ sería 1 según la primera fórmula, pero el teorema 4.1 sólo considera autoformas con peso mayor o igual que 2.

5.3.3. Caso ordinario salvaje

Supongamos que $\rho_p(I_p^{\text{wild}}) \neq \{\text{id}\}$. Por la proposición 2.1, $V^{I_p^{\text{wild}}}$ y $V/V^{I_p^{\text{wild}}}$ son espacios invariantes por la acción de $G_{\mathbb{Q}_p}$. Sabemos que $V^{I_p^{\text{wild}}} \neq \{\mathbf{0}\}$ por el lema 2.1, y como $V \neq V^{I_p^{\text{wild}}}$, entonces necesariamente $\dim V^{I_p^{\text{wild}}} = 1$. Se sigue que $\dim V/V^{I_p^{\text{wild}}} = 1$ también. En otras palabras, $G_{\mathbb{Q}_p}$ actúa en cada espacio como un carácter, y podemos expresar

$$\rho_p = \begin{pmatrix} \theta_2 & * \\ 0 & \theta_1 \end{pmatrix}, \text{ siendo } \theta_1, \theta_2 \colon G_{\mathbb{Q}_p} \to \overline{\mathbb{F}}_p^{\times} \text{ dos caracteres.}$$

Como θ_1 y θ_2 son irreducibles, entonces son moderados por la proposición 2.5, e inducen dos caracteres

$$\gamma_1, \gamma_2 \colon I_p^{\text{tame}} \to \overline{\mathbb{F}}_p^{\times}$$

tales que $\gamma_i(I_p^{\text{tame}}) = \theta_i(I_p)$ para $i = 1, 2$.

Lema 5.3. Los caracteres γ_1 y γ_2 son de nivel 1.

Demostración. Sea $s = \text{Frob}_p \in G_{\mathbb{Q}_p}$. Para $i = 1, 2$, la imagen de γ_i es abeliana, luego se sigue de la proposición 1.18 que $\gamma_i(u) = \gamma_i(sus^{-1}) = \gamma_i^p(u)$ para todo $u \in I_p^{\text{tame}}$. Concluimos que γ_i es un carácter de nivel 1 para $i = 1, 2$. □

Por el lema anterior, para todo $\sigma \in I_p$, se verifica que

$$\theta_1(\sigma) = \gamma_1([\sigma]) = \chi^{\alpha}([\sigma]) \text{ y } \theta_2(\sigma) = \gamma_2([\sigma]) = \chi^{\beta}([\sigma]), \text{ con } \alpha, \beta \in \mathbb{Z}/(p-1)\mathbb{Z},$$

donde $[\sigma]$ denota la clase de σ en I_p^{tame}, y por tanto,

$$\rho_p|_{I_p} = \begin{pmatrix} \chi^{\beta} & * \\ 0 & \chi^{\alpha} \end{pmatrix}, \text{ con } \alpha, \beta \in \mathbb{Z}/(p-1)\mathbb{Z}.$$

Elegimos representantes de α y β tales que $0 \leq \alpha \leq p-2$ y $1 \leq \beta \leq p-1$. Para definir el peso $k(\rho)$, distinguimos los siguientes casos:

Caso $\beta \neq \alpha + 1$ Razonamos igual en el caso ordinario moderado. Es decir, se define el *peso de Serre asociado a* ρ como

$$k(\rho) = 1 + pa + b,$$

siendo $a = \text{mín}\{\alpha, \beta\}$ y $b = \text{máx}\{\alpha, \beta\}$.

Observación. Los representantes α y β se han elegido así para que en el caso $\chi^\alpha = \chi^\beta = 1$ tengamos que elegir $\alpha = 0$ y $\beta = p-1$, y así obtener $k(\rho) = p$ en lugar de $k(\rho) = 1$.

Caso $\beta = \alpha + 1$ Ahora, la acción de I_p en V viene dada por

$$\rho_p|_{I_p} = \begin{pmatrix} \chi^{\alpha+1} & * \\ 0 & \chi^\alpha \end{pmatrix} = \chi^\alpha \otimes \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}. \tag{5.7}$$

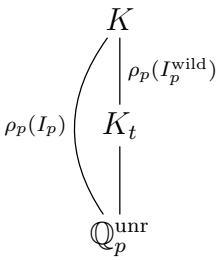
Por tanto, no está claro si la autoforma asociada a la representación antes de hacer el twist por χ^α tiene peso 2 o $p+1$, pues $\chi^2 = \chi^{p+1}$. Para determinarlo, estudiaremos el cociente $\rho_p(I_p)/\rho_p(I_p^{\text{wild}})$. Por la proposición 2.5, χ es moderado, luego

$$\rho_p|_{I_p^{\text{wild}}} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Por otro lado, sea $K = \overline{\mathbb{Q}}_p^{\ker \rho_p}\mathbb{Q}_p^{\text{unr}}$, y sea K_t la máxima subextensión moderada de $K/\mathbb{Q}_p^{\text{unr}}$, es decir, $K_t = K \cap \mathbb{Q}_p^{\text{tame}}$. Observemos que, por el teorema 2.2, $\overline{\mathbb{Q}}_p^{\ker \rho_p}/\mathbb{Q}_p$ es una extensión finita de Galois. Por tanto, los resultados de la sección 1.4 y el teorema 1.3 implican que $K/\mathbb{Q}_p^{\text{unr}}$ y K/K_t son extensiones finitas de Galois tales que

$$\rho_p(I_p) \cong \text{Gal}(K/\mathbb{Q}_p^{\text{unr}}) \text{ y } \rho_p(I_p^{\text{wild}}) \cong \text{Gal}(K/K_t),$$

Tenemos el siguiente diagrama de extensiones y sus correspondientes grupos de Galois:



Lema 5.4. El cociente $\rho_p(I_p)/\rho_p(I_p^{\text{wild}})$ es isomorfo a $(\mathbb{Z}/p\mathbb{Z})^\times$.

Demostración. Como $\chi(I_p^{\text{tame}}) = \mathbb{F}_p^\times$, entonces

$$\rho_p(I_p) \subset \left\{ \begin{pmatrix} z^{\alpha+1} & * \\ 0 & z^\alpha \end{pmatrix} \in \text{GL}_2(\overline{\mathbb{F}}_p) : z \in \mathbb{F}_p^\times \right\}.$$

Consideramos el homomorfismo $\delta\colon \rho_p(I_p) \to (\mathbb{Z}/p\mathbb{Z})^\times$ definido por

$$\begin{pmatrix} z^{\alpha+1} & * \\ 0 & z^\alpha \end{pmatrix} \mapsto \frac{z^{\alpha+1}}{z^\alpha}.$$

Dado que toda matriz de $\rho_p(I_p)$ es de la forma

$$\begin{pmatrix} \chi^{\alpha+1}(\sigma) & * \\ 0 & \chi^\alpha(\sigma) \end{pmatrix} \text{ con } \sigma \in I_p^{\text{tame}},$$

entonces $\delta\left(\rho_p(I_p)\right) = \chi(I_p^{\text{tame}})$, y deducimos que δ es sobreyectivo. Veamos que $\ker\delta = \rho_p(I_p^{\text{wild}})$. En efecto, $M \in \ker\delta$ si y sólo si

$$M = \begin{pmatrix} z^{\alpha+1} & * \\ 0 & z^{\alpha} \end{pmatrix} \text{ con } z \in \mathbb{F}_p^{\times} \text{ y } \delta(M) = z = 1 \in \mathbb{F}_p^{\times}.$$

Equivalentemente, la diagonal de M es $(1,1)$, y por tanto $M \in \rho_p(I_p^{\text{wild}})$. Concluimos que $\ker\delta = \rho_p(I_p^{\text{wild}})$. Finalmente, por el primer teorema de isomorfía de Noether,

$$\rho_p(I_p)/\ker\delta = \rho_p(I_p)/\rho_p(I_p^{\text{wild}}) \cong (\mathbb{Z}/p\mathbb{Z})^{\times},$$

como queríamos. □

El lema anterior junto con el teorema de correspondencia de Galois implican que

$$\rho_p(I_p)/\rho_p(I_p^{\text{wild}}) \cong \text{Gal}(K_t/\mathbb{Q}_p^{\text{unr}}) \cong (\mathbb{Z}/p\mathbb{Z})^{\times}. \tag{5.8}$$

Por otro lado, $\zeta_p \in \mathbb{Q}_p^{\text{tame}}$, luego $\zeta_p \in K_t$. Además, como $[K_t : \mathbb{Q}_p^{\text{unr}}] = p-1$ por (5.8), entonces $K_t = \mathbb{Q}_p^{\text{unr}}(\zeta_p)$.

Dado que $\rho_p(I_p^{\text{wild}})$ es un grupo de orden una potencia de p, abeliano y finito, entonces

$$\rho_p(I_p^{\text{wild}}) \cong \mathbb{Z}/p\mathbb{Z} \underbrace{\times \cdots \times}_{m \text{ veces}} \mathbb{Z}/p\mathbb{Z},$$

y por tanto K se obtiene como el compositum de m extensiones cíclicas de K_t de grado p. Aplicando m veces el teorema central de la teoría de Kummer[4], se sigue que existen $x_1, \ldots, x_m \in K_t$ tales que

$$K = K_t\left(x_1^{1/p}, \ldots, x_m^{1/p}\right) \text{ con } p^m = [K : K_t].$$

De hecho, si denotamos $K_0 = \mathbb{Q}_p^{\text{unr}}$ y teniendo en cuenta que $K_t = K_0(\zeta_p)$, siempre podemos tomar x_i en $K_0^{\times}/(K_0^{\times})^p$ para todo $i = 1, \ldots, m$. Sin embargo, para poder probar esto, se necesitan algunos resultados de cohomología de Galois que están fuera del alcance de este trabajo. Aún así, la explicación de este hecho se puede encontrar en el siguiente post: [mar].

Definición 5.6. En las condiciones anteriores, se dice que ρ_p es *poco ramificada* si

$$v_p(x_i) \equiv 0 \text{ mód } p \text{ para todo } i = 1, \ldots, m,$$

donde v_p denota la extensión de v_p a K_0. De lo contrario, se dice que ρ_p es *muy ramificada*.

Teorema 5.3 (Mazur). *Para todo primo $p \neq 2$, sea $f \in \widetilde{S}_{p+1}(N, \varepsilon)$ una autoforma tal que la representación asociada ρ_f es irreducible. Entonces, $\rho_f|_{G_{\mathbb{Q}_p}}$ es muy ramificada.*

[4] Este teorema es el siguiente: Sean n un entero positivo, y K un cuerpo cuya característica no divida a n y tal que $\zeta_n \in K$. Si L/K es una extensión de Galois tal que $\text{Gal}(L/K)$ es cíclico de orden n, entonces $L = K(\sqrt[n]{c})$ para algún $c \in K$.

Demostración. Ver teorema 2.8 de [Edi92]. □

Por (5.7), tenemos que $\rho_p|_{I_p} = \chi^\alpha \otimes \rho'_p|_{I_p}$, donde

$$\rho'_p|_{I_p} = \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}.$$

Supongamos que ρ proviene de una autoforma cuspidal f, y por tanto, $\rho'_p|_{I_p}$ es la restricción a I_p de la representación asociada a una autoforma cuspidal f'. Se define *peso de Serre* $k(\rho)$ asociado a ρ como sigue:

1. Si ρ_p es muy ramificada y $p \neq 2$, el teorema de Mazur sugiere que f' tiene peso $p+1$. Por tanto, se define
$$k(\rho) = (p+1) + \alpha(p+1) = (\alpha+1)(p+1).$$
2. Si ρ_p es muy ramificada y $p = 2$, el peso de f' debería ser 3 según el razonamiento anterior, pero no existen tales autoformas. En este caso, se define $k(\rho) = 4$.
3. Por último, si ρ_p es poco ramificada, entonces f' tendría peso 2, y se define
$$k(\rho) = 2 + \alpha(p+1).$$

6 Ejemplo y último teorema de Fermat

6.1. Ejemplo numérico

Sea K el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $g(x) = x^4 - 4x^2 + 5$. Este polinomio es irreducible sobre $\mathbb{Q}$ por el criterio de Eisenstein, y como la ecuación $g(x) = 0$ es bicuadrada, obtenemos fácilmente las raíces de g, que son

$$\alpha_1 = \sqrt{2+i}, \quad \alpha_2 = \sqrt{2-i}, \quad \alpha_3 = -\alpha_1, \quad \alpha_4 = -\alpha_2.$$

Por tanto, $K = \mathbb{Q}(\alpha_1, \alpha_2)$. Calculemos el grupo de Galois $G = \mathrm{Gal}(K/\mathbb{Q})$. Tenemos las extensiones de cuerpos

$$\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subset K.$$

Como g es irreducible, entonces $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 4$, y como $\alpha_1\alpha_2 = \sqrt{5}$, se sigue que $[K : \mathbb{Q}(\alpha_1)] \leq 2$. Además, todo automorfismo de K tal que $\alpha_1 \mapsto \alpha_j$, debe verificar $\alpha_3 \mapsto -\alpha_j$, para $j \in \{1, 2, 3, 4\}$. Por tanto, $G \subset D_8$, siendo D_8 el grupo diédrico de orden 8 generado por las permutaciones

$$(\alpha_1, \alpha_2) \overset{\sigma}{\mapsto} (\alpha_2, -\alpha_1) \quad \text{y} \quad (\alpha_1, \alpha_2) \overset{\tau}{\mapsto} (\alpha_1, -\alpha_2).$$

En particular, G sólo puede ser D_8, $C_4 = \langle\sigma\rangle$ o $C_2 \times C_2 = \langle\sigma^2, \tau\rangle$, donde C_n denota el grupo cíclico de orden n, para todo entero positivo n. Veamos que $G = D_8$. En efecto, consideremos el subgrupo $H = \langle\sigma^2\rangle \subset D_8$, y observemos que H también es subgrupo de C_4 y de $C_2 \times C_2$. Por tanto, σ^2 se extiende a un automorfismo de K tal que

$$(\alpha_1, \alpha_2) \overset{\sigma^2}{\longmapsto} (-\alpha_1, -\alpha_2),$$

y podemos considerar el cuerpo fijo K^H. Notemos que σ^2 fija $\alpha_1^2 = 2 + i$ y $\alpha_1\alpha_2 = \sqrt{5}$, luego $\mathbb{Q}(\sqrt{5}, 2+i) = \mathbb{Q}(\sqrt{5}, i) \subset K^H$, y tenemos las extensiones de cuerpos

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}, i) \subset K^H \subset K,$$

Dado que $[\mathbb{Q}(\sqrt{5}, i) : \mathbb{Q}] = 4$ y $[K : K^H] = 2$, entonces $[K : \mathbb{Q}] = 8$, y concluimos que

$$G = D_8 = \langle\sigma, \tau\rangle.$$

Vamos a construir una representación de Galois $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$, siendo p un primo no ramificado en $K/\mathbb{Q}$. El discriminante de K es $\Delta_K = 2^{16} \cdot 5^4$, luego $K/\mathbb{Q}$ es no ramificada en todo primo p tal que $p \notin \{2, 5\}$. Por ejemplo, tomemos $p = 3$. Definimos el homomorfismo $G \to \mathrm{GL}_2(\mathbb{F}_3)$ dado por

$$\sigma \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Así, obtenemos una representación de Galois irreducible

$$\rho\colon G_{\mathbb{Q}} \to G \to \mathrm{GL}_2(\mathbb{F}_3).$$

Después de fijar una $\mathbb{Q}$-inclusión $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, podemos considerar la conjugación compleja $c \in G_{\mathbb{Q}}$, que se restringe a un automorfismo en K. Observemos que

$$(\alpha_1, \alpha_2) \overset{c}{\mapsto} (\alpha_2, \alpha_1),$$

luego $c = \sigma \circ \tau$, y por tanto

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

Concluimos que ρ es impar pues $\det \rho(c) = -1$. Por tanto, podemos aplicar la conjetura de modularidad de Serre a la representación ρ. Vamos a calcular $N(\rho)$, $k(\rho)$ y $\varepsilon(\rho)$.

Para hallar $N(\rho)$, calculamos con SageMath el u-ésimo grupo de ramificación $G_{\ell,u}$ con numeración baja para $\ell \in \{2, 5\}$ y para $u \geq 0$. Para $\ell = 2$, obtenemos:

$$G_{2,0} \cong G_{2,1} \cong C_2 \times C_2, \quad G_{2,2} \cong G_{2,3} \cong C_2, \text{ y } G_{2,4} = \{\mathrm{id}\}.$$

Los subespacios de $V = \mathbb{F}_3^2$ fijos por estos grupos son:

$$V_{2,0} = V_{2,1} = V_{2,2} = V_{2,3} = \{\mathbf{0}\}$$

Por tanto,

$$n(2, \rho) = \sum_{u=0}^{4} \frac{\dim(V/V_{2,u})}{[G_{2,0} : G_{2,u}]} = 6.$$

Análogamente, para $\ell = 5$, obtenemos:

$$G_{5,0} \cong C_2, \quad G_{5,1} = \{\mathrm{id}\}, \text{ y } V_{5,0} = \langle (0,1) \rangle,$$

y se sigue que

$$n(5, \rho) = \dim(V/V_{5,0}) = 2 - \dim(V_{5,0}) = 1.$$

Concluimos que $N(\rho) = 2^6 \cdot 5 = 320$. Además, como ρ es no ramificada en $p = 3$, estamos en el caso ordinario moderado del capítulo anterior, y por tanto, $k(\rho) = 3$. Como la imagen de $\det \rho$ es $\mathbb{F}_3^\times \cong (\mathbb{Z}/2\mathbb{Z})$, entonces $\varepsilon(\rho)$ es un carácter de Dirichlet $\varepsilon\colon (\mathbb{Z}/320\mathbb{Z})^\times \to \overline{\mathbb{F}}_3^\times$ de orden 2. Sea $\varepsilon_0\colon (\mathbb{Z}/320\mathbb{Z})^\times \to \overline{\mathbb{Z}}^\times$ el único carácter tal que $\widetilde{\varepsilon_0(x)} = \varepsilon(x)$ para todo $x \in (\mathbb{Z}/320\mathbb{Z})^\times$, donde $z \mapsto \widetilde{z}$ denota el homomorfismo reducción $\overline{\mathbb{Z}} \to \overline{\mathbb{F}}_3$.

Sea $f \in \widetilde{\mathcal{S}}_3(320, \varepsilon)$ la autoforma normalizada asociada a ρ, y denotemos $a_n(f)$ a sus coeficientes de Fourier. Para hallar las autoformas en $\mathcal{S}_3(320, \varepsilon_0)$ cuyos coeficientes de Fourier están en $\overline{\mathbb{Z}}$ y tales que ε_0 tiene orden 2, utilizaremos la base de datos [LMFDB]. Una búsqueda revela que hay 15 autoformas con estas características. Veamos cuál de ellas se corresponde con f.

Para ello, supongamos que ℓ es un primo tal que $\mathfrak{l} = \ell\mathcal{O}_K$ se descompone totalmente en $K/\mathbb{Q}$. Entonces, el cuerpo de residuos $k_\mathfrak{l}$ coincide con $\mathbb{F}_\ell$, y por tanto, $\rho(\mathrm{Frob}_\ell) = \mathrm{id}$. En particular, $\operatorname{tr}\rho(\mathrm{Frob}_\ell) = 2$, y por el teorema 4.1,

$$\operatorname{tr}\rho(\mathrm{Frob}_\ell) = a_\ell(f) = 2 \text{ en } \overline{\mathbb{F}}_3.$$

Los primeros siete primos ℓ tales que $\mathfrak{l}$ se descompone totalmente en $K/\mathbb{Q}$ son

$$D = \{61, 89, 109, 149, 269, 389, 401\}.$$

Por tanto, de las 15 autoformas mencionadas anteriormente, podemos descartar toda autoforma F tal que

$$a_\ell(F) \not\equiv 2 \text{ mód } 3 \text{ para todo } \ell \in D,$$

donde $a_\ell(F)$ denota el ℓ-ésimo coeficiente de Fourier de F. Una búsqueda en la [LMFDB], revela que podemos descartar todas las autoformas salvo la que tiene etiqueta 320.3.h.e, cuya q-expansión es

$$\begin{aligned} F(q) = {} & 4q + 4q^5 - 4q^9 - 96q^{21} - 92q^{25} + 88q^{29} + 88q^{41} - 4q^{45} + \\ & 92q^{49} - 184q^{61} - 192q^{65} + 288q^{69} - 284q^{81} - 384q^{85} + 584q^{89} + \mathcal{O}(q^{100}). \end{aligned}$$

La reducción módulo 3 de los coeficientes de Fourier de F nos da la q-expansión de f:

$$f(q) = q + q^5 - q^9 + q^{25} - 2q^{29} - 2q^{41} - q^{45} - q^{49} + 2q^{61} + q^{81} + 2q^{89} + \mathcal{O}(q^{100}). \quad (6.1)$$

En realidad, es posible modificar la definición de formas cuspidales módulo un primo p, de modo que podemos considerar autoformas de peso 1. Para ver la definición, se puede consultar la sección 2 de [Edi92]. Con esta definición, el peso de Serre en este ejemplo sería $k(\rho) = 1$. En efecto, la autoforma con etiqueta 320.1.h.a tiene nivel 320, peso 1 y carácter ε_0 de orden 2, y su q-expansión es exactamente la de (6.1). En particular, la reducción módulo 3 de sus coeficientes de Fourier coincide con los coeficientes de Fourier de f.

Por último, cabe destacar que este es un ejemplo de congruencia entre dos autoformas, una teoría que juega un papel central en la demostración de la conjetura de modularidad de Serre.

6.2. Último teorema de Fermat

Teorema 6.1 (Último teorema de Fermat)**.** *Para todo entero $n \geq 3$, la ecuación*

$$x^n + y^n = z^n \quad (6.2)$$

no tiene soluciones enteras no triviales.[1]

[1] Una solución no trivial es una solución (a, b, c) de (6.2) tal que $abc \neq 0$.

Según [Rib08], el caso $n = 3$ fue demostrado por Leonard Euler en 1770, y el caso $n = 4$ fue demostrado por el propio Fermat, aproximadamente en 1670. Por ello, podemos suponer que $n \geq 5$. Veamos que además podemos suponer que n es primo. En efecto, existen tres posibilidades: o bien $3 \mid n$, o bien $4 \mid n$, o bien $p \mid n$, siendo p un primo mayor o igual que 5. En el primer caso, existe un entero k tal que $n = 3k$. Si existiera una solución entera no trivial (a, b, c) de (6.2), entonces (a^k, b^k, c^k) es una solución entera no trivial de la ecuación

$$x^3 + y^3 = z^3,$$

lo cual es absurdo. Si $4 \mid n$, se razona de manera análoga. Aplicando el mismo argumento para el caso $p \mid n$, se deduce que basta probar el teorema cuando $n = p$, siendo p un primo mayor o igual que 5.

Por reducción al absurdo, supongamos que (a, b, c) es una solución entera no trivial de la ecuación

$$x^p + y^p = z^p, \text{ con } p \geq 5 \text{ primo.} \tag{6.3}$$

Como la ecuación (6.3) es homogénea, podemos suponer que a, b, c son coprimos dos a dos. Además, uno de ellos debe ser necesariamente par. Sin pérdida de generalidad, podemos suponer que b es par, que a y c son impares y que $a \equiv -1 \pmod 4$. Definimos las cantidades

$$A = a^p, \quad B = b^p, \quad \text{y} \quad C = c^p,$$

y consideramos la curva elíptica racional

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

El discriminante de E es $\Delta_E = 16(ABC)^2$, y $c_4 = 16(A^2 + AB + B^2)$.

Lema 6.1. La curva elíptica E es semiestable.

Demostración. Sea $\ell \geq 3$ un primo tal que $\ell \mid \Delta_E$. Si $\ell \mid A$ o $\ell \mid B$, entonces $\ell \nmid c_4$, pues $\gcd(A, B) = 1$. Por tanto, E tiene mala reducción multiplicativa en ℓ. Si $\ell \mid C$, entonces $C = A + B \equiv 0 \pmod \ell$, luego $c_4 \equiv 16A^2 \pmod \ell$. Por tanto, $\ell \nmid c_4$, y concluimos que E tiene mala reducción multiplicativa en ℓ.

Si $\ell = 2$, el cambio de variable $(x, y) \mapsto (4x, 8y + 4x)$, produce el siguiente modelo de Weierstrass para E:

$$E'\colon y^2 + xy = x^3 + \frac{B - A - 1}{4}\, x^2 - \frac{AB}{16}\, x.$$

Dado que $A = a^p \equiv -1 \pmod 4$ y que $B = b^p \equiv 0 \pmod{32}$, los coeficientes del modelo anterior son enteros. Además,

$$\Delta_{E'} = \frac{\Delta_E}{2^{12}} = \frac{(ABC)^2}{2^8} \quad \text{y} \quad c_4' = \frac{c_4}{2^4} = A^2 + AB + B^2.$$

En particular, $2 \mid \Delta_{E'}$ y $2 \nmid c_4'$, luego E tiene mala reducción multiplicativa en $\ell = 2$. □

A continuación, consideramos la representación de Galois

$$\overline{\rho}_{E,p}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

asociada a los puntos $E[p]$ de p-torsión de E.

Proposición 6.1. La representación $\overline{\rho}_{E,p}$ es irreducible.

Demostración. Los puntos de 2-torsión de E son

$$E[2] = \{(0,0), (-A,0), (B,0)\} \cup \{O_E\},$$

y todos ellos son racionales. Por tanto, $E(\mathbb{Q})_{\mathrm{tors}}$ tiene orden divisible por 4.

Por reducción al absurdo, supongamos que $\overline{\rho}_{E,p}$ es reducible. Entonces, por el teorema 3.4 y el lema anterior, E o una curva elíptica E' que es $\mathbb{Q}$-isógena a E tiene un punto de p-torsión racional. En el primer caso, $E(\mathbb{Q})_{\mathrm{tors}}$ tiene orden divisible por $p \geq 5$, luego $E(\mathbb{Q})_{\mathrm{tors}}$ tiene orden al menos $4p \geq 20$. Esto es absurdo por el teorema de torsión de Mazur. En el segundo caso, E' tiene un punto de p-torsión racional, y se razona igual que en el caso anterior, teniendo en cuenta que $E'(\mathbb{Q})_{\mathrm{tors}} \cong E(\mathbb{Q})_{\mathrm{tors}}$. □

Por otro lado, la representación $\overline{\rho}_{E,p}$ es impar por la proposición 3.7. Entonces, podemos aplicar la conjetura de modularidad de Serre. Comenzamos calculando el nivel de Serre $N(\overline{\rho}_{E,p})$.

Sea $\ell \neq p$ un primo. En primer lugar, supongamos que E tiene buena reducción en ℓ. Entonces, por la proposición 3.6, $\overline{\rho}_{E,p}$ es no ramificada en ℓ, y por tanto, $n(\ell, \overline{\rho}_{E,p}) = 0$. Por otro lado, supongamos que E tiene mala reducción multiplicativa en ℓ, y supongamos que $\ell \notin \{2, p\}$. Entonces, $\ell \mid \Delta_E$ y por tanto, $\ell \mid abc$. De aquí se sigue que

$$v_\ell(\Delta_E) = v_\ell\left(2^{-8}(abc)^{2p}\right) = 2pv_\ell(abc),$$

y como $v_\ell(abc) > 0$, entonces $v_\ell(\Delta_E) \equiv 0 \mod p$. Por el teorema 3.7, esto equivale a que $\overline{\rho}_{E,p}$ sea no ramificada en ℓ, y por tanto, $n(\ell, \overline{\rho}_{E,p}) = 0$.

Es decir, el único primo que aparece en el nivel de Serre $N(\overline{\rho}_{E,p})$ es 2. Se puede comprobar[2] que $n(2, \overline{\rho}_{E,p}) = 1$, y por tanto, el nivel de Serre asociado a $\overline{\rho}_{E,p}$ es $N(\overline{\rho}_{E,p}) = 2$.

El carácter de Serre asociado a $\overline{\rho}_{E,p}$ es $\varepsilon(\overline{\rho}_{E,p}) = 1$. Esto se debe a que $\det \overline{\rho}_{E,p} = \chi_p$, por la proposición 3.7.

Por último, el peso de Serre $k(\overline{\rho}_{E,p})$ viene dado por el siguiente teorema.

Teorema 6.2. *Sea $E/\mathbb{Q}$ una curva elíptica semiestable. Si E tiene buena reducción en p, entonces $k(\overline{\rho}_{E,p}) = 2$. Si E tiene mala reducción multiplicativa en p, entonces*

$$k(\overline{\rho}_{E,p}) = \begin{cases} 2 & \text{si } v_p(j_E) \equiv 0 \mod p, \\ p+1 & \text{si no.} \end{cases}$$

Demostración. Ver proposición 5 de [Ser87]. □

[2] Ver teorema 2.15d) de [DDT95].

Veamos que $k(\overline{\rho}_{E,p}) = 2$. Por el teorema anterior, basta suponer que E tiene mala reducción multiplicativa en p y demostrar que $v_p(j_E) \equiv 0 \mod p$. El j-invariante de E es

$$j_E = \frac{2^8(C^2 - AB)^3}{(ABC)^2}.$$

Si E tiene mala reducción en p, entonces $p \mid \Delta_E$, luego $p \mid abc$. Se puede comprobar que $p \nmid C^2 - AB$, luego

$$v_p(j_E) = -v_p\left((ABC)^2\right) = -v_p\left((abc)^{2p}\right) = -2pv_p(abc),$$

y como $v_p(abc) > 0$, entonces $v_p(j_E) \equiv 0 \mod p$. Por tanto, el peso de Serre asociado a $\overline{\rho}_{E,p}$ es $k(\overline{\rho}_{E,p}) = 2$. Sin embargo, no existe ninguna autoforma en $\widetilde{\mathcal{S}}_2(2,1)$, lo que concluye la demostración del último teorema de Fermat.

A Apéndice

A.1. Traza y norma

Sea L/K una extensión finita de cuerpos, con $[L:K]=n$, y tomemos una base $\{\mathbf{e}_1,\dots,\mathbf{e}_n\}$ de L como K-espacio vectorial. Dado $\alpha\in L$, consideremos el K-endomorfismo $m_\alpha\colon L\to L$, definido como $m_\alpha(x)=\alpha x$ para todo $x\in L$. Si $m_\alpha(\mathbf{e}_j)=\sum_{i=1}^n a_{ij}\mathbf{e}_j$ para todo $j=1,\dots,n$, la matriz de m_α respecto de la base $\{\mathbf{e}_1,\dots,\mathbf{e}_n\}$ viene dada por (a_{ij}).

Definición A.1. En el contexto anterior, se definen la *traza* y la *norma de* $\alpha\in L$, respectivamente, como

$$\mathrm{tr}_{L/K}(\alpha)=\sum_{i=1}^n a_{ii} \text{ y } N_{L/K}(\alpha)=\det(a_{ij}).$$

Observación. Como la traza y el determinante de la matriz de un K-endomorfismo $L\to L$ no dependen de la base de L elegida, la traza y la norma de un elemento de L tampoco.

El polinomio característico del endomorfismo m_α es

$$f_\alpha(t)=\det(t\,\mathrm{id}-(a_{ij}))=t^n-b_1t^{n-1}+\cdots+(-1)^nb_n\in K[t],$$

y la traza y la norma de $\alpha\in L$ se corresponden con los coeficientes b_1 y b_n, respectivamente.

Proposición A.1. Sea L/K una extensión de cuerpos separable, y fijemos una clausura algebraica $\overline{K}$ de K. Denotemos $\mathrm{Hom}_K(L,\overline{K})$ al conjunto de homomorfismos $L\to\overline{K}$ que fijan cada elemento de K. Entonces,

$$\mathrm{tr}_{L/K}(x)=\sum_{\sigma\in\mathrm{Hom}(L,\overline{K})}\sigma(x) \text{ y } N_{L/K}(x)=\prod_{\sigma\in\mathrm{Hom}(L,\overline{K})}\sigma(x).$$

Demostración. Ver página 9, proposición (2.6) de [Neu13]. □

A.2. Grupos topológicos

Definición A.2. Sean G un espacio topológico con estructura de grupo. Se dice que G es un *grupo topológico* si las aplicaciones

$$\begin{aligned} G\times G&\to G \\ (g_1,g_2)&\mapsto g_1g_2 \end{aligned} \qquad \text{y} \qquad \begin{aligned} G&\to G \\ g&\mapsto g^{-1} \end{aligned}$$

son continuas.

Definición A.3. Sean G y H dos grupos topológicos, y $\varphi\colon G\to H$ un homomorfismo de grupos. Se dice que φ es un *homomorfismo de grupos topológicos* si φ es una aplicación continua.

Proposición A.2. Sea G un grupo topológico.

1. Dado $g \in G$, la traslación $m_g \colon G \to G : h \mapsto gh$ es un homeomorfismo.[1]
2. Si $H \subset G$ es un subgrupo abierto, entonces H es cerrado.

Demostración. Sea $g \in G$. Está claro que m_g es un homomorfismo de grupos, y es biyectivo porque la función $m_{g^{-1}}$ es su inversa. Además, m_g es continua por ser la composición de

$$\begin{aligned} G \to G \times G \to G \\ h \mapsto (g, h) \mapsto gh, \end{aligned}$$

que son funciones continuas. Análogamente, $m_{g^{-1}}$ es continua por ser composición de funciones continuas, luego m_g es un homeomorfismo.

Por otro lado, sea $H \subset G$ un subgrupo abierto. Como las clases de H por la izquierda son de la forma $gH = m_g(H)$ para todo $g \in G$, entonces son abiertas. Dado que

$$G = H \cup \bigcup_{\substack{g \in G/H, \\ g \notin H}} gH$$

entonces H es el complementario del abierto $\bigcup_{\substack{g \in G/H, \\ g \notin H}} gH$, y por tanto, H es cerrado. □

Corolario A.1. Sean G y H grupos topológicos, y $\varphi \colon G \to H$ un homomorfismo de grupos. Entonces, φ es un homomorfismo de grupos topológicos si y sólo si φ es continua en id_G.

A.3. Límites inversos

Definición A.4. Un orden parcial $\leq$ en un conjunto I se dice *dirigido* si para todo $i, j \in I$ existe $k \in I$ tal que $i \leq k$ y $j \leq k$. En este caso, $(I, \leq)$ se llama *conjunto dirigido*.

Definición A.5. Sean $(I, \leq)$ un conjunto dirigido y $\mathscr{C}$ una categoría. Un *sistema inverso en* $\mathscr{C}$ *indexado por* $(I, \leq)$ consiste en una familia $(X_i)_{i \in I}$ de objetos de $\mathscr{C}$ junto con una familia $(\varphi_{ij} \colon X_j \to X_i)_{i \leq j}$ de morfismos de $\mathscr{C}$ tales que

- $\varphi_{ii} = \mathrm{id}_{X_i}$ para todo $i \in I$,
- $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$ para todo $i \leq j \leq k$ en I.

Un tal sistema inverso se denota (X_i, φ_{ij}) siempre que el conjunto dirigido $(I, \leq)$ esté especificado.

Definición A.6. Sean $(I, \leq)$ un conjunto dirigido, $\mathscr{C}$ una categoría, y (X_i, φ_{ij}) un sistema inverso in $\mathscr{C}$ indexado por $(I, \leq)$. Se define el *límite inverso de* (X_i, φ_{ij}) como el par (X, π_i), donde:

$$X = \left\{ (x_i)_{i \in I} \in \prod_{i \in I} X_i : x_i = \varphi_{ij}(x_j) \text{ para todo } i \leq j \text{ en } I \right\},$$

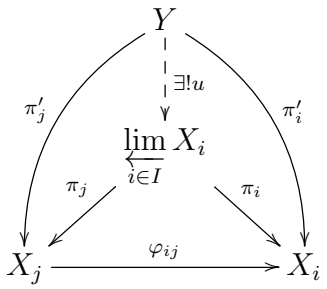
[1] Es decir, un homomorfismo biyectivo y continuo, y con inversa continua.

y $(\pi_i \colon X \to X_i)_{i\in I}$ es una familia de morfismos de $\mathscr{C}$ tal que

$$\pi_i = \varphi_{ij} \circ \pi_j \text{ para todo } i \leq j \text{ en } I.$$

El objeto X se denota $\varprojlim_{i\in I} X_i$, y los morfismos $(\pi_i)_{i\in I}$ se llaman *proyecciones de* $\varprojlim_{i\in I} X_i$.

El límite inverso de (X_i, φ_{ij}) verifica la siguiente propiedad universal: si Y es un objeto de $\mathscr{C}$ y $(\pi'_i \colon Y \to X_i)_{i\in I}$ es una familia de morfismos de $\mathscr{C}$ tal que $\pi'_i = \varphi_{ij} \circ \pi'_j$ para todo $i \leq j$ en I, entonces existe un único morfismo $u \colon Y \to X$ tal que el diagrama



es conmutativo para todo $i \leq j$ en I.

Observación. Si (X_i, φ_{ij}) es un sistema inverso indexado por un conjunto dirigido $(I, \leq)$ en la categoría de grupos topológicos, entonces $\prod_{i\in I} X_i$ está dotado de la topología producto. Además, en este caso, las proyecciones $(\pi_i)_{i\in I}$ de $\varprojlim_{i\in I} X_i$ son continuas.

Definición A.7. Sean $(I, \leq)$ un conjunto dirigido y $I' \subset I$. Se dice que I' es *cofinal en* I si para todo $i \in I$ existe $i' \in I'$ tal que $i \leq i'$.

Teorema A.1. *Sea (X_i, φ_{ij}) un sistema inverso en una categoría $\mathscr{C}$ indexado por un conjunto dirigido $(I, \leq)$. Si $I' \subset I$ es cofinal en I, entonces existe un isomorfismo canónico*

$$\varprojlim_{i\in I} X_i \cong \varprojlim_{i\in I'} X_i.$$

Demostración. Ver [Cla]. □

A.4. Valoraciones en un cuerpo

Continuamos con una introducción a la teoría de valoraciones en un cuerpo. Las referencias principales en las que se basa esta sección son el capítulo II de [Neu13] y el capítulo 7 de [Mil08].

Definición A.8. Sea K un cuerpo. Un *valor absoluto en* K es una función $|\cdot| \colon K \to \mathbb{R}$ tal que para todo $x, y \in K$ se verifica:

1. $|x| \geq 0$. Se tiene la igualdad si y sólo si $x = 0$,
2. $|xy| = |x|\,|y|$,
3. La desigualdad triangular: $|x + y| \leq |x| + |y|$.

Además, se dice que el valor absoluto $|\cdot|$ es *discreto* si $|K^\times| = s\mathbb{Z}$ para algún $s > 0$.

En cualquier cuerpo K, siempre podemos considerar el valor absoluto trivial, definido como $|x| = 1$ para todo $x \in K^\times$ y $|0| = 0$. De ahora en adelante, obviaremos el valor absoluto trivial, luego "valor absoluto"significará "valor absoluto no trivial", a no ser que se especifique lo contrario.

Definición A.9. Un valor absoluto $|\cdot|$ en un cuerpo K se dice *no arquimediano* si satisface la siguiente propiedad, llamada *propiedad ultramétrica*:

$$|x + y| \leq \max\{|x|, |y|\} \text{ para todo } x, y \in K.$$

De lo contrario, se dice que $|\cdot|$ es *arquimediano*.

Dado un valor absoluto $|\cdot|$ en un cuerpo K, podemos definir una distancia dada por $d(x, y) = |x - y|$ para todo $x, y \in K$. Así, (K, d) tiene estructura de espacio métrico, y por tanto, topológico.

Observación A.1. Supongamos que (K, d) es un espacio métrico con d una distancia inducida por un valor absoluto no arquimediano $|\cdot|$. Sean $x, y \in K$, y supongamos que $|x| > |y|$. Entonces, por la propiedad ultramétrica,

$$|x| = |(x - y) + y| \leq \max\{|x - y|, |y|\} \leq \max\{|x|, |y|, |y|\} = |x|,$$

luego todas las desigualdades son igualdades, y por tanto, $|x-y| = |x|$ siempre que $|x| > |y|$.

Como curiosidad, esta propiedad implica que todos los triángulos en un espacio métrico no arquimediano son isósceles: si v_1, v_2 y v_3 son los vértices de un triángulo en K, basta tomar $x = v_3 - v_1$ e $y = v_3 - v_2$ en la observación anterior.

Definición A.10. Dos valores absolutos en un cuerpo K se dicen *equivalentes* si inducen la misma topología en K.

Proposición A.3. Dos valores absolutos $|\cdot|_1$, $|\cdot|_2$ en un cuerpo K son equivalentes si y sólo si existe un número real $s > 0$ tal que

$$|x|_1 = |x|_2^s \text{ para todo } x \in K.$$

Demostración. Ver página 117, proposición (3.3) de [Neu13]. □

Fijemos por convenio que para todo $x \in \mathbb{R}$ se tiene que $x < \infty$, $x + \infty = \infty$ y $\infty + \infty = \infty$.

Definición A.11. Sea K un cuerpo. Una *valoración en* K es una función $v\colon K \to \mathbb{R} \cup \{\infty\}$ tal que para todo $x, y \in K$ se verifica:

1. $v(x) = \infty$ si y sólo si $x = 0$,
2. $v(xy) = v(x) + v(y)$,
3. $v(x + y) \geq \min\{v(x), v(y)\}$.

Además, si existe $s > 0$ tal que $v(K^\times) = s\mathbb{Z}$, se dice que v es una *valoración discreta*. Si $s = 1$, se dice que v está *normalizada*.

Observación A.2. Sea K un cuerpo y denotemos $\log_c$ a la función logaritmo en base c, con $c > 1$ fijo. Dado un valor absoluto no arquimediano $|\cdot|$ en K, la función $v\colon K \to \mathbb{R} \cup \{\infty\}$ definida por

$$v(x) = \begin{cases} -\log_c |x| & \text{si } x \neq 0, \\ \infty & \text{si } x = 0. \end{cases} \tag{A.1}$$

es una valoración en K. Esto se debe a que la función $x \mapsto \log_c(x)$ es creciente para $c > 1$.

Recíprocamente, una valoración v en K también determina una familia de valores absolutos no arquimedianos. En efecto, para $c > 1$ fijo, la función

$$|x| = \begin{cases} c^{-v(x)} & \text{si } x \neq 0, \\ 0 & \text{si } x = 0. \end{cases} \tag{A.2}$$

es un valor absoluto en K, pues la función $x \mapsto c^x$ es creciente para $c > 1$.

Definición A.12. Sea K un cuerpo. Dado un valor absoluto no arquimediano $|\cdot|$ en K, la valoración (A.1) se llama *valoración definida a partir de* $|\cdot|$, para cualquier $c > 1$. Análogamente, dada una valoración v en K, el valor absoluto (A.2) se llama *valor absoluto definido a partir de* v, para cualquier $c > 1$.

Gracias a la proposición A.3, podemos dar la siguiente definición.

Definición A.13. Dos valoraciones v_1, v_2 en un cuerpo K se dicen *equivalentes* si existe un número real $s > 0$ tal que $v_1 = sv_2$.

Sea v una valoración en un cuerpo K. Es directo comprobar a partir de la definición A.11 que el conjunto

$$\mathcal{O}_v = \{x \in K : v(x) \geq 0\}$$

es un anillo, al que llamaremos *anillo de valoración de* (K, v), y que el subconjunto

$$\mathfrak{M}_v = \{x \in K : v(x) > 0\} \subset \mathcal{O}_v$$

es un ideal de $\mathcal{O}_v$, al que llamaremos *ideal de valoración de* (K, v). Si la valoración v está especificada, llamaremos a $\mathcal{O}_v$ (respectivamente, a $\mathfrak{M}_v$) *anillo* (respectivamente, *ideal) de valoración de* K. Además,

- $v(1) = v(1 \cdot 1) = v(1) + v(1)$, luego $v(1) = 0$.
- $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$, luego $v(x^{-1}) = -v(x)$ para todo $x \in K^\times$.

Proposición A.4. Sea v una valoración en un cuerpo K.

1. El conjunto formado por las unidades de $\mathcal{O}_v$ es el ideal $\mathcal{O}_v^\times = \{x \in K : v(x) = 0\}$.
2. $\mathcal{O}_v$ es un anillo local con ideal maximal $\mathfrak{M}_v$.
3. $\mathcal{O}_v$ es íntegramente cerrado.

Demostración. Notemos que $x \in \mathcal{O}_v$ es unidad si y sólo si si existe $y \in \mathcal{O}_v$ tal que $xy = 1$. Esto ocurre si y sólo si $v(xy) = v(x) + v(y) = v(1) = 0$. Como $v(x), v(y) \geq 0$, la igualdad anterior se tiene si y sólo si $v(x) = v(y) = 0$, concluyendo el primer resultado.

Del resultado anterior, se sigue que $\mathfrak{M}_v$ es el complementario de $\mathcal{O}_v^\times$, luego $\mathfrak{M}_v$ es el único ideal maximal de $\mathcal{O}_v$, y se tiene el segundo resultado.

Para el tercer resultado, observemos que si $x \in K$ entonces o $v(x) \geq 0$ o $v(x) < 0$. En el primer caso, $x \in \mathcal{O}_v$, y en el segundo caso, $v(x^{-1}) = -v(x) > 0$, luego $x^{-1} \in \mathcal{O}_v$. Es decir, o bien $x \in \mathcal{O}_v$, o bien $x^{-1} \in \mathcal{O}_v$ para todo $x \in K$.

Por reducción al absurdo, supongamos que existe $\alpha \in K$ no nulo que es raíz de

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \text{ con } a_i \in \mathcal{O}_v \text{ para todo } i = 0, \ldots, n,$$

pero $\alpha \notin \mathcal{O}_v$. Entonces, $\alpha^{-1} \in \mathcal{O}_v$ y por tanto, $\alpha^{-n+1} \in \mathcal{O}_v$. Esto es una contradicción, pues

$$\alpha = -a_1 - a_2\alpha^{-1} - \cdots - a_n(\alpha^{-1})^{n-1} \in \mathcal{O}_v,$$

concluyendo el tercer resultado. □

Definición A.14. Sea v una valoración en un cuerpo K. El cuerpo $\mathcal{O}_v/\mathfrak{M}_v$ se llama *cuerpo de residuos de* K.

Observación. Sea w una valoración discreta en un cuerpo K, es decir, existe $s > 0$ tal que $w(K^\times) = s\mathbb{Z}$. Siempre podemos considerar la valoración discreta normalizada $v = s^{-1}w$. Además, $\mathcal{O}_v = \mathcal{O}_w$, $\mathcal{O}_v^\times = \mathcal{O}_w^\times$ y $\mathfrak{M}_v = \mathfrak{M}_w$. En este caso, se dice que v es la *valoración normalizada asociada a* w.

Definición A.15. Sea v es una valoración discreta en un cuerpo K. Se dice que π es un *uniformizante en* K si $v(\pi) = \min\{v(x) : x \in \mathfrak{M}_v\}$. Si v está normalizada, esto equivale a $v(\pi) = 1$.

Lema A.1. Sea v una valoración discreta normalizada en un cuerpo K. Dado un uniformizante π en K, todo $x \in K^\times$ se expresa de manera única como

$$x = \varepsilon\pi^m, \text{ con } \varepsilon \in \mathcal{O}_v^\times \text{ y } n \in \mathbb{Z}.$$

Demostración. Sea $x \in K^\times$ y supongamos que $v(x) = n \in \mathbb{Z}$. Entonces, como $v(\pi) = 1$,

$$v(x\pi^{-n}) = v(x) + v(\pi^{-n}) = v(x) - nv(\pi) = n - n = 0.$$

Esto equivale a que $\varepsilon = x\pi^{-n} \in \mathcal{O}_v^\times$. Para ver la unicidad, supongamos que $x = \varepsilon\pi^n = \varepsilon_0\pi^{n_0}$, con $\varepsilon_0 \in \mathcal{O}_v^\times$ y $n_0 \in \mathbb{Z}$. Dado que

$$n = v(\varepsilon\pi^n) = v(\varepsilon_0\pi^{n_0}) = n_0,$$

entonces $n = n_0$. Por tanto, necesariamente $\varepsilon = \varepsilon_0$, concluyendo la unicidad y el resultado. □

Proposición A.5. Sean K un cuerpo y v una valoración discreta en K. Entonces, $\mathcal{O}_v$ es un dominio de ideales principales. Si v está normalizada, entonces todos los ideales no nulos de $\mathcal{O}_v$ son de la forma

$$\mathfrak{M}_v^n = \pi^n\mathcal{O}_v = \{x \in K : v(x) \geq n\} \text{ para todo entero } n \geq 0,$$

siendo π un uniformizante en K. Además, existe un isomorfismo

$$\mathfrak{M}_v^n/\mathfrak{M}_v^{n+1} \cong \mathcal{O}_v/\mathfrak{M}_v \text{ para todo entero } n \geq 0.$$

Demostración. Sean $I \subset \mathcal{O}_v$ un ideal no nulo, y $x \in I$ un elemento no nulo tal que $v(x) \leq v(y)$ para todo $y \in I$. Si $v(x) = n$, entonces $x = u\pi^n$ con $u \in \mathcal{O}_v^\times$ y n entero, por el lema anterior. Por tanto, $\pi^n \mathcal{O}_v \subset I$.

Recíprocamente, sea $y = \varepsilon\pi^m \in I$ con $\varepsilon \in \mathcal{O}_v^\times$ y m entero. Entonces, $m = v(y) \geq n$, y por tanto, $y = (\varepsilon\pi^{m-n})\pi^n \in \pi^n\mathcal{O}_v$. Concluimos que $I = \pi^n\mathcal{O}_v$.

Por último, el isomorfismo $\mathfrak{M}_v^n/\mathfrak{M}_v^{n+1} \cong \mathcal{O}_v/\mathfrak{M}_v$ para todo entero $n \geq 0$, se sigue de la correspondencia $a\pi^n \mapsto a \bmod \mathfrak{M}_v$. □

Proposición A.6 (Criterio de Eisenstein)**.** Sea K un cuerpo, y v una valoración discreta en K. Sea $\phi(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathcal{O}_v[x]$ un polinomio tal que $a_i \in \mathfrak{M}_v$ para todo $i = 0, \ldots, n-1$ y $a_0 \notin \mathfrak{M}_v^2$. Entonces, $\phi(x)$ es irreducible en $\mathcal{O}_v[x]$ y en $K[x]$.

Demostración. Ver lema 11.2 de [Sut21]. □

Completación de un cuerpo respecto de un valor absoluto

Dado un valor absoluto $|\cdot|$ en un cuerpo K, podemos obtener un cuerpo completo replicando la construcción de $\mathbb{R}$ a partir de $\mathbb{Q}$. Este procedimiento se llama *completación de K respecto de $|\cdot|$*. Describiremos en qué consiste sin profundizar en los detalles, siguiendo la sección 4 del capítulo II de [Neu13].

Definición A.16. Sean K un cuerpo, $|\cdot|$ un valor absoluto en K, y $\{x_n\}_{n\in\mathbb{N}} \subset K$ una sucesión. Se dice que $\{x_n\}_{n\in\mathbb{N}}$ es una *sucesión de Cauchy respecto de* $|\cdot|$ si para todo $\varepsilon > 0$ existe un natural n_0 tal que

$$|x_n - x_m| < \varepsilon \text{ para todo } n, m \geq n_0.$$

Definición A.17. Un cuerpo K se dice *completo respecto de un valor absoluto* $|\cdot|$ si toda sucesión de Cauchy respecto de $|\cdot|$ definida en K converge a un elemento de K. Es decir, si para toda sucesión $\{x_n\}_{n\in\mathbb{N}} \subset K$ de Cauchy respecto de $|\cdot|$, existe $x \in K$ tal que

$$\lim_{n\to\infty} |x - x_n| = 0.$$

Consideramos el anillo $\mathcal{C}$ de las sucesiones de Cauchy respecto de $|\cdot|$ definidas en K, y el ideal maximal $\mathfrak{m} \subset \mathcal{C}$ formado por las sucesiones $\{x_n\}_{n\in\mathbb{N}} \in \mathcal{C}$ tales que $\lim_{n\to\infty} |x_n| = 0$.

Definición A.18. Se define la *completación de K respecto del valor absoluto* $|\cdot|$ como el cuerpo $\widehat{K} = \mathcal{C}/\mathfrak{m}$.

Notemos que K está incluído en $\widehat{K}$ mediante el homomorfismo que envía un elemento $x \in K$ a la clase de la sucesión constante $(x, x, x, \ldots)$. Además, $|\cdot|$ se extiende por continuidad a un valor absoluto en $\widehat{K}$, dado por

$$\left|\lim_{n\to\infty} x_n\right| = \lim_{n\to\infty} |x_n| \text{ para toda sucesión } \{x_n\}_{n\in\mathbb{N}} \in \mathcal{C},$$

y será habitual llamarlo *extensión de* $|\cdot|$ *a* $\widehat{K}$.

Al igual que en la construcción de $\mathbb{R}$ a partir de $\mathbb{Q}$, se puede verificar que $\widehat{K}$ es un cuerpo completo respecto del valor absoluto canónico en $\widehat{K}$, y que todo elemento de $\widehat{K}$ es el límite de una sucesión de Cauchy respecto de $|\cdot|$ definida en K. Es decir, K es denso en $\widehat{K}$. También se tiene la unicidad de $\widehat{K}$ salvo isometría.

Supongamos además que $|\cdot|$ es un valor absoluto no arquimediano y que v es cualquier valoración definida a partir de $|\cdot|$. Entonces, v también se extiende a una valoración en $\widehat{K}$ por continuidad, dada por

$$\hat{v}\left(\lim_{n\to\infty} x_n\right) = \lim_{n\to\infty} v(x_n) \text{ para toda sucesión } \{x_n\}_{n\in\mathbb{N}} \in \mathcal{C}.$$

También será habitual referirnos a $\hat{v}$ como la *extensión de* v *a* $\widehat{K}$.

Proposición A.7. Sean $\widehat{K}$ la completación de un cuerpo K respecto de un valor absoluto no arquimediano $|\cdot|$, v una valoración definida a partir de $|\cdot|$, y $\hat{v}$ la extensión de v a $\widehat{K}$. Entonces, $v(K^\times) = \hat{v}(\widehat{K}^\times)$.

Demostración. Basta probar que si $\{x_n\}_{n\in\mathbb{N}} \in \mathcal{C}$ es tal que $\lim_{n\to\infty} x_n = x \in \widehat{K}$ con $x \neq 0$, entonces existe un natural n_0 tal que la sucesión $\{v(x_n)\}_{n\in\mathbb{N}}$ es constante para todo $n \geq n_0$.

En efecto, $\{x_n\}_{n\in\mathbb{N}}$ converge a x si y sólo si para todo $\varepsilon > 0$ existe un natural n_0 tal que

$$|x_n - x| < \varepsilon \text{ para todo } n \geq n_0.$$

Tomando $\varepsilon \leq |x|$, tenemos que $\hat{v}(x) < \hat{v}(x_n - x)$ para todo $n \geq n_0$. Por tanto, por la propiedad ultramétrica,

$$v(x_n) = \hat{v}(x_n - x + x) = \min\{\hat{v}(x_n - x), \hat{v}(x)\} = \hat{v}(x) \text{ para todo } n \geq n_0,$$

concluyendo el resultado. □

En las condiciones de la proposición anterior, deducimos que si v es discreta y normalizada entonces $\hat{v}$ también es discreta y normalizada. Si v es discreta, el anillo e ideal de valoración de $\widehat{K}$ son, respectivamente,

$$\widehat{\mathcal{O}}_v = \{x \in \widehat{K} : \hat{v}(x) \geq 0\} \text{ y } \widehat{\mathfrak{M}}_v = \{x \in \widehat{K} : \hat{v}(x) > 0\},$$

y se puede probar que $\mathcal{O}_v$ y $\mathfrak{M}_v$ son densos en $\widehat{\mathcal{O}}_v$ y en $\widehat{\mathfrak{M}}_v$, respectivamente.

Proposición A.8. Sean K un cuerpo, v una valoración discreta normalizada en K, y π un uniformizante en K. Entonces, π es generador de $\widehat{\mathfrak{M}}_v$ en $\widehat{\mathcal{O}}_v$. Además,

$$\widehat{\mathcal{O}}_v/\widehat{\mathfrak{M}}_v^n \cong \mathcal{O}_v/\mathfrak{M}_v^n \text{ para todo entero } n \geq 1.$$

Demostración. Ver página 126, proposición (4.3) de [Neu13] y página 116, lema 7.25 de [Mil08]. □

Una propiedad importante que satisfacen los cuerpos completos respecto de un valor absoluto no arquimediano es el lema de Hensel:

Teorema A.2 (Lema de Hensel)**.** *Sean K un cuerpo completo respecto de un valor absoluto no arquimediano $|\cdot|$, v una valoración definida a partir de $|\cdot|$, y $\phi(x) \in \mathcal{O}_v[x]$ un polinomio tal que $\phi(x) \not\equiv 0 \bmod \mathfrak{M}_v$. Denotemos k_v al cuerpo de residuos de (K, v), y denotemos $\widetilde{\phi}(x) = \phi(x) \bmod \mathfrak{M}_v$. Supongamos que $\widetilde{\phi}(x)$ admite una factorización*

$$\widetilde{\phi}(x) = \widetilde{g}(x)\widetilde{h}(x)$$

en polinomios $\widetilde{g}(x), \widetilde{h}(x) \in k_v[x]$ coprimos entre sí. Entonces, $\phi(x)$ admite una factorización

$$\phi(x) = g(x)h(x)$$

en polinomios $g(x), h(x) \in \mathcal{O}_v[x]$ tales que $\deg g = \deg \widetilde{g}$, y

$$g(x) \equiv \widetilde{g}(x) \bmod \mathfrak{M}_v, \quad y \quad h(x) \equiv \widetilde{h}(x) \bmod \mathfrak{M}_v.$$

Demostración. Ver página 129, teorema (4.6) de [Neu13]. □

Corolario A.2. Sean K un cuerpo completo respecto de un valor absoluto no arquimediano $|\cdot|$, v una valoración definida a partir de $|\cdot|$, y $\phi(x) \in \mathcal{O}_v[x]$ un polinomio mónico. Si $\widetilde{\alpha} \in k_v$ es una raíz simple de $\widetilde{\phi}(x)$, entonces existe una raíz $\alpha \in \mathcal{O}_v$ de $\phi(x)$ tal que $\alpha \equiv \widetilde{\alpha} \bmod \mathfrak{M}_v$.

Extensiones de cuerpos completos

Definición A.19. Sea L/K una extensión algebraica de cuerpos y sean $|\cdot|_K$ y $|\cdot|_L$ valores absolutos en K y L, respectivamente. Se dice que $|\cdot|_L$ *extiende* $|\cdot|_K$ *a* L o que $|\cdot|_K$ *se extiende a* $|\cdot|_L$ *en* L si

$$|x|_L = |x|_K \text{ para todo } x \in K.$$

Análogamente, si v_K y v_L son valoraciones en K y L respectivamente, se dice que v_L *extiende* v_K *a* L o que v_K *se extiende a* v_L *en* L si

$$v_L(x) = v_K(x) \text{ para todo } x \in K.$$

Teorema A.3. *Sea K un cuerpo completo respecto de un valor absoluto $|\cdot|_K$. Sea L/K una extensión finita de grado n. Entonces, $|\cdot|_K$ se extiende a un único valor absoluto en L, dado por la fórmula*

$$|x|_L = \left|N_{L/K}(x)\right|_K^{\frac{1}{n}} \text{ para todo } x \in L^\times. \tag{A.3}$$

Además, L es un cuerpo completo respecto de $|\cdot|_L$.

Demostración. Ver página 131, teorema (4.8) de [Neu13]. □

El siguiente corolario se obtiene sin más que aplicar la función $-\log_c$ para algún $c > 1$ en la fórmula (A.3), asumiendo que $|\cdot|_K$ es no arquimediano.

Corolario A.3. Sean K un cuerpo completo respecto de un valor absoluto no arquimediano $|\cdot|_K$, v_K una valoración definida a partir de $|\cdot|_K$, y L/K una extensión finita de grado n. Entonces, v_K se extiende a una única valoración en L, dada la fórmula

$$v_L(x) = \frac{1}{n} v_K\left(N_{L/K}(x)\right) \text{ para todo } x \in L^\times. \tag{A.4}$$

Observación A.3. Sean K un cuerpo completo respecto de un valor absoluto no arquimediano $|\cdot|_K$, v_K una valoración definida a partir de $|\cdot|_K$, y L/K una extensión finita de grado n. Sea $|\cdot|_L$ el valor absoluto definido en (A.3), y sea v_L la valoración definida en (A.4),

- Será habitual referirnos al valor absoluto $|\cdot|_L$ (respectivamente, la valoración v_L) como la *extensión de* $|\cdot|_K$ (respectivamente, *de* v_K*) a* L.
- El valor absoluto $|\cdot|_L$ es compatible en extensiones finitas de K. En efecto, si L'/L es una extensión finita de grado m, entonces,

$$|x|_{L'} = \left|N_{L'/L}(x)\right|_L^{\frac{1}{m}} = |x|_L^{\frac{m}{m}} = |x|_L \text{ para todo } x \in L^\times.$$

  En otras palabras, $|\cdot|_{L'}$ extiende $|\cdot|_L$ a L'. Análogamente, v_L también es compatible en extensiones finitas de K.
- Fijemos una clausura algebraica $\overline{K}$. Del punto anterior se sigue que $|\cdot|_K$ y v_K se extienden de manera única a $\overline{K}$. Sin embargo, si suponemos que $|\cdot|_K$ y v_K son discretos, sus extensiones a $\overline{K}$ no son discretas, en general. De hecho, $\overline{K}$ no es completo respecto del valor absoluto extendido, aunque la completación de $\overline{K}$ sigue siendo un cuerpo algebraicamente cerrado. Se puede consultar la observación 7.41 de [Mil08] para ver un ejemplo de este fenómeno.
- Supongamos que v_K es discreta. Entonces, de la expresión de (A.4) se sigue que v_L también lo es, pues

$$v_L(L^\times) \subset \frac{1}{n} v_K(K^\times).$$

Cuerpos henselianos

Definición A.20. Un cuerpo K se dice *henseliano respecto de una valoración* v si en $\mathcal{O}_v$ se verifica el lema de Hensel.

Teorema A.4. *Sean K un cuerpo henseliano respecto de una valoración v_K, y $|\cdot|_K$ un valor absoluto no arquimediano definido a partir de v_K. Para toda extensión algebraica L/K, v_K y $|\cdot|_K$ se extienden de manera única a una valoración v_L y a un valor absoluto $|\cdot|_L$ en L, de modo que $\mathcal{O}_{v_L}$ es la clausura entera de $\mathcal{O}_{v_K}$ en L. Si L/K es finita de grado n, entonces*

$$v_L(x) = \frac{1}{n} v_K\left(N_{L/K}(x)\right) \text{ y } |x|_L = \left|N_{L/K}(x)\right|_K^{\frac{1}{n}} \text{ para todo } x \in L^\times.$$

Demostración. Ver página 144, teorema (6.2) de [Neu13]. □

Teorema A.5. *Un cuerpo K es henseliano respecto de una valoración v si y sólo si v se extiende de manera única a cualquier extensión algebraica de K.*

Demostración. Ver página 147, teorema (6.6) de [Neu13]. □

Observación. Sea K un cuerpo de característica 0, v_K una valoración en K y $|\cdot|_K$ un valor absoluto no arquimediano en K definido a partir de v_K.

- Si K es un cuerpo completo respecto de $|\cdot|_K$, entonces K es un cuerpo henseliano respecto de v_K.
- Sea p un primo. Si K es la máxima extensión no ramificada (ver definición 1.12) de una extensión finita de $\mathbb{Q}_p$, entonces K es un cuerpo henseliano respecto de v_K, y v_K es la única extensión de la valoración p-ádica a K. Se recomienda consultar el comentario después de la proposición (7.5) de [Neu13].

Lema A.2. Sean K un cuerpo henseliano de característica 0 respecto de una valoración v_K, y $|\cdot|_K$ un valor absoluto no arquimediano definido a partir de v_K. Fijemos una clausura algebraica $\overline{K}$, y denotemos $|\cdot|$ a la extensión del valor absoluto $|\cdot|_K$ a $\overline{K}$. Entonces,

$$|\sigma(\alpha)| = |\alpha| \text{ para todo } \alpha \in \overline{K} \text{ y } \sigma \in \mathrm{Aut}_K(\overline{K}).$$

Demostración. Sean $\alpha \in \overline{K}$ y $\sigma \in \mathrm{Aut}_K(\overline{K})$. Entonces, α y $\sigma(\alpha)$ tienen el mismo polinomio mínimo $f(x) \in K[x]$, pues $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, y por tanto,

$$N_{K(\alpha)/K}(\alpha) = f(0) = N_{K(\sigma(\alpha))/K}(\sigma(\alpha)).$$

Si $n = \deg f$, se sigue del teorema A.4 que

$$|\sigma(\alpha)| = |N_{K(\sigma(\alpha))/K}(\alpha)|^{1/n} = |N_{K(\alpha)/K}(\alpha)|^{1/n} = |\alpha|,$$

como queríamos. □

Definición A.21. Sean K un cuerpo de característica 0 henseliano respecto de una valoración v_K, y $|\cdot|_K$ un valor absoluto no arquimediano definido a partir de v_K. Fijemos una clausura algebraica $\overline{K}$, y denotemos $|\cdot|$ a la extensión del valor absoluto $|\cdot|_K$ a $\overline{K}$. Sean $\alpha, \beta \in \overline{K}$. Se dice que β *pertenece a* α si

$$|\beta - \alpha| < |\beta - \sigma(\alpha)| \text{ para todo } \sigma \in \mathrm{Aut}_K(\overline{K}) \text{ tal que } \sigma(\alpha) \neq \alpha. \tag{A.5}$$

Como consecuencia de la observación A.1, la condición (A.5) es equivalente a

$$|\beta - \alpha| < |\alpha - \sigma(\alpha)| \text{ para todo } \sigma \in \mathrm{Aut}_K(\overline{K}) \text{ tal que } \sigma(\alpha) \neq \alpha.$$

Proposición A.9 (Lema de Krasner)**.** Sean K un cuerpo de característica 0 henseliano respecto de una valoración v_K, y $|\cdot|_K$ un valor absoluto no arquimediano definido a partir de v_K. Fijemos una clausura algebraica $\overline{K}$, y denotemos $|\cdot|$ a la extensión del valor absoluto $|\cdot|_K$ a $\overline{K}$. Sean $\alpha, \beta \in \overline{K}$. Si β pertenece a α, entonces $K(\alpha) \subset K(\beta)$.

Demostración. Por reducción al absurdo, supongamos que $\alpha \notin K(\beta)$. Entonces, la extensión $K(\alpha, \beta)/K(\beta)$ es separable y no trivial, por lo que existe $\sigma \in \mathrm{Aut}_K(\overline{K})$ tal que $\sigma(\alpha) \neq \alpha$ y $\sigma(\beta) = \beta$. En efecto, basta tomar σ como el automorfismo que envía α a otra raíz del polinomio mínimo de α sobre $K(\beta)$. Entonces, por el lema A.2,

$$|\beta - \alpha| = |\sigma(\beta - \alpha)| = |\sigma(\beta) - \sigma(\alpha)| = |\beta - \sigma(\alpha)|,$$

en contradicción con el hecho de que β pertenece a α. □

A.5. Demostraciones adicionales

La notación de esta sección es la misma que la de la sección 1.4.

Demostración de la proposición 1.11

Demostración. Sea $\phi(x) \in K_\mathfrak{p}[x]$ el polinomio mínimo de ζ_n sobre $K_\mathfrak{p}$, y denotemos $\widetilde{\phi}(x) = \phi(x) \bmod \mathfrak{M}_\mathfrak{p}$ y $\widetilde{\zeta_n} = \zeta_n \bmod \mathfrak{M}_F$. Por definición, ζ_n es raíz del polinomio $x^n - 1$, luego $\phi(x)$ divide a $x^n - 1$. Por tanto, $\widetilde{\phi}(x)$ divide a $x^n - 1 \bmod \mathfrak{M}_\mathfrak{p}$. Como $\gcd(n, p) = 1$, tenemos que

$$(x^n - 1)' = nx^{n-1} \not\equiv 0 \bmod \mathfrak{M}_\mathfrak{p},$$

por lo que $x^n - 1 \bmod \mathfrak{M}_\mathfrak{p}$ es un polinomio separable (es decir, no tiene raíces repetidas). Los divisores de un polinomio separable son polinomios separables, luego $\widetilde{\phi}(x)$ es separable y tiene a $\widetilde{\zeta_n}$ como raíz.

Supongamos por reducción al absurdo que $\widetilde{\phi}(x)$ no es irreducible. Entonces, existen polinomios no constantes $\widetilde{g}(x), \widetilde{h}(x) \in k_\mathfrak{p}[x]$ tales que $\widetilde{\phi}(x) = \widetilde{g}(x)\widetilde{h}(x)$. Como $\widetilde{\phi}(x)$ es separable, $\widetilde{g}(x)$ y $\widetilde{h}(x)$ son coprimos. Por el lema de Hensel, $\phi(x)$ tampoco es irreducible, lo cual es absurdo pues $\phi(x)$ es el polinomio mínimo de ζ_n sobre $K_\mathfrak{p}$. Concluimos que $\widetilde{\phi}(x)$ es irreducible, luego es el polinomio mínimo de $\widetilde{\zeta_n}$ sobre $k_\mathfrak{p}$. En particular, $\deg \phi = \deg \widetilde{\phi}$, luego $[F : K_\mathfrak{p}] = [k_\mathfrak{p}(\widetilde{\zeta_n}) : k_\mathfrak{p}]$. Además, dado que $\widetilde{\zeta_n} \in k_F$, tenemos que

$$[F : K_\mathfrak{p}] \geq [k_F : k_\mathfrak{p}] \geq [k_\mathfrak{p}(\widetilde{\zeta_n}) : k_\mathfrak{p}] = [F : K_\mathfrak{p}]. \tag{A.6}$$

Por tanto, todas las desigualdades de esta cadena deben ser igualdades. En particular, tenemos que $[F : K_\mathfrak{p}] = [k_F : k_\mathfrak{p}]$, y concluimos que $F/K_\mathfrak{p}$ es no ramificada.

Por otro lado, denotemos $f = f(F/K_\mathfrak{p})$. Como $F/K_\mathfrak{p}$ es no ramificada, $[F : K_\mathfrak{p}] = f$. El polinomio $x^n - 1 \in \mathcal{O}_F[x]$ se descompone en factores lineales distintos en $\mathcal{O}_F$, y como $\gcd(n, p) = 1$, esto también ocurre en k_F. Por tanto, el grupo multiplicativo $k_F^\times$ contiene un subgrupo isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Como $k_F = \mathbb{F}_{q^f}$, tenemos que $n \mid q^f - 1$.

Falta probar que f es el menor entero positivo que verifica la propiedad anterior. En efecto, por (A.6), tenemos que $k_F = k_\mathfrak{p}(\widetilde{\zeta_n})$, luego k_F es el cuerpo de descomposición de $\widetilde{\phi}(x)$. Ahora bien, sea f' un entero positivo tal que $n \mid q^{f'} - 1$, y denotemos $k' = \mathbb{F}_{p^{f'}}$. Entonces, el grupo multiplicativo $k'^\times$ contiene un subgrupo isomorfo a $\mathbb{Z}/n\mathbb{Z}$, y todos los elementos de este subgrupo son raíces de la unidad de orden n. Por tanto, el polinomio $x^n - 1$ se descompone en producto de factores lineales en k', luego $\widetilde{\phi}(x)$ tendría n raíces distintas en k'. Se sigue que k' contiene al cuerpo de descomposición de $\widetilde{\phi}(x)$, que es k_F. Concluimos que $f \mid f'$, como queríamos. □

Demostración del teorema 1.6

Demostración. Supongamos que $F = K_\mathfrak{p}(\zeta_{q^n-1})$. Dado que $\gcd(q^n - 1, p) = 1$, la extensión $F/K_\mathfrak{p}$ es no ramificada por la proposición 1.11. Además, $[F : K_\mathfrak{p}] = n$ pues n es el menor de entre todos los enteros positivos f tales que $q^f \equiv 1 \bmod q^n - 1$.

Recíprocamente, supongamos que $F/K_\mathfrak{p}$ es no ramificada de grado n. Como $k_\mathfrak{p} \cong \mathbb{F}_q$, entonces $k_F \cong \mathbb{F}_{q^n}$, luego k_F es el cuerpo de descomposición del polinomio $x^{q^n-1}-1$ sobre $k_\mathfrak{p}$. Sea $\widetilde{\alpha}$ un generador de $k_F^\times$ como grupo cíclico, y sea $\widetilde{\phi}(x) \in k_\mathfrak{p}[x]$ su polinomio mínimo sobre $k_\mathfrak{p}$. Entonces, $\widetilde{\phi}(x)$ divide a $x^{q^n-1}-1$. Como $\widetilde{\phi}(x)$ es irreducible, entonces es coprimo con el cociente $(x^{q^n-1}-1)/\widetilde{\phi}(x)$, que es un polinomio. Por el lema de Hensel, existe un polinomio $\phi(x) \in \mathcal{O}_\mathfrak{p}[x]$ tal que

$$\phi(x) \equiv \widetilde{\phi}(x) \operatorname{mód} \mathfrak{M}_\mathfrak{p} \text{ y } \phi(x) \mid x^{q^n-1}-1 \in \mathcal{O}_\mathfrak{p}[x].$$

Observemos que $\widetilde{\alpha} \in k_F$ es una raíz simple de $\widetilde{\phi}(x)$, visto como polinomio de $k_F[x]$. Por el corolario A.2, existe una raíz $\alpha \in \mathcal{O}_F$ de $\phi(x)$ tal que $\alpha \equiv \widetilde{\alpha} \operatorname{mód} \mathfrak{M}_F$. Por tanto, α es una raíz de $x^{q^n-1}-1$, luego es una raíz primitiva (q^n-1)-ésima de la unidad, pues $\widetilde{\alpha}$ lo es. Como $K_\mathfrak{p}(\alpha) \subset F$ y $K_\mathfrak{p}(\alpha)/K_\mathfrak{p}$ es una extensión no ramificada de grado n, concluimos que $F \cong K_\mathfrak{p}(\alpha) = K_\mathfrak{p}(\zeta_{q^n-1})$.

Finalmente, la extensión $F/K_\mathfrak{p}$ es de Galois ya que F es el cuerpo de descomposición de $x^{q^n-1}-1$ sobre $K_\mathfrak{p}$. Además, la correspondencia biunívoca entre las raíces (q^n-1)-ésimas de la unidad de F y k_F induce un isomorfismo

$$\operatorname{Gal}(F/K_\mathfrak{p}) \cong \operatorname{Gal}(k_F/k_\mathfrak{p}),$$

concluyendo el resultado. □

Demostración del teorema 1.7

Demostración. Sea π un uniformizante en $K_\mathfrak{p}^{\mathrm{unr}}$. La proposición 1.13 y la proposición 1.14 prueban que las extensiones $K_\mathfrak{p}^{\mathrm{unr}}(\sqrt[n]{\pi})/K_\mathfrak{p}^{\mathrm{unr}}$ con $\gcd(n,p)=1$ son moderadas de grado n.

Recíprocamente, supongamos que $F/K_\mathfrak{p}^{\mathrm{unr}}$ es moderada de grado n. Como k_F es algebraicamente cerrado, se sigue de la identidad fundamental que

$$n = [F : K_\mathfrak{p}^{\mathrm{unr}}] = e(F/K_\mathfrak{p}^{\mathrm{unr}})$$

Denotemos $e = e(F/K_\mathfrak{p}^{\mathrm{unr}})$. Como $F/K_\mathfrak{p}^{\mathrm{unr}}$ es moderada, entonces $\gcd(e,p)=1$, y concluimos que $\gcd(n,p)=1$.

Supongamos que π_0 es uniformizante en $K_\mathfrak{p}^{\mathrm{unr}}$. Entonces, si π_F es uniformizante en F, existe una unidad $\varepsilon \in \mathcal{O}_F^\times$ tal que $\pi_0 = \varepsilon^{-1}\pi_F^e$. Como $k_\mathfrak{p}^{\mathrm{unr}} \cong k_F$, existe una unidad ε_0 en el anillo de valoración de $K_\mathfrak{p}^{\mathrm{unr}}$ tal que

$$\varepsilon \equiv \varepsilon_0 \operatorname{mód} \mathfrak{M}_F.$$

Definimos $\pi = \varepsilon_0\pi_0$ y $z = \varepsilon_0^{-1}(\varepsilon - \varepsilon_0)$. Si denotamos $|\cdot|$ a la extensión del valor absoluto $\mathfrak{p}$-ádico a F, entonces la congruencia anterior implica que $z \in \mathfrak{M}_F$, por lo que $|z| < 1$. Además,

$$\pi_F^e = \varepsilon\pi_0 = \varepsilon_0\pi_0 + (\varepsilon_0\pi_0)\,\varepsilon_0^{-1}(\varepsilon - \varepsilon_0) = \pi + \pi z,$$

por lo que

$$|\pi_F^e - \pi| = |\pi z| < |\pi|. \tag{A.7}$$

Ahora, consideremos el polinomio $\phi(x) = x^e - \pi \in K_{\mathfrak{p}}^{\mathrm{unr}}[x]$, y sus raíces $\alpha_1, \ldots, \alpha_e$. Entonces,

$$|\phi(\pi_F)| = \prod_{i=1}^{e} |\pi_F - \alpha_i| = |\pi_F^e - \pi|. \tag{A.8}$$

Por otro lado,

$$|\alpha_i|^e = |\pi| = |\pi_F|^e, \text{ y por tanto, } |\alpha_i| = |\pi_F| \text{ para todo } i = 1, \ldots, e. \tag{A.9}$$

Supongamos por reducción al absurdo que $|\pi_F - \alpha_i| \geq |\alpha_i|$ para todo $i = 1, \ldots, e$. Combinando (A.7), (A.8), (A.9) junto con el hecho de que $|\alpha_i| = |\alpha_j|$ para todo $i, j = 1, \ldots, e$ por ser conjugados (ver lema A.2), llegamos a una contradicción:

$$|\pi| > |\pi_F^e - \pi| = \prod_{i=1}^{e} |\pi_F - \alpha_i| \geq \prod_{i=1}^{e} |\alpha_i| = |\alpha_1|^e = |\pi|.$$

Por tanto, existe un i (digamos, $i = 1$) tal que

$$|\pi_F - \alpha_1| < |\alpha_1|. \tag{A.10}$$

Ahora bien, por la propiedad ultramétrica, tenemos que $|\alpha_1 - \alpha_i| \leq |\alpha_1|$ para todo $i = 2, \ldots, e$. Veamos que, de hecho, esta desigualdad es una igualdad. Para ello, teniendo en cuenta que $|e| = 1$ y derivando la expresión de $\phi(x)$ como producto, observamos que

$$|\phi'(\alpha_1)| = |\alpha_1|^{e-1} = \prod_{i=2}^{e} |\alpha_1 - \alpha_i|.$$

Por reducción al absurdo, supongamos que existe un i (digamos, $i = 2$) tal que $|\alpha_1 - \alpha_2| < |\alpha_1|$. Entonces, la igualdad anterior nos lleva a una contradicción:

$$|\alpha_1|^{e-1} = \prod_{i=2}^{e} |\alpha_1 - \alpha_i| = |\alpha_1 - \alpha_2| \prod_{i=3}^{e} |\alpha_1 - \alpha_i| < |\alpha_1| \, |\alpha_1|^{e-2} = |\alpha_1|^{e-1}.$$

Por tanto, $|\alpha_1 - \alpha_i| = |\alpha_1|$ para todo $i = 2, \ldots, e$. Entonces, se sigue de (A.10) que

$$|\pi_F - \alpha_1| < |\alpha_1| = |\alpha_1 - \alpha_i| \text{ para todo } i = 2, \ldots, e.$$

Por el lema de Krasner (ver proposición A.9), tenemos que $K_{\mathfrak{p}}^{\mathrm{unr}}(\alpha_1) \subset K_{\mathfrak{p}}^{\mathrm{unr}}(\pi_F)$, y por tanto,

$$K_{\mathfrak{p}}^{\mathrm{unr}} \subset K_{\mathfrak{p}}^{\mathrm{unr}}(\alpha_1) \subset K_{\mathfrak{p}}^{\mathrm{unr}}(\pi_F) \subset F.$$

Ahora, α_1 es una raíz del polinomio $\phi(x) = x^e - \pi$, que es irreducible por el criterio de Eisenstein. Luego, $[K_{\mathfrak{p}}^{\mathrm{unr}}(\alpha_1) : K_{\mathfrak{p}}^{\mathrm{unr}}] \geq e = n = [F : K_{\mathfrak{p}}^{\mathrm{unr}}]$, y concluimos que

$$K_{\mathfrak{p}}^{\mathrm{unr}}(\sqrt[n]{\pi}) \cong K_{\mathfrak{p}}^{\mathrm{unr}}(\alpha_1) \cong F,$$

como queríamos. □

Demostración de la proposición 1.19

Demostración. La primera igualdad es trivial. Probemos la segunda. Por la primera observación de la sección 5 del capítulo 1, $I(F/K_\mathfrak{p})$ es el núcleo del homomorfismo reducción

$$\begin{aligned}\pi_{F/K_\mathfrak{p}}\colon \mathrm{Gal}(F/K_\mathfrak{p}) &\to \mathrm{Gal}(k_F/k_\mathfrak{p})\\ \sigma &\mapsto \sigma \bmod \mathfrak{M}_F.\end{aligned}$$

Concluimos el resultado, pues el subcuerpo fijo por $\ker \pi_{F/K_\mathfrak{p}}$ coincide con la máxima subextensión no ramificada de $F/K_\mathfrak{p}$, es decir, con $F \cap K_\mathfrak{p}^{\mathrm{unr}}$. Se puede consultar la proposición (9.11) en la página 173 de [Neu13] para ver una demostración de este hecho.

Probemos la tercera igualdad. La inclusión $I^{\mathrm{wild}}(F/K_\mathfrak{p}) \subset G_1$ no es difícil de comprobar, veamos cómo probar la otra. Dado que $I^{\mathrm{wild}}(F/K_\mathfrak{p}) = \mathrm{Gal}(F/F \cap K_\mathfrak{p}^{\mathrm{tame}})$, basta probar que la restricción de G_1 a $F \cap K_\mathfrak{p}^{\mathrm{tame}}$ es trivial, y esto equivale a probar que si $F/K_\mathfrak{p}$ es moderada entonces $G_1 = \{\mathrm{id}\}$. Podemos asumir que $K_\mathfrak{p} = K_\mathfrak{p}^{\mathrm{unr}}$, pues $G_0 = I(F/K_\mathfrak{p})$.

Así, supongamos que $F/K_\mathfrak{p}$ es moderada. Entonces, por el teorema 1.7, $F \cong K_\mathfrak{p}(\sqrt[m]{\pi})$, siendo $m = [F : K_\mathfrak{p}]$ y π un uniformizante en $K_\mathfrak{p}$. En la demostración del teorema citado, se prueba que $\sqrt[m]{\pi}$ es uniformizante en F. Dado un automorfismo no trivial $\sigma \in G$, entonces $\sigma(\sqrt[m]{\pi}) = \zeta_m \sqrt[m]{\pi}$ para alguna raíz primitiva m-ésima de la unidad $\zeta_m \in K_\mathfrak{p}$. Como $\mathfrak{M}_F^2$ está generado por $(\sqrt[m]{\pi})^2$, entonces

$$\sigma(\sqrt[m]{\pi}) \not\equiv \zeta_m \sqrt[m]{\pi} \bmod \mathfrak{M}_F^2,$$

y concluimos que $G_1 = \{\mathrm{id}\}$. Por tanto, $G_1 \subset I^{\mathrm{wild}}(F/K_\mathfrak{p})$. □

Bibliografía

[Car86] Henri Carayol. «Sur les représentations l-adiques associées aux formes modulaires de Hilbert». En: *Annales scientifiques de l'École Normale Supérieure*. Vol. 19. 3. 1986, págs. 409-468.

[Cla] Claudius. *Proving* $\varprojlim S_i \cong \varprojlim S_j$ *where* $J \subseteq I$ *cofinal*. Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/1854822 (version: 2016-07-10). eprint: https://math.stackexchange.com/q/1854822. URL: https://math.stackexchange.com/q/1854822.

[Con10] Keith Conrad. «Ostrowski for number fields». En: *Expository papers on Algebraic Number Theory. https://kconrad. math. uconn. edu/blurbs/gradnumthy/ostrowskinumbfield. pdf* (2010).

[CR66] Charles W Curtis e Irving Reiner. *Representation theory of finite groups and associative algebras*. Vol. 356. American Mathematical Soc., 1966.

[DDT95] Henri Darmon, Fred Diamond y Richard Taylor. «Fermat's last theorem». En: *Current developments in mathematics* 1995.1 (1995), págs. 1-154.

[Del06] Pierre Deligne. «Formes modulaires et representations e-adiques». En: *Séminaire Bourbaki vol. 1968/69 Exposés 347-363*. Springer, 2006, págs. 139-172.

[DI95] Fred Diamond y John Im. «Modular forms and modular curves». En: *Seminar on Fermat's last theorem*. Amer. Math. Soc. 1995, págs. 39-133.

[Die07] Luis Dieulefait. *The level 1 weight 2 case of Serre's conjecture*. 2007. arXiv: math/0412099 [math.NT].

[DPV19] Luis Dieulefait, Ariel Pacetti y Fernando Rodríguez Villegas. *Representaciones de Galois*. 2019. URL: https://sweet.ua.pt/apacetti/cursos/Final.pdf.

[DS05] Fred Diamond y Jerry Michael Shurman. *A first course in modular forms*. Vol. 228. Springer, 2005.

[DS74] Pierre Deligne y Jean-Pierre Serre. «Formes modulaires de poids 1». En: *Annales scientifiques de l'École Normale Supérieure*. Vol. 7. 4. 1974, págs. 507-530.

[Edi92] Bas Edixhoven. «The weight in Serre's conjectures on modular forms». En: *Inventiones mathematicae* 109.1 (1992), págs. 563-594.

[Ful08] William Fulton. «Algebraic curves». En: *An Introduction to Algebraic Geom* 54 (2008).

[grg] grghxy. *Frobenius elements in infinite extensions*. MathOverflow. eprint: https://mathoverflow.net/q/220608. URL: https://mathoverflow.net/q/220608.

[Gro90] B. Gross. «A tameness criterion for Galois representations associated to modular forms mod p». En: *Duke Mathematical Journal* 61 (1990), págs. 445-517. URL: https://api.semanticscholar.org/CorpusID:121043436.

[Har13] Robin Hartshorne. *Algebraic geometry*. Vol. 52. Springer Science & Business Media, 2013.

[Hum12] James E Humphreys. *Introduction to Lie algebras and representation theory*. Vol. 9. Springer Science & Business Media, 2012.

[Kat06] Nicholas Katz. «A result on modular forms in characteristic p». En: vol. 601. Nov. de 2006, págs. 53, 61. ISBN: 978-3-540-08348-1. DOI: 10.1007/BFb0063944.

[Kha06] Chandrashekhar Khare. «Serre's modularity conjecture: The level one case». En: *Duke Mathematical Journal* 134.3 (2006), págs. 557-589. DOI: 10.1215/S0012-7094-06-13434-8. URL: https://doi.org/10.1215/S0012-7094-06-13434-8.

[KW04] Chandrashekhar Khare y Jean-Pierre Wintenberger. *On Serre's reciprocity conjecture for 2-dimensional mod p representations of the Galois group of Q*. 2004. arXiv: math/0412076 [math.NT].

[KW09a] Chandrashekhar Khare y Jean-Pierre Wintenberger. «Serre's modularity conjecture (I)». En: *Inventiones mathematicae* 178.3 (2009), págs. 485-504.

[KW09b] Chandrashekhar Khare y Jean-Pierre Wintenberger. «Serre's modularity conjecture (II)». En: *Inventiones mathematicae* 178.3 (2009), págs. 505-586.

[Liv89] Ron Livné. «On the conductors of mod/Galois representations coming from modular forms». En: *Journal of Number Theory* 31.2 (1989), págs. 133-141.

[LMFDB] The LMFDB Collaboration. *The L-functions and modular forms database*. https://www.lmfdb.org. 2024.

[Loz11] Álvaro Lozano-Robledo. *Elliptic curves, modular forms, and their L-functions*. Vol. 58. American Mathematical Soc., 2011.

[Mar] Samuel Marks. *Galois representations*. URL: https://people.math.harvard.edu/~smarks/mod-forms-tutorial/mf-notes/galois-reps.pdf.

[mar] marlu. *Serre's Modularity Conjecture – Weight*. URL: https://math.stackexchange.com/q/3238515.

[Maz77] Barry Mazur. «Modular curves and the Eisenstein ideal». En: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 47.1 (1977), págs. 33-186.

[MG78] Barry Mazur y Dorian Goldfeld. «Rational isogenies of prime degree». En: *Inventiones mathematicae* 44 (1978), págs. 129-162.

[Mil03] James S Milne. «Fields and Galois theory». En: *Courses Notes, Version* 4 (2003).

[Mil08] James S Milne. *Algebraic number theory*. JS Milne, 2008.

[MS77] Daniel A Marcus y Emanuele Sacco. *Number fields*. Vol. 2. Springer, 1977.

[Neu13] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Springer Science & Business Media, 2013.

[Rib08] Paulo Ribenboim. *Fermat's last theorem for amateurs*. Springer Science & Business Media, 2008.

[RS99] Kenneth A Ribet y William A Stein. «Lectures on Serre's conjectures». En: *Arithmetic algebraic geometry (Park City, UT, 1999)* 9 (1999), págs. 143-232.

[Ser+77] Jean-Pierre Serre et al. *Linear representations of finite groups*. Vol. 42. Springer, 1977.

[Ser13] Jean-Pierre Serre. *Local fields*. Vol. 67. Springer Science & Business Media, 2013.

[Ser72] Jean-Pierre Serre. «Propriétés galoisiennes des points d'ordre fini des courbes elliptiques». En: *Invent. math* 15 (1972), págs. 259-331.

[Ser87] Jean-Pierre Serre. «Sur les représentations modulaires de degré 2 de Gal (Q/Q)». En: *Duke Mathematical Journal* 54.1 (1987), págs. 179-230.

[Ser97] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. AK Peters/CRC Press, 1997.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer, 2009.

[Sil13] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2013.

[ST92] Joseph H. Silverman y John Torrence Tate. *Rational points on elliptic curves*. Vol. 9. Springer, 1992.

[Sut21] Andrew Sutherland. *Lecture Notes 11. Number Theory I*. https://ocw.mit.edu/courses/18-785-number-theory-i-fall-2021/resources/mit18_785f21_lec11/. 2021.

[Ulm15] Douglas Ulmer. *Conductors of l-adic representations*. 2015. arXiv: 1307.4525 [math.NT].

[Wie08] Gabor Wiese. «Galois representations». En: *Lecture notes* (2008).