UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Tesis de Licenciatura

Formas Modulares y Representaciones de Galois: la Conjetura de Serre

Maximiliano Camporino

Director: Ariel Pacetti

Marzo de 2011

Agradecimientos

Uf, es difícil agradecer a todos los que lo merecen, pero acá va mi mejor intento.

Primero que nada quiero agradecerle a mis viejos, Eduardo y Patricia, sin los que definitivamente no estaría donde estoy.

A mi hermanita Agus, que más allá de buenos y malos momentos siempre estuvo ahi para acompañarme, aun cuando ella misma no se diera cuenta.

A mi tía Gra, con la que siempre supe (y se) que puedo contar.

Saliendo un poco de la familia y entrando a la matemática...

A Flora y Patricia, gracias a las que empezó todo.

A Ariel, que me dejo encontrar mi lugar en esta cuestión, y además pasó un lindo veranito leyendo y releyendo lo que escribía, siempre con la mejor onda.

A Marco y Teresa, gracias por dedicarle tiempo a tratar de mejorar este trabajo.

A Luis, que en menos de un mes me ayudó a aclarar un montón de cosas.

Al plantel del seminario, Nico, Marce, Martín y Charly que me ayudó a ir descubriendo el lugar donde me había metido, y sobre todas las cosas me enseñó el valor de una buena bondiola.

A toda la gente que de a poco fue mostrandome que no le había errado a la carrera, profesores como Matías, Gabriel, Andrea, Daniel, Patu, Pablo y Eduardo y también Seba, Leandro, Roman, Nico, Mariano y Dani.

Y a todos los que hicieron que esto sea más interesante, Tom, Christian, Marcos, Gaby, Pablo, Quimey, Xime, Julian, Vero, otra vez Charly (y gracias por la notación), Lucho y aca probablemente me esté olvidando de un montón de gente.

Y ya fuera de la facultad (aunque no tanto...)

A mi rodilla derecha, que decidió que era hora de recibirse.

A Fede, que aunque seguro no está de acuerdo, fue un gran compañero de trabajo.

A los que estan lejos, aunque insistan en que no tanto, Javi, Cintia, Lucas.

Al flaco, Nico, que a pesar de que no nos vemos muy seguido para mi es

un buen amigo.

A Luli y Pablo, que siempre que nos encontramos es como si la última vez hubiese sido ayer.

A la barra de Fondo, que hizo que todo sea mucho más divertido, Agus, Fede, Tute, De, Javi, Dani, Sergio, Nano y Tin.

Y a los que estuvieron desde el principio, gracias por la amistad Sergio, Changui, Pablo, Pampa, Julian, Ruso y Fede.

Gracias por todo.

Maxi

Introducción

El panorama actual de buena parte de la teoría de números esta compuesto por las diversas interacciones entre tres mundos diferentes.

En primer lugar tenemos a los objetos geométricos, que surgen naturalmente de los problemas más emblemáticos del área, como ser la resolución de ecuaciones diofánticas. Ejemplos típicos de estos elementos son las curvas elípticas y las variedades abelianas.

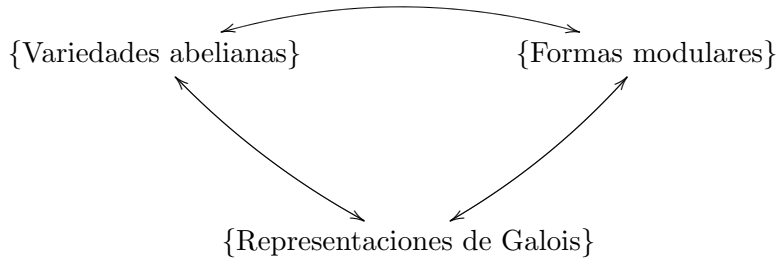
Este mundo es quizás el puente más angosto entre la teoría de números y la geometría algebraica. A pesar de que esta última pone a nuestra disposición un verdadero arsenal teórico, los problemas relacionados con estos objetos suelen ser particularmente difíciles.

Otro componente de esta estructura esta formado por los objetos relacionados con el cálculo. El estudio de elementos de índole esencialmente analítica, tales como las formas modulares o formas automorfas, prueba ser curiosamente fructífero para los problemas que nos interesan. Este universo se encuentra, en cierto modo, en las antípodas del anterior: su relación con los problemas de la teoría de números no es tan clara pero al mismo tiempo su funcionamiento se comprende mucho mejor.

Finalmente, existe un universo algebraico que, de alguna forma, sirve para vincular lo analítico y lo geométrico: el de las representaciones. La idea es sencilla, asociar a nuestros objetos, tanto a los geométricos como a los analíticos, representaciones de ciertos grupos, poniendo a nuestra disposición una teoría muy rica y con muchos años de desarrollo.

En el presente trabajo, estos tres mundos aparecen representados por los que probablemente sean sus habitantes más conocidos: variedades abelianas, formas modulares y representaciones de Galois.

Debemos tener en mente un mapa de la forma:



y nos interesará entender que relaciones hay entre los distintos vértices del triángulo. Contrariamente a lo que la ilustración puede sugerir, no existen correspondencias uno a uno entre nuestros objetos, algunos universos son mucho mas grandes que otros.

No es difícil asociar a toda variedad abeliana una representación de Galois, de todas las rutas posibles de nuestro mapa esta es probablemente la más sencilla de transitar.

El primer paso importante en dirección a nuestro objetivo fue dado por Eichler y Shimura, que asociaron variedades abelianas a ciertas formas modulares ([DS05, Capítulo 9]). Varios años más adelante, Deligne, con la colaboración de Serre, fue un paso más adelante: construyó representaciones de Galois a partir de una familia mucho mas grande de formas modulares, coincidiendo en los casos de Eichler-Shimura con la representación ligada al objeto geométrico ([Del71], [DS74]).

Con estas construcciones nuestro mapa comenzó a estar más completo y fueron cobrando fuerza dos preguntas naturales: ¿qué objetos geométricos provienen del mundo modular? ¿y qué representaciones?.

Estas preguntas plantearon desafíos notablemente difíciles y las respuestas dadas forman parte de los resultados más resonantes de los últimos años, en cuanto sirvieron para resolver varios problemas clásicos. El más famoso de ellos, claro está, es el último Teorema de Fermat.

Las respuestas a las que hacemos referencia consisten, básicamente, en dos teoremas.

Por un lado, tenemos la conjetura de Taniyama-Shimura, hoy llamada Teorema de Modularidad, que afirma que toda curva elíptica definida sobre $\mathbb{Q}$ puede obtenerse a partir de una forma modular. Finalmente probada

por Breuil en 2001, quien completó los trabajos previos de Taylor, Wiles, Conrad, et al., esta conjetura mantuvo en vilo a muchos de los matemáticos más reconocidos del área en los últimos años, probablemente por su fuerte conexión con el teorema de Fermat, encontrada por Frey y Ribet entre otros.

Relacionado con la segunda pregunta, aparece el tema central de esta presentación: la conjetura de Serre. Esta asegura que ciertas representaciones con imagen en cuerpos finitos provienen de formas modulares. Se trata de un trabajo muy reciente, ya que fue probada en un primer caso por Dieulefait en [Die07] y por Khare y Wintenberger en [KW09a] independientemente, y luego con total generalidad por Khare y Wintenberger (en [KW09b] y [KW09c]).

Vale destacar que estamos hablando de un resultado aún más fuerte que el Teorema de Modularidad. En su paper original ([Ser87]) Serre da una prueba de como su conjetura implica el Último Teorema de Fermat. Más aún, es posible derivar de ella la misma conjetura de Taniyama-Shimura.

Estos resultados marcaron sin dudas dos hitos en el estudio de la teoría de números dentro de la filosofía que planteamos. Sin embargo, es preciso notar que se trata solo del primer paso de un largo camino. Las generalizaciones posibles son variadas y probablemente la mayor importancia de ambos teoremas radique en que marcan el camino a seguir. En lo que a la formulación de nuevas preguntas refiere, son sin dudas un ejemplo del espíritu de los resultados que deben buscarse.

En cuanto al presente trabajo, los primeros dos capítulos intentarán presentar la teoría de formas modulares y de representaciones de Galois, teniendo siempre como meta final el comprender el contenido de la conjetura de Serre. En el último capítulo, enunciaremos precisamente la conjetura en sus dos versiones y presentaremos alguna generalización.

Índice general

Capítulo 1

Representaciones de Galois

En esta sección presentaremos generalidades sobre la teoría de representaciones de Galois, segundo ingrediente fundamental en la formulación de la conjetura de Serre. Introduciremos las definiciones básicas del tema teniendo en mente los ejemplos que nos interesan.

1.1. Definiciones

1.1.1. Grupos de Galois de extensiones finitas

Comenzamos recordando parte de la estructura de los grupos de Galois de cuerpos de números.

Dada una extensión finita de cuerpos de números (aquellos que son extensiones finitas de $\mathbb{Q}$) L/K podemos considerar los respectivos anillos de enteros O_L y O_K. Recordemos que los primos de estos anillos de enteros están relacionados, para cada primo $p \in O_K$, el ideal pO_L se factoriza como producto de ideales primos de O_L ([Mar77]). Por otro lado, cada ideal primo $\wp \subset O_L$ aparece en la factorización de exactamente un primo de O_K, precisamente de $p = \wp \cap O_K$. Diremos que en este caso $\wp$ divide a p o está sobre p, la notación será $\wp | p$.

Sea $K/\mathbb{Q}$ una extensión finita y Galois. Dado un primo $p \in \mathbb{Z}$ y un primo $\wp | p$ de O_K definimos los siguientes subgrupos del grupo de Galois $G = \mathrm{Gal}(K/\mathbb{Q})$:

$D_\wp = \{\sigma \in G : \sigma(\wp) = \wp\}$, el subgrupo de descomposición en $\wp$.
$I_\wp = \{\sigma \in G : \sigma(x) \equiv x \,(mod\, \wp)\ \forall x \in O_K\}$, el subgrupo de inercia en $\wp$.

Recordemos que todo primo de O_K tiene asociada una valuación $v_\wp$ (definida como: $v_\wp(x) = \alpha$ tal que $\wp^{-\alpha} \cdot x$ es un ideal incluido en O_K no divisible por $\wp$) que induce un valor absoluto en K. Siempre podemos considerar la completación de K respecto de tal valor absoluto (cuerpo al que llamaremos $K_\wp$) que resulta ser una extensión finita de $\mathbb{Q}_p$, siendo el subgrupo de descomposición isomorfo a $\mathrm{Gal}(K_\wp/\mathbb{Q}_p)$.

El anillo de enteros $O_\wp$ de $K_\wp$ tiene un único ideal maximal $M_\wp$, lo que permite definir un morfismo

$$O_\wp \to O_\wp/M_\wp \cong \mathbb{F}_q \text{ un cuerpo finito al que llamaremos } \mathbb{F}_\wp.$$

Este morfismo induce una aplicación entre los grupos de Galois:

$$\mathrm{Gal}(K_\wp/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{F}_\wp/\mathbb{F}_p).$$

Este último morfismo es sobreyectivo pero no necesariamente inyectivo, de hecho su núcleo es el subgrupo formado por los elementos de $\mathrm{Gal}(K_\wp/\mathbb{Q}_p)$ que dejan fijos a los elementos de $O_\wp$ módulo $M_\wp$. Si lo componemos con el isomorfismo entre $\mathrm{Gal}(K_\wp/\mathbb{Q}_p)$ y $D_\wp$ obtenemos pasando al cociente por el núcleo un isomorfismo:

$$\phi_\wp : \frac{D_\wp}{I_\wp} \to \mathrm{Gal}(\mathbb{F}_\wp/\mathbb{F}_p).$$

Recordemos que para los cuerpos finitos, los grupos de Galois de extensiones finitas son siempre cíclicos. Más aún, el grupo de Galois de una extensión de cuerpos finitos $\mathbb{F}_{q^n}/\mathbb{F}_q$ está siempre generado por un elemento distinguido, el morfismo de Frobenius. Este morfismo está definido como $F(x) = x^q$.

Esto permite definir, cada vez que $I_\wp = 0$, un elemento distinguido en $D_\wp$, la preimagen de F. Llamaremos a este elemento $Frob_\wp$. Si $\wp$ y $\wp'$ son dos primos distintos sobre p, los elementos $Frob_\wp$ y $Frob_{\wp'}$ son conjugados vía cualquier morfismo que cumpla $\sigma(\wp) = \wp'$. Notaremos entonces $Frob_p$ a la clase de conjugación de $Frob_\wp$. Por la observación anterior esta definición tiene sentido, ya que la clase no depende del primo $\wp$ elegido.

Para pruebas y detalles sobre estas construcciones, se puede consultar [Mar77] y [Neu99].

1.1.2. Grupos de Galois de extensiones infinitas

Queremos dar nociones de grupo de descomposición, inercia y morfismos de Frobenius en el caso de una extensión $K/\mathbb{Q}$ no necesariamente finita. Utilizaremos algunas definiciones y resultados sobre teoría de Galois infinita, que pueden ser encontrados en [Mil08].

Recordemos que si $K/\mathbb{Q}$ es una extensión infinita entonces K es la unión de todas sus subextensiones finitas y su grupo de Galois resulta:

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(F/\mathbb{Q}),$$

donde F recorre todas las subextensiones de $K/\mathbb{Q}$ con $F/\mathbb{Q}$ Galois y finitas. Este isomorfismo proviene de identificar un morfismo $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ con el elemento del límite $(\sigma|_F)_F$. En este mismo espíritu, dado un primo $p \subset \mathbb{Q}$, un primo de K sobre p es una sucesión de primos $(\wp_F)_F$, uno por cada subextensión finita de K, de modo que $\wp_{\mathbb{Q}} = p$ y si $F' \subseteq F$ entonces $\wp_F$ está sobre $\wp_{F'}$.

Se define entonces el subgrupo de descomposición de un primo $\wp \subset K$ como:

$$D_\wp = \varprojlim D_{\wp_F}$$

y el subgrupo de inercia:

$$I_\wp = \varprojlim I_{\wp_F}.$$

Nuevamente, ambas definiciones tienen sentido pues si $F' \subset F$ entonces $\wp_F \cap O_F = \wp_{F'}$ y por lo tanto si $\sigma \in D_{\wp_F}$ (respectivamente $I_{\wp_F}$) entonces $\sigma|_{F'} \in D_{\wp_{F'}}$ (respectivamente $I_{\wp_{F'}}$).

Teniendo definidos los subgrupos de descomposición e inercia buscamos morfismos similares a los del caso finito. Para eso necesitamos un reemplazo para la completación $K_\wp$, definimos:

Definición 1.1.1. *La completación de K respecto de $\wp$ se define como $K_\wp = \bigcup F_{\wp_F}$ con F recorriendo las subextensiones de K tales que $F/\mathbb{Q}$ es Galois y finita.*

Definición 1.1.2. *Definimos el cuerpo residual de K respecto de $\wp$ como $\mathbb{F}_\wp = \bigcup \mathbb{F}_{\wp_F}$ con F recorriendo las subextensiones de K tales que $F/\mathbb{Q}$ es Galois y finita.*

Con todos estos elementos, estamos en condiciones de enunciar:

Proposición 1.1.3. *Sean $K/\mathbb{Q}$ una extensión algebraica y Galois, p un primo de $\mathbb{Q}$ y $\wp$ un primo de K arriba de p. Entonces existen morfismos $\psi_\wp : D_\wp \to \mathrm{Gal}(K_\wp/\mathbb{Q}_p)$ y $\pi_\wp : \mathrm{Gal}(K_\wp/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{F}_\wp/\mathbb{F}_p)$ tales que $\psi_\wp$ es un isomorfismo y $\pi_\wp$ es un morfismo sobreyectivo con núcleo igual a $\psi_\wp(I_\wp)$.*

Esta proposición es consecuencia del siguiente lema:

Lema 1.1.4. *Sean $\alpha : \{G'_i, g'_{ij}\} \to \{G_i, g_{ij}\}$ y $\beta : \{G_i, g_{ij}\} \to \{G''_i, g''_{ij}\}$ morfismos entre sistemas proyectivos de grupos topológicos compactos y Hausdorff tales que la sucesión $G'_i \xrightarrow[\alpha_i]{} G_i \xrightarrow[\beta_i]{} G''_i$ es exacta para todo i. Entonces la sucesión:*

$$\varprojlim G'_i \xrightarrow{\alpha} \varprojlim G_i \xrightarrow{\beta} \varprojlim G''_i$$

es exacta.

Demostración. Sea $(x_i)_{i\in I}$ un elemento del núcleo de β, es decir tal que $\beta_i(x_i) = 1$ para todo i. Definamos los conjuntos $Y_i = \alpha_i^{-1}(x_i)$, estos resultan cerrados de G_i (y por lo tanto compactos) y no vacíos por la exactitud de la sucesión en i. Es posible probar, utilizando el teorema de Tychonoff y un argumento de compacidad, que el límite de espacios topológicos compactos y Hausdorff no vacíos es nuevamente un espacio compacto, Hausdorff y no vacío.

En virtud de ésto el conjunto $Y = \varprojlim Y_i$ es no vacío y como $\alpha(y) = (x_i)_{i\in I}$ para todo $y \in Y$, resulta que $(x_i)_{i\in I} \in Im(\alpha)$.

Esto prueba $\mathrm{Ker}(\beta) \subset Im(\alpha)$, la prueba de la otra contención consiste en verificar que $\beta \circ \alpha = 0$, pero esto es cierto pues $\beta_i \circ \alpha_i = 0$ para todo $i \in I$. □

Ahora sí, estamos en condiciones de probar la proposición:

Demostración. Observemos que de la definición de $K_\wp$ y $\mathbb{F}_\wp$ se deduce que $\mathrm{Gal}(K_\wp/\mathbb{Q}_p) \cong \varprojlim \mathrm{Gal}(L_{\wp_L}/\mathbb{Q}_p)$ y $\mathrm{Gal}(\mathbb{F}_\wp/\mathbb{F}_p) \cong \varprojlim \mathrm{Gal}(\mathbb{F}_{\wp_L}/\mathbb{F}_p)$ donde L recorre todas las subextensiones de $K/\mathbb{Q}$ tales que $L/\mathbb{Q}$ es finita y Galois. Podemos definir entonces un morfismo

$$\psi_\wp : D_\wp \to \mathrm{Gal}(K_\wp/\mathbb{Q}_p),$$

como límite de las aplicaciones $\psi_{\wp_F} : D_\wp \to D_{\wp_F} \to \mathrm{Gal}(F_{\wp_F}/\mathbb{Q}_p)$ (donde el morfismo entre los grupos de descomposición es la restricción). De forma análoga podemos definir un morfismo $\pi_\wp : \mathrm{Gal}(K_\wp/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{F}_\wp/\mathbb{F}_p)$.

Recordemos que el grupo de Galois de una extensión de $\mathbb{Q}$ tiene una topología natural a saber la de Krull. Dicha topología es la topología discreta en el caso de extensiones finitas, y en el caso no finito es la que hace que las proyecciones a las subextensiones finitas sean siempre continuas, o equivalentemente, al pensar una extensión como límite de subextensiones finitas, es la inducida por el límite inverso.

Luego podemos hacer uso del lema, que nos dice por un lado que el morfismo ϕ es un isomorfismo, por la exactitud de

$$0 \longrightarrow D_\wp \xrightarrow{\psi_\wp} \mathrm{Gal}(K_\wp/\mathbb{Q}_p) \longrightarrow 0 \ ,$$

y por otro lado que π es sobreyectivo y su núcleo es $\phi(I_\wp)$, por la exactitud de

$$0 \longrightarrow I_\wp \xrightarrow{\psi_\wp} \mathrm{Gal}(K_\wp/\mathbb{Q}_p) \xrightarrow{\pi_\wp} \mathrm{Gal}(\mathbb{F}_\wp/\mathbb{F}_p) \longrightarrow 0 \ .$$

□

Observemos que los morfismos ϕ y π construidos satisfacen que el siguiente diagrama:

$$\begin{array}{ccccc} D_\wp & \xrightarrow{\psi_\wp} & \mathrm{Gal}(K_\wp/\mathbb{Q}_p) & \xrightarrow{\pi_\wp} & \mathrm{Gal}(\mathbb{F}_\wp/\mathbb{F}_p) \\ \downarrow & & \downarrow & & \downarrow \\ D_{\wp_L} & \longrightarrow & \mathrm{Gal}(L_{\wp_L}/\mathbb{Q}_p) & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{\wp_L}/\mathbb{F}_p) \end{array} \ , \tag{1.1}$$

es conmutativo para toda L subextensión de K tal que $L/\mathbb{Q}$ es Galois y finita (y pasando al límite, para toda L subextensión de K).

Estamos ahora en una situación similar a la de las extensiones finitas, los morfismos construidos inducen un isomorfismo:

$$\phi_\wp : \frac{D_\wp}{I_\wp} \to \mathrm{Gal}(\mathbb{F}_\wp/\mathbb{F}_p).$$

Como mencionamos en la prueba de la Proposición 1.1.3, el grupo de Galois de una extensión L/K siempre puede ser dotado de una topología, llamada topología de Krull.

Por otro lado, en el caso de una extensión de un cuerpo finito, $\mathbb{F}/\mathbb{F}_q$, podemos definir en $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$ un morfismo de Frobenius F, de la misma forma que en el caso finito, a saber $F(x) = x^q$. Este morfismo resulta ser límite de los morfismos de Frobenius de las subextensiones de $\mathbb{F}$ finitas sobre $\mathbb{F}_q$. Si bien en este caso $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$ no resulta ser el grupo generado por F, sí lo es

topológicamente. Precisamente, $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q) = \overline{\langle F \rangle}$ la clausura topológica del subgrupo generado por F. Esto es consecuencia de que $\pi_L(\langle F \rangle) = \mathrm{Gal}(L/\mathbb{F}_q)$ para toda L subextensión de $\mathbb{F}$ finita sobre $\mathbb{F}_q$.

Entonces podemos, siempre que $I_\wp = 0$, definir en $D_\wp$ un elemento distinguido, que llamaremos $Frob_\wp$, como la preimagen del Frobenius. Nuevamente, vale que dados dos primos $\wp$ y $\wp'$ sobre un mismo primo p, existe un morfismo que envía uno en el otro. Resulta también que la conjugación por ese morfismo es un isomorfismo entre $D_\wp$ y $D_{\wp'}$ que envía $Frob_\wp$ a $Frob_{\wp'}$. Tenemos entonces, al igual que en el caso finito, que los elementos de Frobenius de los primos sobre un primo fijo p forman una clase de conjugación de $\mathrm{Gal}(K/\mathbb{Q})$ a la que llamaremos $Frob_p$.

Ahora, observemos que dada una subextensión E de K, la proyección $\mathrm{Gal}(\mathbb{F}_\wp/\mathbb{F}_p) \to \mathrm{Gal}(\mathbb{F}_{\wp_E}/\mathbb{F}_p)$ envía el Frobenius de K al Frobenius de E, entonces, en virtud de la conmutatividad del Diagrama 1.1, resulta que la proyección $D_\wp \to D_{\wp_E}$ envía $Frob_\wp$ en $Frob_{\wp_E}$, es decir la elección de elementos distinguidos en los grupos de descomposición se hace de forma compatible.

1.1.3. Representaciones de Galois

Ya estamos en condiciones de definir las representaciones de Galois y ciertas nociones asociadas.

Definición 1.1.5. *Una representación de Galois es un morfismo continuo:*

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(k),$$

donde k es un cuerpo (usualmente $k = \mathbb{C}$, $\overline{\mathbb{Q}_p}$ o $\overline{\mathbb{F}_p}$).

En la definición, la topología en $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ es la de Krull y la topología de $\mathrm{GL}_n(k)$ es la inducida por la topología usual de k.

Antes que nada, fijemos ciertos nombres, llamaremos a las representaciones:

- p-ádicas, cuando $k = \overline{\mathbb{Q}_p}$,
- de Artin, cuando $k = \mathbb{C}$,
- módulo p, cuando $k = \overline{\mathbb{F}_p}$.

Además, denotaremos por $G_{\mathbb{Q}}$ al grupo $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. En general, llamaremos G_K a $\mathrm{Gal}(\overline{K}/K)$.

Hay una propiedad importante de estos tres tipos de representaciones: en los tres casos la imagen está controlada de alguna manera. Siendo más precisos, valen las siguientes tres proposiciones:

Proposición 1.1.6. *La imagen de cualquier representación ρ módulo p está contenida en $\mathrm{GL}_n(\mathbb{F}_q)$ donde $\mathbb{F}_q$ es alguna extensión finita de $\mathbb{F}_p$. En otras palabras, es finita.*

Demostración. Observemos que la topología de $\overline{\mathbb{F}_p}$ es discreta: por un lado un conjunto es abierto allí si y solo si su intersección con los subcuerpos finitos es siempre abierta. Tenemos entonces que cualquier conjunto resulta abierto, pues su intersección con cualquier cuerpo finito en $\overline{\mathbb{F}_p}$ es siempre abierta (la topología de éstos es discreta).

Luego, la topología de $\mathrm{GL}_n(\overline{\mathbb{F}_p})$ también es discreta (es la topología producto, pensándolo como subespacio de $\overline{\mathbb{F}_p}^{n\times n}$). Por otro lado, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ es compacto y ρ es continua, por lo que la imagen de ρ es un subconjunto compacto de un espacio discreto y por lo tanto es finita. □

Proposición 1.1.7. *Toda representación de Artin tiene imagen finita.*

Demostración. Tenemos en $\mathrm{GL}_n(\mathbb{C})$ la norma de operador, definida como $\|T\| = \sup_{v\in\mathbb{C}^n} \|Tv\|$. Como ρ es continua, podemos elegir un subgrupo abierto $U \subseteq G_{\mathbb{Q}}$ de forma que $\rho(U)$ esté incluido en la bola de radio $\frac{1}{2}$ y centro Id.

Supongamos ahora que existe un $u \in U$ tal que $\rho(u) \neq Id$, llamemos $T = \rho(u)$. Si T tiene un autovalor $\lambda \neq 1$, tomemos v un autovector de norma 1 y observemos que:

$$\|T^n - Id\| \geq \|(T^n - Id)(v)\| = \|\lambda^n.v - v\| = |\lambda^n - 1| \geq \frac{1}{2},$$

para un n suficientemente grande, esto es absurdo pues T^n está en $\rho(U)$. Por otro lado, si el único autovalor de T es 1, la forma de Jordan de T (llamémosla J) tiene unos en la diagonal y alguna entrada debajo de la diagonal igual a 1. Luego, la matriz $J - Id$ tiene norma mayor o igual a 1 y resulta:

$$\|T - Id\| = \|J - Id\| \geq \frac{1}{2}.$$

Lo que es absurdo, por lo que $\rho(U) = \{Id\}$.

Finalmente, al ser U un subgrupo abierto, tiene índice finito en $G_{\mathbb{Q}}$, de donde $\rho(U) = \{0\}$ tiene índice finito en $Im(\rho)$ y por lo tanto la imagen de ρ es finita. □

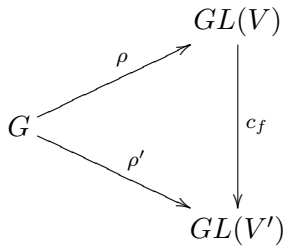
Proposición 1.1.8. *La imagen de cualquier representación p-ádica ρ está contenida en $\mathrm{GL}_n(F)$ donde F es una extensión finita de $\mathbb{Q}_p$. En general, esta imagen es infinita.*

Demostración. Utilizaremos el teorema de Baire, para eso primero debemos escribir a $\overline{\mathbb{Q}_p}$ como unión de numerables extensiones finitas de $\mathbb{Q}_p$.
La construcción es conocida y se puede realizar como sigue: primero podemos escribir a la máxima extensión no ramificada de $\mathbb{Q}_p$ (a la que llamaremos $\mathbb{Q}_p^{nr}$) como unión de $\mathbb{Q}_p[\omega_n]$, donde ω_n es una raíz n-ésima de la unidad y n es coprimo con p. Luego, $\overline{\mathbb{Q}_p}$ es la unión de las extensiones $\mathbb{Q}_p^{nr}[\sqrt[n]{p}]$ cuando n recorre los naturales.

Ahora, tenemos a $\overline{\mathbb{Q}_p} = \bigcup F_i$ y por lo tanto $\mathrm{GL}_n(\overline{\mathbb{Q}_p}) = \bigcup \mathrm{GL}_n(F_i)$. Además, cada $\mathrm{GL}_n(F_i)$ es un cerrado e $Im(\rho) = \bigcup \mathrm{GL}_n(F_i) \cap Im(\rho)$. De esta manera, $Im(\rho)$ es un compacto escrito como unión numerable de subespacios cerrados, por el teorema de Baire, alguno de estos subespacios debe tener interior no vacío, sea $\mathrm{GL}_n(F_r) \cap Im(\rho)$ un tal subespacio. Como además es un subgrupo, al tener interior no vacío resulta ser abierto y por lo tanto tiene índice finito en $Im(\rho)$. Se deduce de esto que $Im(\rho)$ está generado por $\mathrm{GL}_n(F_r) \cap Im(\rho)$ y finitos elementos $T_1, \ldots, T_s$ y por lo tanto está incluido en el generado por $\{\mathrm{GL}_n(F_r), T_1, \ldots, T_s\} \subseteq \mathrm{GL}_n(F)$ donde F es el cuerpo generado por F_r y los coeficientes de los T_i. □

Por último, notemos que dada una representación $\rho : G \to \mathrm{GL}_n(k)$, siempre podemos identificar a $\mathrm{GL}_n(k)$ con los automorfismos lineales de un k-espacio vectorial V (basta tomar $V = k^n$). Entonces, ρ le da a un tal V una acción de G compatible con la de k, en otras palabras, tener una representación ρ es equivalente a tener un kG-módulo V (aquí, kG es el álgebra de grupo).

El único detalle a remarcar es que esta equivalencia está bien definida salvo isomorfismo, dada una representación se pueden elegir varios espacios vectoriales y todos resultan isomorfos como kG-módulos. Diremos que dos representaciones son isomorfas, cuando los espacios vectoriales subyacentes son isomorfos como kG-módulos. No es difícil probar que en este caso, si $f : V \to V'$ es el isomorfismo de kG-módulos, el diagrama:



conmuta, donde c_f es la conjugación por f. A partir de ahora, notaremos indistintamente al conjunto de llegada de las representaciones como $\mathrm{GL}_n(k)$, $GL(V)$ o $Aut(V)$.

1.1.4. Ramificación

Nos interesa entender como se comportan las representaciones en cada primo, para eso definiremos la noción de ramificación.

Definición 1.1.9. *Dado un primo $p \in \mathbb{Z}$ y una representación de Galois $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$, decimos que ρ es no ramificada en p cuando $\rho(I_\wp) = \{Id\}$ para todo primo $\wp$ de $\overline{\mathbb{Q}}$ sobre p.*

Observemos que dados dos primos $\wp$ y $\wp'$ de $\overline{\mathbb{Q}}$ sobre un mismo p, los subgrupos $I_\wp$ y $I_{\wp'}$ son conjugados vía cualquier morfismo que envíe $\wp$ a $\wp'$. Por lo tanto, $I_\wp \subseteq \mathrm{Ker}(\rho)$ si y solo si $I_{\wp'} \subseteq \mathrm{Ker}(\rho)$. Esto quiere decir que para que ρ sea no ramificada en p basta con que $I_\wp \subseteq \mathrm{Ker}(\rho)$ para **algún** primo $\wp$ sobre p.

También es importante notar que cuando ρ no ramifica en p, podemos definir para cada primo $\wp$ sobre p al elemento $\rho(Frob_\wp)$ ya que la restricción $\rho : D_\wp \to \mathrm{GL}_n(K)$ pasa al cociente por $I_\wp$ y $Frob_\wp$ es justamente un elemento de $D_\wp/I_\wp$. Notamos $\rho(Frob_p)$ a los elementos formados por la imagen de la clase de conjugación $\{Frob_\wp : \wp | p\}$.

Por último, podemos relacionar la noción de ramificación de una representación de Galois con la noción tradicional de ramificación de un primo en una extensión de la siguiente forma:

Proposición 1.1.10. *Sea ρ una representación de Galois y $L/\mathbb{Q}$ la subextensión de $\overline{\mathbb{Q}}$ fija por $\mathrm{Ker}(\rho)$. Entonces ρ no ramifica en un primo p si y solo si p no ramifica en L*

Demostración. Sea $\pi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$ la proyección dada por la restricción a L. Sean, por otro lado, $\wp$ sobre $\wp_L$ sobre p primos de $\overline{\mathbb{Q}}$, L y $\mathbb{Q}$ respectivamente. Observemos que p no ramifica en L si y solo si $I_{\wp_L} = \{Id\}$. Por otro lado, $I_{\wp_L} = \pi(I_\wp)$, por lo que $I_{\wp_L} = \{Id\}$ si y solo si $I_\wp \subseteq \mathrm{Ker}(\pi) = \mathrm{Gal}(\overline{\mathbb{Q}}/L) = \mathrm{Ker}(\rho)$, es decir si y solo si ρ no ramifica en p. □

Con esta nueva caracterización de la ramificación podemos decir algo más sobre los primos que ramifican en una representación cualquiera. Notemos que manteniendo la notación de la proposición anterior, resulta que $Im(\rho) \cong G_\mathbb{Q}/\mathrm{Ker}(\rho) \cong \mathrm{Gal}(L/\mathbb{Q})$. Se tiene entonces, por las Proposiciones 1.1.6 y 1.1.7, que en los casos de representaciones módulo p y representaciones de Artin, la extensión $L/\mathbb{Q}$ es finita y por lo tanto ramificada en finitos primos. Esto nos dice que toda representación de Artin o módulo p ramifica solo en finitos primos.

La misma conclusión no se aplica a las representaciones p-ádicas, de hecho, existen representaciones con imagen en $\mathrm{GL}_n(\overline{\mathbb{Q}_p})$ que ramifican en infinitos primos (en [Ram99] se realiza un construcción). Este no es el caso que queremos estudiar, así que de aquí en adelante cada vez que hablemos de una representación p-ádica estaremos haciendo la suposición adicional de que ρ ramifica solo en finitos primos.

Apuntamos ahora a probar que las representaciones que nos interesan quedan determinadas por su valor en los Frobenius de los primos que no ramifican. Para eso, necesitamos utilizar el Teorema de Chebotarev, que enunciamos a continuación.

Definición 1.1.11 (Densidad)**.** *Sea L/K una extensión de cuerpos de números y Σ_K el conjunto de los primos de K. Dado un subconjunto $X \subseteq \Sigma_K$ definimos:*

$$a_n(X) = \#\{\wp \in X : N_{K/\mathbb{Q}}(\wp) \leq n\}.$$

Y decimos que X tiene densidad natural o aritmética d si:

$$\lim_{n\to\infty} \frac{a_n(X)}{a_n(\Sigma_K)} = d.$$

Una observación pertinente es que la densidad aritmética de un conjunto bien puede no existir. Un ejemplo es el de los primos de $\mathbb{Z}$ que tienen como primera cifra a 1. Es posible probar que este conjunto no tiene densidad.

Ahora sí, estamos en condiciones de enunciar el teorema:

Teorema 1.1.12 (Chebotarev)**.** *Sea L/K una extensión finita y Galois de cuerpos de números. Llamemos $G = \mathrm{Gal}(L/K)$ y sea $X \subseteq G$ un subconjunto estable por conjugación.*

Definamos $R_X = \{p \in \Sigma_K : Frob_p \subseteq X$ y p no ramifica en $L\}$. Entonces R_X tiene densidad aritmética $\#X/\#G$

La demostración excede los límites del presente trabajo, pero se puede encontrar material relacionado en [Ser89, I-7] y [Ser89, I-26].

El teorema tiene dos corolarios que nos interesan, la única observación que debemos hacer es que todo conjunto finito de primos tiene densidad cero, por lo tanto, los conjuntos de densidad positiva son siempre infinitos.

Corolario 1.1.13. *Dada L/K extensión finita y Galois de cuerpos de números y $g \in \mathrm{Gal}(L/K)$, existen infinitos $\wp \in \Sigma_L$ tales que $Frob_\wp = g$.*

Demostración. Sea X la clase de conjugación de g, Chebotarev asegura que hay infinitos primos $p \in \Sigma_K$ no ramificados en L tales que $Frob_p = X$ (vale la igualdad pues ambas son una clase de conjugación). El corolario queda probado pues por cada uno de estos primos, existe un $\wp|p$ tal que $Frob_\wp = g$. □

Corolario 1.1.14. *Sea L/K una extensión de cuerpos de números en la que ramifican finitos primos. Entonces los elementos de Frobenius de los primos no ramificados son densos en* $\mathrm{Gal}(L/K)$.

Demostración. Si L/K es finita, el corolario anterior prueba que los Frobenius cubren todo el grupo de Galois.

En el caso L/K infinita, recordemos que dado un elemento $g \in \mathrm{Gal}(L/K)$, los entornos básicos de g son de la forma $\pi^{-1}(\hat{g})$, donde $\hat{g} \in \mathrm{Gal}(E/K)$, y E es una subextensión de L/K Galois y finita sobre K y $\hat{g}$ es tal que $\pi(g) = \hat{g}$ con $\pi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ la proyección dada por la restricción. En otras palabras, tenemos por cada subextensión E de L/K Galois y finita sobre K un entorno básico de g, $U_E = \{\sigma \in \mathrm{Gal}(L/K) : \sigma|_E = g|_E\}$. Veamos que para cualquier E, existe un primo de L cuyo Frobenius está en U_E.

Aplicando Chebotarev en la extensión E/K sabemos que hay infinitos primos $\wp \in \Sigma_E$ tales que $Frob_\wp = g|_E$. Alguno de estos primos debe ser no ramificado en L, puesto que en L/E ramifican solo finitos primos (se deduce de que en L/K ramifican solo finitos primos). Sea $\wp$ un tal primo y $\hat{\wp}|\wp$ un primo en L. Como notamos al final de la Sección 2.1.2, $Frob_{\hat{\wp}}|_E = Frob_\wp = g|_E$, es decir $Frob_{\hat{\wp}} \in U_E$ como queríamos. □

Finalmente, veamos como estos dos corolarios se traducen en un resultado sobre representaciones:

Corolario 1.1.15. *Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ una representación de Galois que ramifica en finitos primos. Entonces ρ está determinada por los valores $\rho(Frob_{\wp})$, donde $\wp$ recorre todos los primos de $\overline{\mathbb{Q}}$ no ramificados en ρ.*

Demostración. Notemos nuevamente L al cuerpo fijo por $\mathrm{Ker}(\rho)$. Observemos que nuestra representación se factoriza por:

$$\overline{\rho} : \mathrm{Gal}(L/\mathbb{Q}) \cong G_{\mathbb{Q}}/\mathrm{Ker}(\rho) \to \mathrm{GL}_n(K),$$

quedando ρ determinada por $\overline{\rho}$. Por otro lado, nuestra hipótesis sobre la ramificación de ρ nos dice que en $L/\mathbb{Q}$ ramifican finitos primos, y en virtud del Corolario 1.1.14 los elementos de Frobenius son densos en $\mathrm{Gal}(L/\mathbb{Q})$. Por lo tanto, al ser $\overline{\rho}$ continua, queda determinada por los valores $\overline{\rho}(Frob_{\wp})$ donde $\wp$ recorre los primos de L arriba de primos $p \in \mathbb{Q}$ que no ramifican en ρ.

Solo resta notar que si $\hat{\wp}$ es un primo de $\overline{\mathbb{Q}}$ arriba de $\wp$ primo de L entonces $\rho(\hat{\wp}) = \overline{\rho}(\wp)$, por lo que ρ queda determinada por los valores de $\rho(\hat{\wp})$, donde $\wp$ recorre los primos de $\overline{\mathbb{Q}}$ arriba de primos $p \in \mathbb{Q}$ no ramificados en ρ. □

Por último resaltemos que no es necesario imponer a una representación con coeficientes en $\overline{\mathbb{Q}_p}$ que solo ramifique en finitos primos para que los elementos de Frobenius la determinen. Es posible probar que el conjunto de ramificación de una representación cayendo en $\mathrm{GL}_n(\overline{\mathbb{Q}_p})$ y cumpliendo ciertas condiciones extra tiene densidad cero, por lo que los Frobenius de los primos no ramificados la determinan (esto se encuentra hecho en [KR01]). Sin embargo esto no es cierto para toda representación, existen incluso casos patológicos que ramifican en todos los primos de $\mathbb{Q}$ (ver [Ser89, III-12])

1.2. Dos ejemplos

En esta sección daremos nuestros dos primeros ejemplos de representaciones p-ádicas: el caracter ciclotómico y las representaciones provenientes de curvas elípticas.

1.2.1. El caracter ciclotómico

Antes que nada fijemos un primo $p \in \mathbb{Q}$, vamos a construir una representación p-ádica con $n = 1$.

Para cada $i \in \mathbb{N}$ consideremos la extensión ciclotómica $\mathbb{Q}[\zeta_i] = K_i$ generada por ζ_i una raíz p^i-ésima de la unidad. Para cada uno de estos i tenemos una proyección:

$$\chi_p^{(i)} : G_{\mathbb{Q}} \to \mathrm{Gal}(K_i/\mathbb{Q}) \cong (\mathbb{Z}/p^i\mathbb{Z})^\times$$

y estos morfismos son compatibles entre sí (conmutan con las proyecciones que hay entre los K_i). Por lo tanto dan lugar a un morfismo:

$$\chi_p : G_{\mathbb{Q}} \to \varprojlim_{i\in\mathbb{N}} (\mathbb{Z}/p^i\mathbb{Z})^\times \cong \mathbb{Z}_p^\times.$$

Por otro lado éste es el mismo que se obtiene al hacer actuar a $G_{\mathbb{Q}}$ en $K = \bigcup K_i$, pues el limite inverso de grupos de Galois de extensiones contenidas cada una dentro de la siguiente es isomorfo al grupo de Galois de la unión.

Resaltemos que la identificación que estamos haciendo entre $\mathrm{Gal}(K_i/\mathbb{Q})$ y $(\mathbb{Z}/p^i\mathbb{Z})^\times$ no depende de ninguna elección, al morfismo que eleva las raíces primitivas a la k le corresponde la clase de k en $\mathbb{Z}/p^i\mathbb{Z}$.

Veamos que esta representación entra en la categoría de las que nos interesan, es decir, estudiemos su comportamiento en los primos. Recordemos que buscamos estudiar solo representaciones que ramifiquen en finitos primos.

Afirmamos que el caracter ciclótomico ramifica solo en p. Para ver eso, sea $q \neq p$ un primo de $\mathbb{Q}$, queremos ver que $I_Q \subseteq \mathrm{Ker}(\chi_p)$ para algún primo $Q|q$ de $\overline{\mathbb{Q}}$. Sea Q un tal primo y $\sigma \in I_Q$, $\chi_p(\sigma)$ queda definida por como actúa σ en cada K_i, más aún, por como actúa en cada ζ_i. Si Q_i es la restricción de Q a K_i, observemos que σ debe cumplir que:

$$\sigma(\zeta_i) \equiv \zeta_i \,(Q_i).$$

Como $\sigma(\zeta_i) = \zeta_i^k$ para algún k en $(\mathbb{Z}/p^i\mathbb{Z})^\times$, k debe satisfacer $\zeta_i^k - \zeta_i \in Q_i$, pero si $k \neq 1$ entonces $\zeta_i^k - \zeta_i = \zeta_i(\zeta_i^{k-1} - 1)$ que es un elemento de norma potencia de p y por lo tanto no puede estar en un primo arriba de q. Concluimos entonces que debe valer que para todo i, $\sigma(\zeta_i) = \zeta_i$, de donde σ actúa trivialmente en todos los K_i y resulta $\chi_p(\sigma) = Id$.

Hemos probado que para todo $q \neq p$, $\chi_p(I_Q) = \{Id\}$ para todo primo $Q|q$, es decir χ_p es no ramificada en q.

Finalmente, notemos que χ_p debe ramificar en p pues en caso contrario la extensión L fija por $\mathrm{Ker}(\chi_p)$ sería una extensión de $\mathbb{Q}$ que no ramifica en ningún primo, por lo que debería ser $L = \mathbb{Q}$. Pero esto implicaría que $\mathrm{Ker}(\chi_p) = G_{\mathbb{Q}}$, es decir que χ_p es trivial, lo que no es cierto.

Para terminar de caracterizar estas representaciones, podemos calcular el valor que toma en los elementos de Frobenius:

Sea $q \neq p$ un primo. Queremos calcular $\chi_p(Frob_q)$, la imagen de la clase de conjugación. Observemos que en este caso, al ser la imagen abeliana y los elementos de $\chi_p(Frob_q)$ todos conjugados, resulta que $\chi_p(Frob_q)$ consta de un solo elemento.

Tomemos entonces un primo $Q|q$ y calculemos $\chi_p(Frob_Q)$. Para eso, debemos estudiar la acción de $Frob_Q$ en las extensiones K_i, en otras palabras, queremos decir como actúa $Frob_{Q_i}$ en K_i (observemos que $Frob_Q$ no está bien definido en $G_{\mathbb{Q}}$, pero $Frob_{Q_i}$ sí lo está en $\mathrm{Gal}(K_i/\mathbb{Q})$).

Llamemos F_i a $Frob_{Q_i}$, sabemos que $F_i(\zeta_i) \equiv {\zeta_i}^q \, (Q_i)$, y podemos aplicar un argumento similar al que usamos para estudiar la ramificación. $F_i(\zeta_i) = \zeta_i^r$ para algún $r \in \mathbb{Z}/p^i\mathbb{Z}$ y la condición del Frobenius nos dice que r debe satisfacer que $\zeta_i^r - \zeta_i^q \in Q_i$, pero si $r \neq q$ (en $\mathbb{Z}/p^i\mathbb{Z}$), se tiene $\zeta_i^r - \zeta_i^q = \zeta_i^q(\zeta_i^{r-q} - 1)$ que tiene norma potencia de p y por lo tanto no puede estar en un ideal arriba de q.

La conclusión es que $Frob_Q$ actúa en los K_i elevando las raíces primitivas a la q, es decir como el elemento $q \in \mathbb{Z}/p^i\mathbb{Z}$. Luego se identifica con el elemento $q \in \mathbb{Z}_p$ en el límite, en otras palabras $\chi_p(Frob_q) = q$.

1.2.2. Representaciones provenientes de curvas elípticas

Otra familia importante de representaciones es la proveniente de los puntos de torsión de curvas elípticas.

Haremos una pequeña introducción a la teoría de curvas elípticas, enunciando los resultados que vamos a utilizar. Una buena introducción al tema es presentada en [TS92] y [Sil09] sirve como material de referencia.

Una curva elíptica $E/\mathbb{Q}$ definida sobre $\mathbb{Q}$ es una curva que se puede dar por una ecuación de la forma:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2}$$

donde $a_1, \ldots, a_6$ son números racionales y $x^3 + a_2x^2 + a_4x + a_6$ es un polinomio con raíces simples.

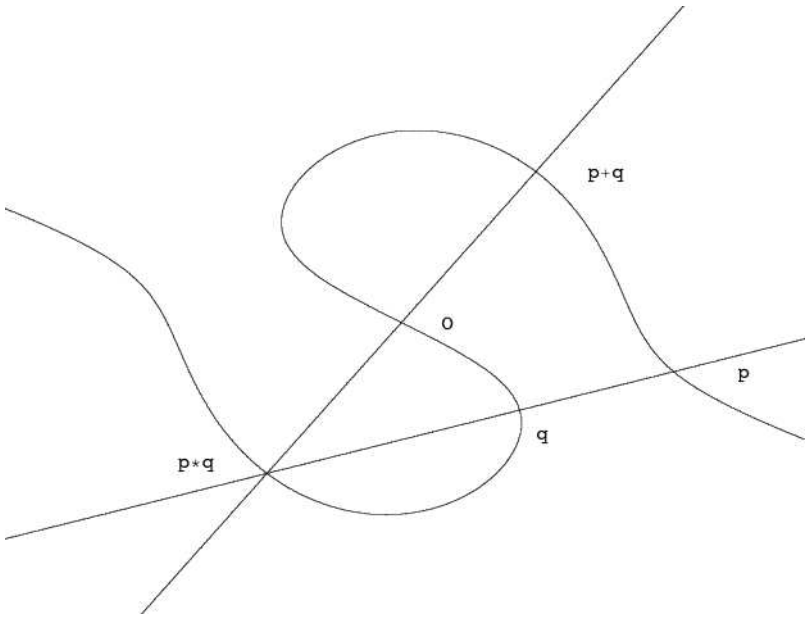
En un principio, intentamos buscar puntos (x, y) con coordenadas en $\mathbb{Q}$ que cumplan esta ecuación. Resolver este tipo de problemas fue la piedra fundamental para el estudio de estos objetos. Sin embargo, para comprenderlos, a menudo resulta fructífero analizar las soluciones en distintos cuerpos. En principio, tiene sentido hablar de una solución a una ecuación como 1.2 con coordenadas en cualquier cuerpo K que sea una extensión de $\mathbb{Q}$. Pero se puede ir mas lejos, pues siempre se puede limpiar denominadores para

obtener una ecuación en $\mathbb{Z}$, con lo que podemos plantear la existencia de soluciones en los cuerpos finitos $\mathbb{F}_p$ a la reducción módulo p de la ecuación.

Todo esto debe ser planteado con cierto cuidado, pero para nuestros fines solo diremos que dado un cuerpo K, llamamos puntos racionales de E sobre K al conjunto de soluciones en K a la ecuación que define a E. Notaremos a este conjunto $E[K]$.

Observemos que al reducir coeficientes módulo p podemos obtener una curva singular, es decir, tal que el polinomio a la derecha de la igualdad tenga una raíz múltiple. En este caso, decimos que p es un primo de mala reducción para E. Notemos que esto sucede si y solo si p divide al discriminante del polinomio en cuestión. Por lo tanto, los primos de mala reducción son finitos y tiene sentido definir el invariante $N(E)$ como su producto.

Uno de los aspectos más salientes de las curvas elípticas es que siempre es posible definir en $E[K]$ una ley de grupo. Sobre $\mathbb{Q}$ o $\mathbb{R}$ esta ley puede definirse de forma geométrica como sigue: primero fijamos un punto racional O cualquiera. Luego, dados dos puntos P y Q, definimos su suma $P + Q$ como muestra la ilustración:



Por supuesto, esto es solo una interpretación geométrica que se puede traducir algebraicamente. Así, la definición dada es equivalente a decir que

$P + Q$ es un punto de $\mathbb{Q}^2$ o $\mathbb{R}^2$ cuyas coordenadas son iguales a ciertas funciones polinomiales con coeficientes en $\mathbb{Z}$ de las coordenadas de P y Q. Es esta última la forma de definir la ley que puede trasladarse al caso de un cuerpo cualquiera K. Lo que debemos rescatar aquí es que dados $E/\mathbb{Q}$ una curva elíptica y K un cuerpo, el conjunto de puntos racionales $E[K]$ tiene una estructura de grupo de forma que la operación está definida por ciertas funciones polinomiales con coeficientes en $\mathbb{Z}$.

Una característica notable de la ley de grupo definida en $E[K]$ es que siempre que K sea un cuerpo de números, el grupo $E[K]$ resulta ser finitamente generado. Este resultado es conocido como el Teorema de Mordell-Weil y es uno de los resultados básicos mas importantes en lo que a curvas elípticas se refiere.

Otro resultado, que será importante para construir nuestras representaciones, es el que nos habla de la estructura de $E[\mathbb{C}]$. Lo que vale es que existe un retículo R de $\mathbb{C}$ (es decir, un $\mathbb{Z}$-módulo de rango 2 que genera todo $\mathbb{C}$ como $\mathbb{R}$-espacio vectorial) tal que $E[\mathbb{C}]$ es isomorfo al cociente $\mathbb{C}/R$. Geométricamente, lo que tenemos es un toro (la idea de la demostración se encuentra en [TS92, II.2.], para una prueba detallada se puede ver [Sil09, VI.5.]).

Esta caracterización tiene como consecuencia el siguiente hecho, si definimos $E[n] \subset E[\mathbb{C}]$ como el subgrupo de puntos que se anulan al repetir la operación n veces (los llamaremos puntos de n-torsión) entonces

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Esto es consecuencia de que el subgrupo de puntos de n-torsión de un cociente como el que tenemos tiene esa estructura.

Con estas herramientas ya estamos en condiciones de construir nuestras representaciones. La idea de la construcción es hacer actuar a $G_{\mathbb{Q}}$ en los $E[n]$. Para esto, es clave observar que los elementos de $E[n]$ tienen coordenadas en $\overline{\mathbb{Q}}$. La razón por la que esto sucede es la siguiente, si fijamos el neutro del grupo en un punto racional O, un elemento P está en $E[n]$ si

$$P + P + \ldots + P = O,$$

que por lo que dijimos antes es equivalente a que los coeficientes de P satisfagan que al evaluar cierta función polinomial en ellos obtenemos un resultado

racional. Esto nos dice que las coordenadas de los puntos de n-torsión satisfacen ciertas ecuaciones con coeficientes en $\mathbb{Z}$ por lo que son algebraicos sobre $\mathbb{Q}$. Sabemos entonces que $E[n] \subset E[\overline{\mathbb{Q}}]$.

Por otro lado, $E[\overline{\mathbb{Q}}]$ tiene equipada una acción de $G_{\mathbb{Q}}$ dada por actuar coordenada a coordenada. Como E está definida por una ecuación polinomial con coeficientes en $\mathbb{Z}$, aplicar un morfismo de $G_{\mathbb{Q}}$ manda puntos racionales en puntos racionales. Además esta acción respeta la ley de grupo. Nuevamente, esto sucede porque la operación está definida por evaluar ciertos polinomios con coeficientes racionales en las coordenadas de los puntos, y los morfismos de $G_{\mathbb{Q}}$ conmutan con los polinomios de coeficientes racionales. Tenemos entonces que si $P \in E[n]$ y $\sigma \in G_{\mathbb{Q}}$

$$n\sigma(P) = \sigma(nP) = \sigma(O) = O,$$

es decir, $\sigma(P) \in E[n]$ o en otras palabras, para todo n, $G_{\mathbb{Q}}$ actúa en $E[n]$.

Construyamos a partir de estas acciones una representación p-ádica. Para eso, consideremos las acciones $G_{\mathbb{Q}} \curvearrowright E[p^n]$ para cada $n \in \mathbb{N}$ y el siguiente objeto:

$$T_p[E] = \varprojlim_{n \in \mathbb{N}} E[p^n],$$

donde el límite está siendo tomado respecto a los morfismos $[p] : E[p^{n+1}] \to E[p^n]$ dados por la multiplicación por p. Llamamos a $T_p[E]$ el módulo de Tate p-ádico de E. Como cada $E[p^n]$ es un $\mathbb{Z}/p^n\mathbb{Z}$-módulo de rango 2 y los morfismos respetan esta estructura, $T_p[E]$ resulta ser un $\mathbb{Z}_p$-módulo de rango 2.

Por otro lado, nuestra acción es consistente con los morfismos $[p]$, por lo que tenemos una acción $G_{\mathbb{Q}} \curvearrowright T_p[E]$. Eligiendo una base, esto nos da una representación

$$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p).$$

Esta representación refleja ciertas propiedades de la curva elíptica que solo mencionaremos. Por un lado, los primos que ramifican son p y los q que dividen a $N(E)$, el producto de los primos de mala reducción de la curva elíptica.

En cuanto a los Frobenius, dado un primo $q \nmid pN(E)$, $\rho_{E,p}(Frob_q)$ es un conjunto de elementos conjugados, por lo que tiene sentido hablar de su traza y su determinante. El resultado que se tiene es (ver [Sil09, V.2.3.1.] y [Sil09, VII.2])

$$det(\rho_{E,p}(Frob_q)) = q \quad \text{y} \quad tr(\rho_{E,p}(Frob_q)) = a_q,$$

donde $a_q = q + 1 - \#(E[\mathbb{F}_q])$ la cantidad de puntos racionales sobre $\mathbb{F}_q$.

1.3. Familias compatibles de representaciones

Es notable que en los dos ejemplos presentados en el capítulo anterior no construimos solo una representación de Galois, en ambos casos la construcción dio lugar a una familia de representaciones $\{\rho_p\}$, con p recorriendo los primos de $\mathbb{Z}$, que presenta ciertas características comunes entre sus miembros.

Es inspirado en estos ejemplos que presentamos el concepto de compatibilidad entre representaciones. En buena parte de los casos las representaciones p-ádicas aparecen en familias de este tipo, procederemos a dar las definiciones correspondientes. Recordemos que notamos Σ_K al conjunto de primos de un cuerpo K.

Definición 1.3.1. *Una representación p-ádica ρ se dice racional (respectivamente entera) si existe un conjunto finito $S \subset \Sigma_{\mathbb{Q}}$ tal que*

- *ρ es no ramificada fuera de S,*
- *si $p \notin S$, los coeficientes del polinomio característico de $\rho(Frob_p)$ están en $\mathbb{Q}$ (respectivamente en $\mathbb{Z}$).*

Observemos que los elementos de $\rho(Frob_p)$ son todos conjugados y por lo tanto su polinomio característico está bien definido. A partir de ahora notaremos lo notaremos $P_{\rho,\,p}$.

Observación 1.3.2. Así como trabajamos con representaciones de $G_{\mathbb{Q}}$, es posible estudiar representaciones de G_K donde $K/\mathbb{Q}$ es una extensión finita. Notemos que toda representación de $G_{\mathbb{Q}}$ induce por restricción una de G_K y si la original es racional (entera) entonces la restricción también lo es. Esto sucede porque los elementos de Frobenius de K son potencias de los de $\mathbb{Q}$.

Ejemplo 1.3.3. *χ_p y $\rho_{E,p}$ son enteras para todo primo p y toda curva elíptica $E/\mathbb{Q}$.*

Ya podemos definir la noción de compatibilidad entre representaciones.

Definición 1.3.4. *Consideremos dos representaciones de Galois racionales, ρ p-ádica y ρ' p'-ádica. Diremos que son compatibles si existe un conjunto $S \subset \Sigma_{\mathbb{Q}}$ finito tal que:*

- *ρ y ρ' son no ramificadas fuera de S,*
- *para todo $q \notin S$, $P_{\rho,q} = P_{\rho',q}$.*

Es preciso destacar que la hipótesis de la racionalidad de ρ y ρ' es necesaria para que esta definición tenga sentido, pues en principio $P_{\rho,q}$ tiene coeficientes en $\mathbb{Q}_p$ y $P_{\rho',q}$ en $\mathbb{Q}_{p'}$, situación en la que no tiene sentido pedir que sean iguales.

A partir de la definición de representaciones compatibles podemos extrapolar la noción de familia compatible de representaciones, existe sin embargo un concepto mas fuerte: el de familia estrictamente compatible. A continuación definimos ambos.

Definición 1.3.5. *Consideremos para cada primo p una representación de Galois p-ádica y racional ρ_p. Diremos que la familia $\{\rho_p\}_{p\in\mathbb{Z}}$ es compatible si para todo par de primos p y q, ρ_p y ρ_q son compatibles.*

Diremos que la familia $\{\rho_p\}_{p\in\mathbb{Z}}$ es estrictamente compatible si existe un conjunto finito $S \subset \Sigma_{\mathbb{Q}}$ tal que:

- *para todo $q \notin S \cup \{p\}$, ρ_p es no ramificada en q y $P_{\rho_p,q}$ tiene coeficientes racionales,*
- *para todo $q \notin S \cup \{p, p'\}$, $P_{\rho_p,q} = P_{\rho_{p'},q}$.*

Dada una familia estrictamente compatible, existe un S mínimo satisfaciendo ambas condiciones, llamamos a tal S el conjunto excepcional de la familia.

Ejemplo 1.3.6. Las familias $\{\chi_p\}$ y $\{\rho_{E,p}\}$ son familias estrictamente compatibles, la primera con conjunto excepcional $S = \emptyset$ y la segunda con $S = \{p \in \mathbb{Z} : p|N(E)\}$ el conjunto de primos de mala reducción de $E/\mathbb{Q}$.

La condición de compatibilidad, junto con ciertas hipótesis extra, hace que las representaciones estén unívocamente determinadas. El concepto que nos interesa estudiar es el de simplicidad o irreducibilidad.

Definición 1.3.7. *Diremos que una representación $\rho : G \to Aut(V)$ es simple o irreducible si el G-módulo asociado V no tiene ningún sub G-módulo no nulo, es decir si no existe ningún subespacio $W \subset V$ propio y no nulo tal que $g.W \subset W$ para todo $g \in G$. Diremos que una representación es semisimple si se descompone como suma directa de representaciones simples.*

Una representación racional cualquiera ρ no tiene por qué ser semisimple, sin embargo, siempre es posible construir una representación semisimple asociada. Además, dicha construcción resulta única. Probaremos esto en las siguientes proposiciones.

Proposición 1.3.8. *Dado G un grupo y $\rho : G \to \mathrm{GL}_n(K)$ una representación, existe una representación $\rho_{ss} : G \to \mathrm{GL}_n(K)$ semisimple tal que el polinomio característico de $\rho(g)$ es igual al de $\rho_{ss}(g)$ para todo $g \in G$.*

Demostración. Consideremos un G-módulo V asociado a la representación (es decir, pensemos a $\mathrm{GL}_n(K)$ como $Aut(V)$ con V un K espacio vectorial). Afirmamos que existe una cadena de G-módulos V_i tales que:

$$\{0\} = V_0 \subset V_1 \subset \ldots \subset V_r = V$$

y cada cociente V_{i+1}/V_i es simple.

Esto se consigue de la siguiente manera: tomemos como S_1 un sub G-módulo propio maximal. Para esto, comenzamos con cualquier submódulo S y a cada paso tomamos un submódulo propio que lo contenga. Como una cadena de este tipo dentro de V tiene largo a lo sumo dim V (a cada paso tomamos un subespacio vectorial de V) con este proceso llegamos a lo que buscamos. De este modo, V/S_1 no tiene submódulos propios, pues no existe ningún submódulo entre V y S_1. Procedemos de la misma manera en cada paso, construido S_i, tomamos S_{i+1} como un submódulo propio maximal de S_i. Como la dimensión sobre K de estos subespacios baja en cada paso, existe un r tal que $S_r = \{0\}$. Finalmente tomamos $V_i = S_{r-i}$.

Definimos entonces la semisimplificación de V como

$$V_{ss} = V_0 \oplus V_1/V_0 \oplus \ldots \oplus V_r/V_{r-1},$$

y la semisimplificación de ρ, ρ_{ss}, como la representación dada por la acción de G en V_{ss} (observemos que ρ_{ss} está definida salvo conjugación, pues distintas elecciones de una base de V_{ss} nos dan distintas representaciones ρ_{ss}, todas conjugadas).

Resta probar que para todo $g \in G$ los elementos $\rho(g)$ y $\rho_{ss}(g)$ tienen el mismo polinomio característico. Para eso observemos como se escribe la matriz de la multiplicación por g en una base particular, miremos $\{v_1, \ldots v_n\}$ base de V construida eligiendo primero una base de V_1, extendiendo a una de V_2, luego a una de V_3 y así sucesivamente hasta completar la base de V.

La base así construida cumple que para todo i existe un r_i tal que $\{v_1, \ldots, v_{r_i}\}$ es base de V_i y $\{\overline{v}_{r_i+1}, \ldots, \overline{v}_{r_{i+1}}\}$ es base de V_{i+1}/V_i. Resulta entonces que $\{\overline{v}_1, \ldots, \overline{v}_n\}$ es base de V_{ss}. Ahora, si miramos las matrices

de la multiplicación por $\rho(g)$ y $\rho_{ss}(g)$ en las bases definidas anteriormente, tenemos que:

$$[\rho(g)] = \begin{pmatrix} A_1 & * & * & * \\ 0 & A_2 & * & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & 0 & A_r \end{pmatrix} \quad \text{y} \quad [\rho_{ss}(g)] = \begin{pmatrix} A_1 & 0 & 0 & 0 \\ 0 & A_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & A_r \end{pmatrix}$$

donde los A_i son bloques cuadrados de lado $r_i - r_{i-1}$. Es evidente que estas matrices tienen el mismo polinomio característico. □

Esto prueba la existencia de una representación semisimple compatible con ρ, el problema es que para realizar esta construcción hicimos múltiples elecciones, por lo que no está garantizada la buena definición de ρ_{ss}. En general, es consecuencia del siguiente teorema:

Teorema 1.3.9 (Brauer-Nesbitt)**.** *Sea k un cuerpo, A una k-álgebra y V, V' dos A-módulos semisimples de dimensión finita sobre k. Si para todo $a \in A$ el polinomio característico de la multiplicación por a en V coincide con el de la multiplicación por a en V' entonces V y V' son isomorfos.*

Para una prueba se puede consultar [Wei03, 7.2.4]. En nuestro caso, el teorema se aplica pues tener una representación $\rho : G \to \mathrm{GL}_n(k)$ es lo mismo que tener un kG-módulo de dimensión n sobre k. Luego, al construir dos semisimplificaciones de ρ con elecciones distintas de los V_i estamos construyendo dos kG-módulos semisimples tales que los polinomios característicos de los $g \in G$ coinciden (y comparando matrices como en la demostración de la proposición, coinciden para todos los elementos de kG). Brauer-Nesbitt asegura entonces que los dos kG-módulos son isomorfos y por lo tanto las representaciones son conjugadas.

Cuando el cuerpo k tiene característica cero, una condición más débil garantiza que para que las representaciones sean conjugadas, es suficiente que las trazas de los elementos $\rho(g)$ coincidan (ver [Lan02, XVII 3.8.]). Gracias a esto podemos probar:

Proposición 1.3.10. *Dada ρ una representación de Galois p-ádica y racional y p' un primo, existe a lo sumo una representación p'-ádica, racional y semisimple compatible con ρ. En particular, la semisimplificación ρ_{ss} es la única representación p-ádica, racional y semisimple compatible con ρ.*

Demostración. Alcanza con probar que dos representaciones p-ádicas, semisimples y compatibles son isomorfas. Sean ρ y ρ' dos tales representaciones. Sabemos que para todo q primo fuera de un conjunto finito S, vale que $\rho(Frob_q)$ y $\rho'(Frob_q)$ tienen el mismo polinomio característico y por lo tanto la misma traza.

Sabemos entonces que $Tr(\rho)$ y $Tr(\rho')$ son dos funciones continuas de $G_{\mathbb{Q}}$ en $\mathbb{Q}_p$ que coinciden en un conjunto denso, esto implica que debe ser iguales. Luego, por la versión para característica cero de Brauer-Nesbitt, resulta que ρ y ρ' son isomorfas, como queríamos probar. □

Una última observación es que mediante estas proposiciones hemos probado que dada una representación p-ádica, existe a lo sumo una familia compatible a la que puede pertenecer. Como en nuestros ejemplos las representaciones aparecen siempre como parte de familias compatibles es natural preguntarse acerca de la existencia de tales familias para cualquier ρ. En [Die04] se prueba que bajo ciertas hipótesis, dada ρ una representación p-ádica, existe una familia compatible que la tiene como miembro.

1.4. El conductor de una representación

Estudiaremos un último invariante asociado a las representaciones de Galois: el conductor de Artin.

El conductor es una medida de la ramificación de una representación en los primos. Se define localmente en cada primo, por lo que daremos una definición en cuerpos locales y dada una representación de nuestro grupo de Galois de un cuerpo global encontraremos una forma de recolectar la información de cada primo mirando una representación de cuerpos locales adecuada.

Para dar su definición debemos profundizar un poco más en la estructura de los grupos de Galois definiendo los grupos de ramificación. Empezaremos dando estas definiciones en el caso de extensiones finitas y luego buscaremos una forma de pasar a extensiones infinitas. Recordemos que un cuerpo local es un cuerpo equipado de una valuación discreta v, completo respecto a esta y con cuerpo residual perfecto.

1.4.1. Los grupos de ramificación

Sea L/K una extensión Galoisiana de cuerpos locales, $[L : K] < \infty$, llamemos G a $\mathrm{Gal}(L/K)$ y v_K y v_L a las valuaciones de K y L respectivamente. Además M_K (respectivamente M_L) será el único ideal maximal de

O_K (O_L) y llamaremos a cualquier elemento que lo genere uniformizador local.

Notaremos $e_{L/K}$ y $f_{L/K}$ a los índices de ramificación e inercia de la extensión. Recordemos que $f_{L/K}$ es el grado de la extensión de los cuerpos residuales y $e_{L/K}$ es la potencia con la que el único ideal maximal de L divide al de K.

Así, las valuaciones v_L y v_K están normalizadas para que los uniformizadores locales tengan valuación uno, por lo que dado un $x \in K$, $v_L(x) = e_{L/K} v_K(x)$. Otra propiedad importante es que siempre $e_{L/K} f_{L/K} = [L : K]$. Un primer acercamiento a la teoría de cuerpos locales se puede encontrar en [Ser79] y [Neu99]. A lo largo del capítulo utilizaremos resultados que se pueden encontrar en ambas referencias.

Finalmente, sea p la característica de los cuerpos residuales. Los subgrupos de ramificación se definen como sigue.

Definición 1.4.1. *Para todo $s \in \mathbb{R}$,*

$$G_s = \{\sigma \in G : v_L(\sigma(a) - a) \geq s + 1 \ \ , \forall a \in O_L\}.$$

De la definición se deduce lo siguiente:

- $G_{-1} = G$.
- G_s es el subgrupo de inercia para todo $-1 < s \leq 0$.
- Llamaremos a G_1 subgrupo de inercia salvaje, como veremos mas adelante es el único p-Sylow de G_0.

Dada una extensión L/K con grupo de Galois $G = \mathrm{Gal}(L/K)$ tendremos dos notaciones posibles para los grupos de ramificación: G_i y $G_i(L/K)$.

Lema 1.4.2. *Los G_i son subgrupos normales de G.*

Demostración. Sea $\sigma \in G_s$, $\phi \in G$, entonces:

$$v_L(\phi\sigma\phi^{-1}(a) - a) = v_L(\phi(\sigma\phi^{-1}(a) - \phi^{-1}(a))) = v_L(\sigma\phi^{-1}(a) - \phi^{-1}(a)) \geq s+1$$

para todo $a \in O_L$. La última igualdad vale pues los morfismos del grupo de Galois preservan la valuación. Resulta entonces que $\phi\sigma\phi^{-1} \in G_s$ como queríamos. □

A fines de encontrar una forma de saber en que grupos de ramificación se encuentra un morfismo $\sigma \in \mathrm{Gal}(L/K)$ debemos estudiar la relación entre los anillos de enteros de L y K.

Proposición 1.4.3. *Sea L/K finita, entonces existe $x \in O_L$ tal que $O_L = O_K[x]$.*

Demostración. Comencemos por llamar $\mathbb{F}_L$ al cuerpo residual de L y $\mathbb{F}_K$ al de K. Observemos que si $x \in O_L$ es tal que $\mathbb{F}_L = \mathbb{F}_K[\overline{x}]$ entonces el conjunto $\{x^i {\pi_L}^j\}$ con $0 \leq i < f_{L/K}$ y $0 \leq j < e_{L/K}$ genera a O_L como O_K-módulo. Esto es consecuencia del lema de Nakayama, ya que por un lado es claro que sus clases generan a $O_L/\pi_K.O_L$ y π_K es el generador del ideal maximal de O_K.

Considerando esto, tomemos y tal que $\mathbb{F}_L = \mathbb{F}_K[\overline{y}]$. Sea $\widehat{m} \in \mathbb{F}_K[X]$ el polinomio minimal de $\overline{y}$ y $m \in K[X]$ algún levantado de $\widehat{m}$. Observemos que $\overline{m(y)} = \widehat{m}(\overline{y}) = 0$, lo que quiere decir que $v_L(m(y)) > 0$ pues su clase en el cuerpo residual es 0.

Ahora tenemos dos posibilidades, si $v_L(m(y)) = 1$ entonces $m(y)$ es un uniformizador local y como dijimos antes un conjunto de productos de potencias de y y $m(y)$ genera a O_L como O_K-módulo, de donde $O_L = O_K[y]$.

Si $v_L(m(y)) > 1$, tomemos un uniformizador π_L y sea $x = y + \pi_L$. Resulta que $\overline{x} = \overline{y}$ y:

$$m(x) = m(y + \pi_L) = m(y) + \pi_L m'(y) + \pi_L^2 z$$

para algún $z \in O_L$.

Notemos que por un lado $v_L(m(y)) > 1$ y $v_L(\pi_L^2 z) > 1$ y por otro, al ser $\overline{m'(y)} = \widehat{m}'(\overline{y}) \neq 0$ en el cuerpo residual, $m'(y)$ es una unidad y $v_L(\pi_L m'(y)) = 1$.

Deducimos de esto que $v_L(m(x)) = v_L(m(y) + \pi_L m'(y) + \pi_L^2 z) = 1$, es decir $m(x)$ es un uniformizador local y $\overline{x}$ genera la extensión residual por lo que, vía el mismo razonamiento que antes, $O_L = O_K[x]$ como queríamos. □

A partir de esto, podemos definir el siguiente invariante de σ.

Definición 1.4.4. *Sea $\sigma \in \mathrm{Gal}(L/K)$. Definimos $i_G(\sigma) = v_L(\sigma(x) - x)$, donde x es tal que $O_L = O_K[x]$.*

La buena definición de $i_G(\sigma)$ es consecuencia del siguiente lema.

Lema 1.4.5. *$\sigma \in G_s$ si y solo si $i_G(\sigma) \geq s + 1$.*

Demostración. Sea π_L un uniformizador local de O_L. Un σ está en G_s si y solo si actúa trivialmente en $O_L/({\pi_L}^{s+1}) \cong O_K[x]/({\pi_L}^{s+1})$ lo que sucede si y solo si $\sigma(x) \equiv x\,({\pi_L}^{s+1})$ que es lo mismo que decir $i_G(\sigma) \geq s + 1$. □

En el caso totalmente ramificado, se puede tomar un x particular, como afirma el siguiente lema.

Lema 1.4.6. *Si L/K es totalmente ramificada y π_L es un uniformizador local entonces $O_L = O_K[\pi_L]$*

Demostración. Probemos primero que $L = K[\pi_L]$, para eso, sea $m(X) = a_0 + a_1X + \ldots + a_rX^r$ el polinomio minimal de π_L y $n = [L : K]$. Observemos que si $r < n$ se tiene:

$$a_1\pi_L + \ldots + a_r{\pi_L}^r = -a_0 \in K,$$

pero $v_L(a_i)$ es múltiplo de n para todo i (pues $n = e$ el grado de ramificación de la extensión), por lo que las valuaciones de los $a_i\pi_L^i$ son todas distintas ($v_L(a_i\pi_L^i) \equiv i\,(mod\, n)$) y por lo tanto:

$$v_L(-a_0) = \min_{1\leq i\leq r} a_i\pi_L^i \neq 0\,(mod\, n),$$

lo que contradice que $a_0 \in K$. Por lo tanto $r = n$ y π_L genera a L.

Ahora, dado un $x \in O_L$, se escribe como $x = b_0 + b_1\pi_L + \ldots + b_s\pi_L^s$ con $a_i \in K$ y $s < n$. Queremos ver que $v_K(b_i) \geq 0$ (o lo que es lo mismo, que $v_L(b_i) \geq 0$), nuevamente $v_L(b_i)$ es múltiplo de n para todo i, de donde las valuaciones de los $b_i\pi_L^i$ son todas distintas. Por otro lado, si existe algún t para el que $v_L(b_t) < 0$ entonces $v_L(b_t\pi_L^t) = v_L(b_t) + v_L(\pi_L^t) < -n + t < 0$ y luego:

$$v_L(x) = \min_{0\leq i\leq s} v_L(b_i\pi_L^i) < 0,$$

lo que es absurdo, pues x es entero. Entonces todos los b_i son enteros y con esto hemos probado que $O_L = O_K[\pi_L]$ □

Con estas herramientas podemos tratar de entender un poco mejor la estructura de los grupos de ramificación. Los G_i son una filtración de G que está relacionada con la filtración $U_L^{(i)}$ de las unidades de O_L definida como:

$$U_L^{(i)} = \{x \in O_L : x \equiv 1\,(mod\, \pi_L^i)\}.$$

La relación que hay es la siguiente:

Lema 1.4.7. *Sea $s \geq 0$, entonces $\phi : G_s/G_{s+1} \to U_L^{(s)}/U_L^{(s+1)}$ definido por $\phi(\sigma) = \frac{\sigma(\pi_L)}{\pi_L}$ es un morfismo inyectivo que no depende de la elección del uniformizador π_L.*

Demostración. Antes que nada, observemos que podemos suponer que $K = L^{G_0}$ pues los grupos de ramificación para $s \geq 0$ son los mismos en ambas extensiones. Estamos entonces en el caso L/K totalmente ramificada.

Ahora, como L/K es totalmente ramificada, $O_L = O_K[\pi_L]$. Vale entonces que:

$$\begin{aligned} \sigma \in G_r \iff & \quad v_L(\sigma(\pi_L) - \pi_L) \geq r+1 \quad \iff \\ & \quad \sigma(\pi_L) \equiv \pi_L \,(mod\, \pi_L^{r+1}) \quad \iff \\ & \quad \tfrac{\sigma(\pi_L)}{\pi_L} \equiv 1 \,(mod\, \pi_L^r) \quad \iff \frac{\sigma(\pi_L)}{\pi_L} \in U_L^{(r)}. \end{aligned}$$

Esto prueba directamente que ϕ está bien definida y que es inyectiva. Resta ver que no depende del uniformizador elegido y de esto se deducirá que es morfismo. Sean entonces $\sigma \in G_s$ y π, π' dos uniformizadores. Sabemos que existe $u \in U_L$ tal que $\pi = u.\pi'$ y se tiene:

$$\frac{\sigma(\pi)}{\pi}\left(\frac{\sigma(\pi')}{\pi'}\right)^{-1} = \frac{\sigma(u)}{u} \equiv 1 \,(mod\, \pi_L^{s+1}),$$

donde la última implicación se debe a que $\sigma(u) \equiv u \,(mod\, \pi_L^{s+1})$.

Esto nos dice que $\frac{\sigma(\pi)}{\pi}$ y $\frac{\sigma(\pi')}{\pi'}$ son iguales en $U_L^{(s)}/U_L^{(s+1)}$ y por lo tanto ϕ no depende del uniformizador.

Por último, si $\sigma, \sigma' \in G_s$ se tiene:

$$\phi(\sigma \circ \sigma') = \frac{\sigma(\sigma'(\pi_L))}{\pi_L} = \frac{\sigma(\sigma'(\pi_L))}{\sigma'(\pi_L)}\frac{\sigma'(\pi_L)}{\pi_L} = \phi(\sigma)\phi(\sigma'),$$

y la última igualdad vale porque $\sigma'(\pi_L)$ es un uniformizador y ϕ no depende de cual se elija. □

Esto nos da cierta información sobre los G_i que se puede deducir de las propiedades de la filtración $U_L^{(i)}$. Recordemos que esta cumplía:

- $U_L^{(0)}/U_L^{(1)} \cong \mathbb{F}_L^{\times}$,
- $U_L^{(n)}/U_L^{(n+1)} \cong \mathbb{F}_L$ para todo $n \geq 1$.

Deducimos que $|G_0/G_1|$ divide a $p^r - 1$ para algún r y que para todo $i \geq 1$, $|G_i/G_{i+1}|$ es una potencia de p. Esto demuestra un resultado que enunciamos al principio de esta sección: G_1 es un subgrupo normal de G_0 y tiene como cardinal la máxima potencia de p que divide a $|G_0|$ (pues tiene índice coprimo con p). Es por lo tanto el único p-subgrupo de Sylow de G_0.

Queremos ahora dar una definición de los grupos de ramificación para una extensión arbitraria de un cuerpo local K. Inspirados en las definiciones

de grupos de descomposición e inercia en los casos de extensiones infinitas de un cuerpo de números, la idea será considerar el límite inverso de los grupos de ramificación de las subextensiones finitas. Sin embargo, ante esta primera idea surge un problema: los grupos de ramificación no se llevan bien con las proyecciones entre grupos de Galois, es decir, no es cierto que dada $E/L/K$ y $\pi : \mathrm{Gal}(E/K) \to \mathrm{Gal}(L/K)$ resulte $\pi(G_i^E) \subseteq G_i^L$.

Ante esta situación, definiremos, reacomodando los índices de los grupos de ramificación, otra filtración de G que se comporta bien con las proyecciones. Los próximos resultados apuntarán a realizar esa construcción.

Lema 1.4.8. *Dada L/K finita y F un cuerpo intermedio, vale:*

$$G_s(L/K) \cap \mathrm{Gal}(L/F) = G_s(L/F).$$

Demostración. Es inmediato de las definiciones. □

Proposición 1.4.9. *Sean L/K finita y Galois y F/K una subextensión Galois. Si $G = \mathrm{Gal}(L/K)$, $H = \mathrm{Gal}(L/F)$, $\sigma \in \mathrm{Gal}(F/K)$ entonces:*

$$i_{G/H}(\sigma) = \frac{1}{e_{L/F}} \sum_{\phi|_F = \sigma} i_G(\phi) = \frac{1}{e_{L/F}} \sum_{\tau \in H} i_G(\sigma'\tau),$$

donde los $\phi \in G$ y σ' es un levantado cualquiera de σ a G.

Demostración. Sean x tal que $O_L = O_K[x]$ e y tal que $O_F = O_K[y]$. Tenemos:

- $e_{L/F}.i_{G/H}(\sigma) = v_L(\sigma(y) - y)$,
- $i_G(\sigma') = v_L(\sigma'(x) - x)$.

Aquí $\sigma'|_F = \sigma$. Lo que queremos ver se traduce entonces en que los elementos:

$$a = \sigma'(y) - y \quad \text{y} \quad b = \prod_{\tau \in H} (\tau\sigma'(x) - x)$$

tienen la misma valuación. Para eso, veamos que $a|b$ y $b|a$:

Llamemos f al polinomio minimal de x sobre F. Resulta que $f(T) = \prod_{\tau \in H} (T - \tau(x))$. Por otro lado, consideremos $\sigma'(f)$ el polinomio que se obtiene al aplicar σ' coeficiente a coeficiente. Observemos que $\sigma'(f)(x) = \prod_{\tau \in H} (T - \tau\sigma'(x)) = b$ (aquí estamos usando que H es normal y por lo tanto $\sigma' H = H\sigma'$).

Tenemos entonces:

$$b = \sigma'(f)(x) = \sigma'(f)(x) - f(x) = \sum_{i=0}^{r} (\sigma'(a_i) - a_i)x^i.$$

Pero además $v_L(\sigma'(a_i) - a_i) = v_L(\sigma(a_i) - a_i) \geq i_{G/H}(\sigma) = v_L(\sigma'(y) - y)$. Esto quiere decir que $a = \sigma'(y) - y$ divide a $\sigma'(a_i) - a_i$ para todo i y por lo tanto divide a b. Finalmente, para ver que $b|a$:

Escribamos $y = g(x)$ con $g \in O_K[T]$. Tenemos entonces el polinomio $g(T) - y \in O_F[T]$ que se anula en x. Por lo tanto:

$$\begin{aligned} g(T) - y = f(T)h(T) \quad &\Longrightarrow \\ g(T) - \sigma'(y) = \sigma'(g)(T) - \sigma'(y) = \sigma'(f)(T)\sigma'(h)(T) \quad &\Longrightarrow \quad T = x \\ a = y - \sigma'(y) = \sigma'(f)(x).\sigma'(h)(x) = b.z. & \end{aligned}$$

Esto concluye la demostración. □

Para reindexar los grupos de ramificación precisamos ciertas funciones ϕ y ψ.

Sea L/K finita, notemos por g_i al cardinal del grupo de ramificación G_i. Consideremos primero la función $\alpha_{L/K} : [-1, \infty) \to [0, 1]$ dada por $\alpha_{L/K}(s) = \frac{1}{[G_0:G_s]} = \frac{g_s}{g_0}$. Y definamos

$$\phi_{L/K}(s) = \int_0^s \alpha_{L/K}(t)dt.$$

En otras palabras, $\phi_{L/K}$ es una función continua, lineal a trozos que cumple:

- $\phi_{L/K}(0) = 0$, más aun $\phi_{L/K}(t) = t$ para todo $t \in [-1, 0]$,
- $\phi'_{L/K}(s) = \frac{g_s}{g_0}$,
- $\phi_{L/K}(s) = \frac{1}{g_0}(g_1 + \ldots + g_{\lfloor s \rfloor} + (s - \lfloor s \rfloor)g_{\lceil s \rceil})$ si $s > 0$.

Lema 1.4.10. *Sea* $\theta(s) = -1 + \frac{1}{g_0} \sum_{\sigma \in G} \min\{i_G(\sigma), s + 1\}$. *Entonces* $\theta = \phi$.

Demostración. Observemos que ambas son funciones continuas y lineales a trozos. Entonces basta chequear que coinciden en 0 y que, en los puntos en los que son derivables, sus derivadas coinciden.

Se tiene, por un lado:

$$\theta(0) = -1 + \frac{1}{g_0}(\sum_{\sigma \in G_0} 1 + \sum_{\sigma \notin G_0} 0) = -1 + 1 = 0.$$

Y por otro, para $s \notin \mathbb{N}$:

$$\theta'(s) = \frac{\#\{\ \sigma \in G : i_G(\sigma) \geq s+1\}}{g_0} = \frac{\#\{\sigma \in G_s\}}{g_0} = \frac{g_s}{g_0} = \phi'(s).$$

Entonces debemos tener $\theta = \phi$. □

Probemos un último lema antes de hablar de los grupos de ramificación.

Lema 1.4.11. *Sean L/K extensión finita y Galois, F/K una subextensión de Galois. Sea $H = \mathrm{Gal}(L/F)$, $\sigma' \in \mathrm{Gal}(F/K)$ y tomemos σ una extensión de σ' a L tal que $i_{L/K}(\sigma)$ es máximo. Entonces:*

$$\phi_{L/F}(i_{L/K}(\sigma) - 1) = i_{F/K}(\sigma') - 1.$$

Demostración. En primer lugar, probaremos que si $\tau \in H$ entonces $i_{L/K}(\sigma\tau) = \min\{i_{L/K}(\sigma), i_{L/K}(\tau)\}$. Luego, haciendo uso de la Proposición 1.4.9 y el Lema 1.4.10 obtendremos el resultado.

Sea entonces $\tau \in H$ y $x \in O_L$ tal que $O_L = O_K[x]$, separemos en casos:

•*Si $i_{L/K}(\sigma) > i_{L/K}(\tau)$:*

$$\begin{aligned} i_{L/K}(\sigma\tau) &= v_L(\sigma\tau(x) - x) &&= v_L(\sigma(x) - x + \sigma(\tau(x) - x)) = \\ &= v_L(\tau(x) - x) &&= i_{L/K}(\tau). \end{aligned}$$

•*Si $i_{L/K}(\sigma) \leq i_{L/K}(\tau)$:*

Tanto σ como τ están en $G_{i_{L/K}(\sigma)-1}$, por lo tanto $\sigma\tau$ también. Entonces $i_{L/K}(\sigma\tau) \geq i_{L/K}(\sigma)$. Por otro lado, $\sigma\tau$ es un levantado de σ' y por la maximalidad de σ vale la otra desigualdad. Se tiene entonces $i_{L/K}(\sigma\tau) = i_{L/K}(\sigma)$.

Sabemos entonces que $i_{L/K}(\sigma\tau) = \min\{i_{L/K}(\sigma), i_{L/K}(\tau)\}$, luego por la Proposición 1.4.9:

$$i_{F/K}(\sigma') = \frac{1}{e_{L/F}} \sum_{\tau \in H} i_{L/K}(\sigma\tau) = \frac{1}{e_{L/F}} \sum_{\tau \in H} \min\{i_{L/K}(\sigma), i_{L/K}(\tau)\}.$$

Restando 1 a ambos lados, observando que $e_{L/F} = |H_0|$ y usando Lema 1.4.10 finalmente obtenemos:

$$i_{F/K} - 1 = \phi_{L/F}(i_{L/K}(\sigma) - 1).$$ □

Con esta proposición podemos entender la interacción de los grupos de ramificación con las proyecciones. Precisamente, vale:

Teorema 1.4.12 (Herbrand)**.** *Sean L/K extensión Galois y finita, F/K una subextensión Galois, $G = \mathrm{Gal}(L/K)$ y $H = \mathrm{Gal}(L/F)$. Llamemos π a la proyección de G en H. Entonces vale:*

$$\pi(G_s(L/K)) = \frac{G_s(L/K)H}{H} = G_{\phi_{L/F}(s)}(F/K).$$

Demostración. Notemos que $\sigma' \in G_sH/H$ si y solo si existe $\sigma \in G$ tal que $\sigma|_F = \sigma'$ y $i_{L/K}(\sigma) \geq s+1$. Como $\phi_{L/F}$ es creciente y biyectiva, esta última condición es equivalente a que $\phi_{L/F}(i_{L/K}(\sigma) - 1) \geq \phi_{L/F}(s)$.

Sea entonces σ la extensión de σ' a L con mayor $i_{L/K}(\sigma)$, tenemos por el lema anterior:

$$\begin{aligned} \sigma' \in \pi(G_s) \iff \quad & \phi_{L/F}(i_{L/K}(\sigma) - 1) \geq \phi_{L/F}(s) \quad \iff \\ & i_{F/K}(\sigma') - 1 \geq \phi_{L/F}(s) \quad \iff \sigma' \in G_{\phi_{L/F}}(s). \end{aligned}$$

Quedando el teorema probado. □

Con estas herramientas, estamos en condiciones de definir la reindexación de los grupos de ramificación. Llamamos $\psi_{L/K} = \phi_{L/K}^{-1}$ y definimos como:

$$G^t(L/K) = G_{\psi_{L/K}(t)}(L/K),$$

la numeración superior de los grupos de ramificación. Estos grupos sí funcionan bien con las proyecciones, para probarlo precisamos el siguiente resultado sobre ϕ:

Lema 1.4.13. *Sean L/K finita y Galois y F/K una subextensión Galois. Entonces $\phi_{L/K} = \phi_{F/K} \circ \phi_{L/F}$.*

Demostración. Nuevamente estamos comparando dos funciones lineales a trozos y continuas, por lo que será suficiente probar que coinciden en 0 y que, donde existen, sus derivadas son iguales.

Llamemos como antes $G = \mathrm{Gal}(L/K)$ y $H = \mathrm{Gal}(L/F)$. Identificamos a $\mathrm{Gal}(F/K)$ con G/H. Se tiene por el Teorema 1.4.12:

$$(G/H)_{\phi_{L/F}(s)} = G_sH/H \cong G_s/(G_s \cap H) \cong G_s/H_s.$$

Luego:

$$\begin{aligned} {\phi'}_{L/K}(s) = \frac{|G_s|}{|G_0|} = \frac{|H_s|}{|H_0|}\frac{|(G/H)_{\phi_{L/F}(s)}|}{|(G/H)_0|} = \\ = {\phi'}_{L/F}(s){\phi'}_{F/K}(\phi_{L/F}(s)) = (\phi_{F/K} \circ \phi_{L/F})'(s). \end{aligned}$$

Por otro lado, $\phi_{F/K}(\phi_{L/F}(0)) = \phi_{F/K}(0) = 0 = \phi_{L/K}(0)$, lo que termina de probar el lema.

□

Corolario 1.4.14. *Sean L, F y K, entonces $\psi_{L/K} = \psi_{L/F} \circ \psi_{F/K}$.*

Ya podemos probar lo que queríamos:

Proposición 1.4.15. *Sean L, F y K, $\pi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ la proyección, entonces:*

$$\pi(G^t(L/K)) = G^t(F/K).$$

Demostración. Manteniendo la notación del lema anterior, para todo t tenemos, por el Teorema 1.4.12:

$$\pi(G^t) = \pi(G_{\psi_{L/K}(t)}) = (G/H)_{\phi_{L/F}(\psi_{L/K}(t))},$$

pero por el Corolario 1.4.14:

$$(G/H)_{\phi_{L/F}(\psi_{L/K}(t))} = (G/H)_{\psi_{F/K}(t)} = (G/H)^t.$$ □

Observemos otras propiedades de la numeración superior de los grupos de ramificación, sea L/K finita y G su grupo de Galois:

- Si L/K es no ramificada entonces $\phi_{L/K} = \psi_{L/K}$.
- $G_0 = G^0$ y por lo tanto L/K es no ramificada si y solo si $G^0 = \{0\}$.
- El grupo de inercia salvaje $G_1 = \{0\}$ si y solo si $G_s = \{0\}$ para todo $s > 0$. Esto ocurre si y solo si $G^s = \{0\}$ para todo $s > 0$. En este caso decimos que L/K es mansamente ramificada.

Ahora que ya hemos definido la numeración superior de los grupos de ramificación y tenemos probado que se comportan bien con las proyecciones, podemos dar una definición para las extensiones infinitas.

Definición 1.4.16. *Sea L/K una extensión infinita, definimos los grupos de ramificación de L/K como:*

$$G^u(L/K) = \varprojlim_{L/F/K} G^u(F/K),$$

donde F recorre todas las subextensiones de L/K tales que F/K es finita y Galois.

1.4.2. El conductor

Como dijimos en un principio, definiremos el conductor de una representación en base a la acción de los grupos de ramificación. Primero en el caso local:

Definición 1.4.17. *Sea K un cuerpo local de característica residual p y $\rho : G_K \to GL(V)$ una representación, donde V es un F-espacio vectorial y F un cuerpo. Dado un subgrupo H de $GL(V)$, notaremos por V^H a los elementos de V que quedan fijos por todos los morfismos de H.*

Definimos el conductor de ρ como:

$$n(\rho) = \int_{-1}^{\infty} codim\, V^{\rho(G^u(\overline{K}/K))} du.$$

Y el exponente Swan de ρ como:

$$sw(\rho) = \int_{0}^{\infty} codim\, V^{\rho(G^u(\overline{K}/K))} du.$$

Hagamos algunas observaciones sobre la definición:

- Si L es el cuerpo fijo por el núcleo de ρ entonces nuestra representación se factoriza por una $\widehat{\rho} : \mathrm{Gal}(L/K) \to GL(V)$ y resulta:

  $$\rho(G^u(\overline{K}/K)) = \widehat{\rho}(\pi(G^u(\overline{K}/K))) = \widehat{\rho}(G^u(L/K)),$$

  es decir, el conductor depende solo de como actúan los grupos de ramificación de L/K.

- Si ρ no ramifica en (π_K) el primo de K, entonces L/K es no ramificada y $\rho(G^u(\overline{K}/K)) = \widehat{\rho}(G^u(L/K)) = \widehat{\rho}(0) = Id$ para todo $u > -1$. Reemplazando en la formula, resulta que en ese caso $n(\rho) = 0$.

- El conductor y el exponente Swan difieren en un término calculable, vale que $n(\rho) = sw(\rho) + \mathrm{codim}\, V^{\rho(G^0(\overline{K}/K))}$.

- En el caso en el que V tiene dimensión 1, los espacios $V^{\rho(G^u(\overline{K}/K)}$ tienen dimensión 0 o 1 dependiendo de si $G^u(\overline{K}/K) \subset \mathrm{Ker}(\rho)$ o no. Se cumple entonces que $sw(\rho)$ es el menor u tal que $G^u \subset \mathrm{Ker}(\rho)$.

- La definición que dimos puede tener un problema: la integral no tiene por qué converger. En el caso de una representación de Artin o una representación módulo p la extensión L/K es finita y los grupos de ramificación son eventualmente triviales por lo que esto no es un problema.

Cuando la representación es p-ádica, la integral también es convergente, como puede verse en [Wie08, 3.1.].

- Una pregunta pertinente es cuando cambian los grupos de ramificación, es decir: ¿para qué valores de u vale que los grupos $G^{u-\epsilon}$ y $G^{u+\epsilon}$ son distintos para todo $\epsilon \in \mathbb{R}$?.

  En extensiones abelianas, los valores de u para los que esto sucede son todos enteros. Este resultado se conoce como el Teorema de Hasse-Arf y una prueba puede encontrarse en [Ser79, V.7.]. Para una extensión cualquiera esto no es cierto, llamamos a estos valores "saltos en la numeración superior".

- Observemos que estamos integrando un función que es constante a trozos, por lo que, realmente, el conductor es la suma de ciertas codimensiones, cada una modificada por un coeficiente que es la distancia entre un salto y el siguiente.

- Ante los dos puntos anteriores, uno podría sospechar que el conductor de una representación cualquiera no tiene por qué ser entero (pues lo definimos como una suma de números no necesariamente enteros). Sin embargo, en los casos que nos interesan (representaciones de Artin, p-ádicas o módulo p) siempre es un número natural. El caso de una representación de Artin puede encontrarse en [Ser79] y los casos de representaciones p-ádicas y módulo p en [Wie08, 3.1.] cuando $p \neq \mathrm{char}(K)$ y en [RS01, Lema 2.3.] cuando son iguales.

En el caso de K un cuerpo de números, recordemos primero que para cada primo $\wp$ en $\overline{K}$ sobre un p de K, el subgrupo de descomposición $D_\wp \cong \mathrm{Gal}(\overline{K_\wp}/K_\wp)$ por lo que dada una representación ρ de G_K, su restricción $\rho|_{D_\wp}$ se puede pensar como una representación de un cuerpo local.

Además, si elegimos otro primo $\wp'$ sobre p, los subgrupos de descomposición son conjugados por algún elemento $\sigma \in \mathrm{Gal}(\overline{K}/K)$ lo que implica que las restricciones $\rho|_{D_\wp}$ y $\rho|_{D_{\wp'}}$ son isomorfas vía la conjugación por $\rho(\sigma)$.

Definición 1.4.18. *Sea K un cuerpo de números y $\rho : G_K \to \mathrm{GL}_n(k)$ una representación de Galois que ramifica en finitos primos. Si k tiene característica q y p es un primo de K que no está arriba de q, definimos el exponente del conductor en p como:*

$$n_p(\rho) = n(\rho|_{D_\wp})$$

para algún primo $\wp$ de k sobre p. La parte coprima con q del conductor de la representación ρ será:

$$N(\rho) = \prod_{\substack{p \in K \\ p \nmid q}} p^{n_p(\rho)}.$$

Hagamos dos pequeñas observaciones sobre esta definición. Primero, el exponente $n_p(\rho)$ no depende del primo $\wp$ elegido, pues primos distintos dan representaciones isomorfas. Segundo, notemos que en los primos p en los que ρ es no ramificada, la restricción $\rho|_{D_\wp}$ tampoco lo es, por lo que $n_p(\rho) = 0$. Como ρ ramifica en finitos primos, la definición de $N(\rho)$ tiene sentido, pues el producto que consideramos es finito.

1.5. Una construcción: la reducción módulo p de una representación p-ádica

Una construcción importante en el mundo de las representaciones p-ádicas es la reducción módulo p. Esto consiste en asociar a toda representación p-ádica ρ, una representación $\overline{\rho}$ módulo p relacionada con ρ mediante una proyección.

Para realizar esta construcción debemos probar que dada una representación p-ádica, siempre existe una representación conjugada (es decir, podemos elegir una base apropiada del espacio V) que tiene imagen contenida en las matrices con coeficientes enteros.

Proposición 1.5.1. *Sea $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(L)$ una representación p-ádica (aquí L es la extensión finita de $\mathbb{Q}_p$ en la que la imagen toma valores). Sea V un L-espacio vectorial asociado a la representación, entonces existe un retículo estable T. Es decir un O_L-módulo $T \subset V$ cuyos elementos generan a V como L-espacio vectorial y tal que $\rho(\sigma)(T) \subset T$ para todo $\sigma \in G_\mathbb{Q}$.*

Demostración. Fijemos la base B de V que da lugar a la representación con imagen en $\mathrm{GL}_n(L)$. Sea M el O_F-módulo generado por B. Consideremos el siguiente subgrupo de $G_\mathbb{Q}$, $H = \{\sigma \in G_\mathbb{Q} : \rho(\sigma)(M) \subseteq M\}$.

Observemos que H es el conjunto de elementos σ de $G_\mathbb{Q}$ tales que la matriz $\rho(\sigma)$ tiene coeficientes en O_L, es decir, si $U = \{A \in \mathrm{GL}_n(L) :$ A tiene coeficientes en $O_L\}$ entonces $H = \rho^{-1}(U)$. Como O_L es un abierto de L, U es un abierto de $\mathrm{GL}_n(L)$ y H resulta un abierto de $G_\mathbb{Q}$.

Al ser H un subgrupo abierto de $G_\mathbb{Q}$, tiene índice finito. Sean entonces $g_1, \ldots, g_r$ representantes de las coclases de H en $G_\mathbb{Q}$. Afirmamos que T

el O_L-módulo generado por los elementos de $\{g_1L, \ldots, g_rL\}$ es un retículo estable.

Es evidente que es estable, lo que debemos probar es que tiene rango n. Pero esto es consecuencia de que L es el cuerpo de fracciones de O_L que es un dominio integro, así, un O_L-módulo libre tiene rango igual a la dimensión del espacio vectorial que se consigue al extender escalares a L. □

Notemos que ahora, haciendo un cambio de base a una base del retículo estable, obtenemos una representación conjugada ρ' con imagen en las matrices inversibles con coeficientes enteros. Llamemos $R \subset \mathrm{GL}_n(L)$ a este conjunto. Tenemos

$$G_{\mathbb{Q}} \xrightarrow{\rho'} R \xrightarrow{\pi} \mathrm{GL}_n(\mathbb{F}_L) \ ,$$

donde π consiste en aplicar la proyección coeficiente a coeficiente. Construimos así una representación asociada con coeficientes en un cuerpo finito. El inconveniente que tenemos es que fue a partir de una elección de un retículo estable, por lo que la reducción de ρ puede no estar bien definida. Lo que sí podemos afirmar es que su semisimplificación lo está. Esto es cierto pues el polinomio característico de la reducción de un elemento es la reducción de su polinomio característico, por lo que dadas dos reducciones semisimples, los polinomios característicos de sus imágenes coinciden y por el Teorema de Brauer-Nesbitt (1.3.9) son isomorfas. Decimos entonces que la reducción está bien definida a menos de semisimplificación.

Para terminar el capítulo, enunciemos la siguiente proposición que relaciona el conductor de una representación p-ádica ρ y su reducción. No daremos una prueba, pero se puede encontrar en [Wie08, 3.1.].

Proposición 1.5.2. *Sean K y F extensiones finitas de $\mathbb{Q}_p$ y $\mathbb{Q}_\ell$ respectivamente, donde p y ℓ son dos primos distintos. Sea $\rho : G_K \to \mathrm{GL}_n(F)$ una representación y $\overline{\rho}$ una reducción. Entonces $sw(\rho) = sw(\overline{\rho})$.*

Observación: Esto no nos dice que sus conductores coincidan, pero sí que difieren en un término calculable.

Capítulo 2

Formas Modulares

En este capítulo repasaremos la teoría básica de formas modulares. Las formas modulares son ciertas funciones holomorfas del semiplano complejo superior que tienen asociados dos invariantes: el peso y el nivel. Con el fin de hacer el trabajo más ameno, desarrollaremos primero la teoría en el caso de nivel 1. En un segundo acercamiento, introduciremos el concepto de nivel en general, haciendo hincapié en las diferencias y similitudes con el caso previamente estudiado.

Para introducir estos conceptos precisaremos algunas herramientas del análisis complejo. Un buen texto introductorio se puede encontrar en [Con78].

2.1. Formas modulares de nivel 1

En esta primera parte seguiremos el tratamiento dado en [Ser73], [Lan76] y [Kob93]. Cualquiera de los tres textos es útil como referencia introductoria.

2.1.1. El grupo modular

Para dar las condiciones que definen a las formas modulares debemos estudiar la acción de ciertos grupos de matrices en el semiplano complejo superior.

Dada una matriz de $M \in \mathrm{GL}_2(\mathbb{R})$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, definimos la acción de M en los elementos de $\mathbb{C} \cup \{\infty\}$ como

$$Mz = \frac{az + b}{cz + d}.$$

Un calculo sencillo prueba que dados $M \in \mathrm{GL}_2(\mathbb{R})$ y $z \in \mathbb{C}$,

$$\mathrm{Im}(Mz) = \det(M)\frac{\mathrm{Im}(z)}{|cz+d|^2},$$

con lo que deducimos que las matrices de $\mathrm{GL}_2(\mathbb{R})$ con determinante positivo actúan en el semiplano complejo superior $\mathfrak{h} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

La acción en la que estamos interesados es la de un grupo más pequeño: $\mathrm{SL}_2(\mathbb{R})$, y dentro de él, en la de las matrices con coeficientes enteros. Observemos que toda matriz $M \in \mathrm{SL}_2(\mathbb{Z})$ actúa igual que $-M$ en $\mathfrak{h}$, entonces la acción se factoriza por $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\pm Id$, grupo al que a partir de ahora notaremos G y llamamos el grupo modular completo.

Hablemos un poco de la estructura de G, ésta se encuentra íntimamente relacionada con su acción sobre $\mathfrak{h}$. Tenemos en el grupo modular dos elementos:

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

Afirmamos que S y T generan todo G. Esto se puede probar por un argumento inductivo pero se consigue una demostración más sencilla estudiando primero la acción en $\mathfrak{h}$. Lo que vamos a hacer es encontrar en $\mathfrak{h}$ un conjunto de representantes para las órbitas de esta acción.

Sea $D \subset \mathfrak{h}$ el subconjunto formado por los números complejos de parte real entre $-1/2$ y $1/2$ y módulo mayor o igual que 1 (ver Figura 2.1).

D no es exactamente un conjunto de representantes, pero está cerca. Precisamente:

Proposición 2.1.1. *Sean G, $\mathfrak{h}$ y D como antes, $P = e^{2\pi i/3}$ y $Q = -\overline{P}$ los puntos marcados en la Figura 2.1. Entonces vale:*

- *Para todo $z \in \mathfrak{h}$ existe un $g \in G$ tal que $gz \in D$.*
- *Si para dos puntos z y z' de D existe $g \in G$ tal que $gz = z'$ entonces $Re(z) = \pm 1$ y $z = z' \pm 1$ o bien $|z| = 1$ y $z' = -1/z$.*
- *Para todo $z \in D - \{i, P, Q\}$ el estabilizador de z en G es el subgrupo trivial. El estabilizador de i es el subgrupo generado por S, el de P el generado por ST y el de Q el generado por TS.*

Demostración. Para el primer punto, fijemos un $z \in D$. Recordemos que:

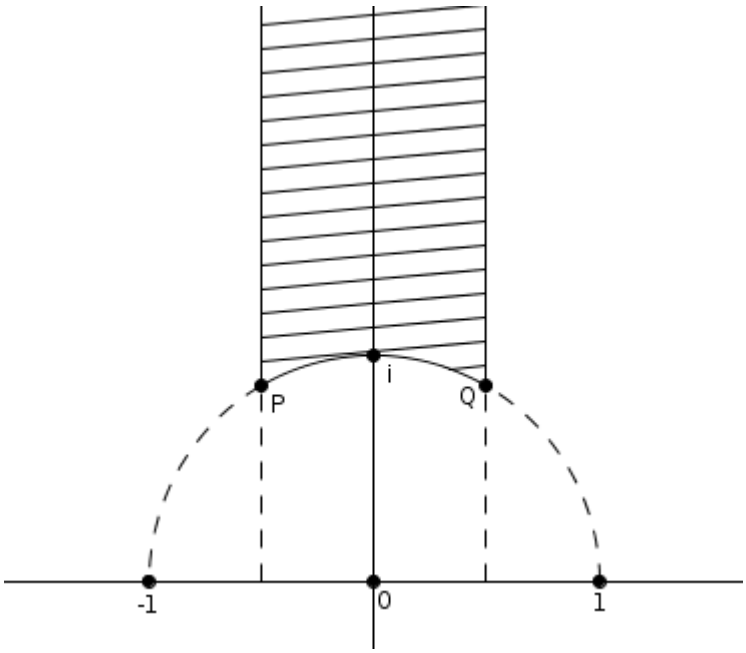


Figura 2.1: Un gráfico de D

$$\mathrm{Im}(gz) = \frac{\mathrm{Im}(z)}{|cz+d|^2}.$$

Observemos que al ser c y d enteros, $|cz+d|$ alcanza un mínimo (pues recorre algunos elementos de un retículo de $\mathbb{C}$) por lo que $\mathrm{Im}(gz)$ alcanza un máximo. Sea $\hat{g} \in G$ un elemento que maximiza $\mathrm{Im}(gz)$ y apliquemos T las veces que sea necesario para que la parte real de $T^n(\hat{g}z)$ esté entre $-1/2$ y $1/2$. Afirmamos que $T^n\hat{g}z \in D$. Para esto, alcanza con probar que $|T^n\hat{g}z| \geq 1$, pero si éste no fuera el caso, entonces $-(T^n\hat{g}z)^{-1} = ST^n\hat{g}z$ tendría parte imaginaria mayor que $\mathrm{Im}(T^n\hat{g}z) = \mathrm{Im}(\hat{g}z)$, lo que es absurdo.

Notemos que el mismo argumento funciona si tomamos a $\hat{g}$ como el elemento del subgrupo de G generado por S y T que maximiza la parte imaginaria de gz. Esto prueba algo más fuerte, que existe un elemento $g \in \langle S, T\rangle$ tal que $gz \in D$.

Para probar el resto de la proposición, sean $z \in D$ y $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$

tales que $gz \in D$. Podemos suponer sin perdida de generalidad que $\mathrm{Im}(gz) \geq \mathrm{Im}(z)$. Esto sucede si y solo si $|cz + d| \leq 1$. Observemos que como $z \in D$ y c y d son enteros, esto solo puede suceder si $c = -1, 0$ o 1, pues si $|c| \geq 2$ entonces $\mathrm{Im}(cz + d) = \mathrm{Im}(cz) > 1$ (pues $\mathrm{Im}(z) \geq \frac{\sqrt{3}}{2} > \frac{1}{2}$ para todo $z \in D$).

En el caso $c = 0$, resulta $d = 1$ o -1 con lo que g es una traslación por b o $-b$. Como z y gz están en D la únicas posibilidades son que g sea una traslación por 1 y $\mathrm{Re}(z) = -1/2$ o que g sea una traslación por -1 y $\mathrm{Re}(z) = 1/2$.

En el caso $c = 1$, debemos tener $|z+d| \leq 1$ con lo que $d = 0$ o $z \in \{P, Q\}$ y $d = \pm 1$.

En el primer caso, debe ser $|z| = 1$ y $b = -1$ de donde $gz = a - 1/z$. Pero como $|z| = 1$, $-1/z \in D$ y a debe ser 0 a menos que $1/z \in \{P, Q\}$ caso en el cual obtenemos las posibilidades $a = 1, -1$ y $z = P$ o Q.

Si $z = P$ o $z = Q$ tenemos $d = 0, 1$ o $d = 0, -1$ respectivamente. En el caso $z = P$, $d = 1$, debe valer $a - b = 1$ y $gP = a - 1/(1 + P) = a + P$, de donde $a = 0$ o 1. El caso $z = Q$ es análogo.

Finalmente, el caso $c = -1$ se puede transformar en $c = 1$ cambiando g por $-g$, que es otro representante de la misma clase.

Si estudiamos todos los casos que hemos detallado, comprobaremos que con esto quedan probados los items 2 y 3. □

Ahora estamos en condiciones de probar el resultado sobre la generación de G.

Proposición 2.1.2. *Si S y T son los elementos de G antes mencionados, vale que $G = \langle S, T \rangle$.*

Demostración. Haremos uso de la proposición anterior, específicamente del hecho de que dado un elemento cualquiera $w \in \mathfrak{h}$ existe un $g' \in \langle S, T \rangle$ tal que $g'w \in D$.

Tomemos un $g \in G$ y un elemento $z \in \mathfrak{h}$ que esté en el interior de D. Sabemos que existe un $g' \in \langle S, T \rangle$ tal que $g'gz \in D$. Pero entonces z y $g'gz$ son dos elementos del interior de D. De la proposición anterior se deduce primero que $z = g'gz$ pues z no está en el borde de D, por lo que no puede haber otro elemento de su órbita en D. Y luego que $g'g = Id$, pues está en el estabilizador de z, un elemento del interior de D. Concluimos que $g = g'^{-1} \in \langle S, T \rangle$ como queríamos. □

Más adelante nos interesará estudiar los subgrupos de $\mathrm{SL}_2(\mathbb{Z})$. Por el momento, la información que tenemos es suficiente para desarrollar la teoría de nivel 1.

2.1.2. Formas modulares

Como mencionamos en la sección anterior, las formas modulares son funciones holomorfas del semiplano complejo superior que cumplen con ciertas restricciones. Estas son dos: una ecuación funcional y una condición de crecimiento.

Fijemos un número entero k y sea $f : \mathfrak{h} \to \mathbb{C}$ una función meromorfa. La primer condición que f debe satisfacer para ser una forma modular de peso k y nivel 1 es que

$$\forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ f(z) = (cz+d)^{-k} f(gz). \tag{2.1}$$

Observemos que si k es impar, la única función que satisface esta condición es la constante 0, pues poniendo $g = -Id$ se debe tener que para todo $z \in \mathfrak{h}$

$$f(z) = (-1)^k f(gz) = -f(z),$$

implicando que $f(z) = 0$.

Ahora, podemos hacer actuar a $\mathrm{GL}_2^+(\mathbb{R})$, el grupo de matrices con coeficientes en $\mathbb{R}$ y determinante positivo, en el conjunto de funciones meromorfas $f : \mathfrak{h} \to \mathbb{C}$ como sigue, si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ definimos

$$f|_k[g] = (\det g)^{k/2}(cz+d)^{-k} f(gz).$$

Se puede chequear que esto efectivamente define una acción, es decir, dadas dos matrices g y $h \in \mathrm{GL}_2^+(\mathbb{R})$ vale que $f|_k[gh] = (f|_k[g])|_k[h]$. Con esta notación, lo que estamos pidiendo para que f satisfaga ser una forma modular de peso k es $f|_k[g] = f$ para todo $g \in \mathrm{SL}_2(\mathbb{Z})$.

Notemos que en virtud de la Proposición 2.1.2 y de la existencia de la acción que acabamos de definir, alcanzará con chequear que f satisface esta ecuación funcional para S y para T.

Resulta que f cumple la ecuación funcional para todo $g \in \mathrm{SL}_2(\mathbb{Z})$ si y solo si:

$$f(z) = z^{-k} f(-1/z) \quad \text{y} \quad f(z) = f(z+1).$$

Ahora, si tenemos una f que cumple la segunda de estas igualdades vale que $f(z) = f(z+1)$, lo que nos permite expresar a f como una función $\tilde{f}$ de $q = e^{2\pi iz}$. Esta nueva función está definida en el disco $\{|q| < 1\}$ con el origen removido y resulta meromorfa. Diremos que f es meromorfa (holomorfa) en infinito si $\tilde{f}$ se extiende a una función meromorfa (holomorfa) del disco completo $\{|q| < 1\}$.

Ya estamos en condiciones de dar las definiciones que nos interesan.

Definición 2.1.3. *Una función meromorfa $f : \mathfrak{h} \to \mathbb{C}$ es una función modular de peso k y nivel 1 si:*

- *f satisface (2.1).*
- *f es meromorfa en infinito.*

Cuando además f es holomorfa en todo $\mathfrak{h}$ y en infinito, decimos que es una forma modular.

Si f es una función modular, la función $\tilde{f}(q)$ admite un desarrollo como serie de Laurent alrededor de 0, es decir:

$$\tilde{f}(q) = \sum_{n \in \mathbb{Z}} a_n q^n,$$

para todo $q \neq 0$ en un entorno del origen. Llamamos a este desarrollo la q-expansión de f. Cuando f es holomorfa en infinito, los coeficientes negativos de esta expansión resultan iguales a 0.

Dada una forma modular f, definimos el valor de f en infinito como

$$f(\infty) = \tilde{f}(0) = a_0.$$

Si $f(\infty) = 0$, llamamos a f *forma cuspidal*.

Por último, observemos que dadas dos formas modulares de peso k, f_1 y f_2, la suma $f_1 + f_2$ es también una forma modular de peso k. Además, si ambas son cuspidales, la suma resulta cuspidal. También se obtiene una forma modular (resp. cuspidal) al multiplicar a f por un escalar de $\mathbb{C}$ por lo que el conjunto de formas modulares (resp. cuspidales) de peso k tiene estructura de $\mathbb{C}$-espacio vectorial. Llamamos M_k al espacio de formas modulares de peso k y S_k al de formas cuspidales.

Destaquemos también, que si g es una forma modular de peso k' entonces el producto fg es nuevamente una forma modular, pero de peso $k + k'$. Esto nos dice que $M = \bigoplus_{k=1}^{\infty} M_k$ tiene estructura de $\mathbb{C}$-álgebra graduada.

Otra interpretación

En esta sección daremos otra definición de forma modular, equivalente a la anterior. Estas pueden verse como funciones saliendo del conjunto de reticulados de $\mathbb{C}$. Especifiquemos primero lo que entendemos por esto.

Definición 2.1.4. *Sea V un $\mathbb{R}$-espacio vectorial de dimensión finita. Un reticulado de V es un subgrupo $\Gamma \subset V$ discreto que genera a V como $\mathbb{R}$-espacio vectorial. Esto es equivalente a que exista una base de $\mathbb{R}$ que genera a Γ como $\mathbb{Z}$-módulo.*

Llamemos ∇ al conjunto de retículos de $\mathbb{C}$. Para cada $\Gamma \in \nabla$, existe una base z_1, z_2 de Γ tal que $\mathrm{Im}(z_1/z_2) > 0$ (en este caso, llamaremos a z_1, z_2 base *orientada*). Observemos que dos pares de este tipo (z_1, z_2) y (z_1', z_2') generan el mismo retículo si y solo si existe una matriz M de $\mathrm{SL}_2(\mathbb{Z})$ tal que $M \cdot (z_1, z_2) = (z_1', z_2')$, donde esta acción es la usual de las matrices sobre los pares ordenados.

Por otro lado, tenemos definido

$$\phi : X = \{(z_1, z_2) \in \mathbb{C} \times \mathbb{C} : \mathrm{Im}(z_1/z_2) > 0\} \to \mathfrak{h},$$

por $\phi(z_1, z_2) = z_1/z_2$. Un simple cálculo muestra que ϕ respeta la acción de G definida en ambos conjuntos, por lo que hay una aplicación inducida

$$\tilde{\phi} : X/G \to \mathfrak{h}/G.$$

Esto nos da una función que va de ∇ a $\mathfrak{h}/G$. Observemos que dos retículos Γ y Γ' van a parar a un mismo elemento de $\mathfrak{h}/G$ si existen bases orientadas (z_1, z_2) y (z_1', z_2') de Γ y Γ' tales que $z_1/z_1' = z_2/z_2' = \lambda$, lo que es equivalente a decir que $\Gamma = \lambda\Gamma'$. Hemos probado:

Lema 2.1.5. *Existe una biyección*

$$\psi : \nabla/\mathbb{C}^\times \to \mathfrak{h}/G$$

que consiste en asignar a cada retículo Γ el elemento z_1/z_2, donde (z_1, z_2) es una base orientada de Γ.

Con esta biyección, podemos identificar a las formas modulares con ciertas funciones a valores complejos saliendo de ∇. Diremos que una

$$F : \nabla \to \mathbb{C}$$

es una función de peso k si para todo $\lambda \in \mathbb{C}^\times$ y $\Gamma \in \nabla$ vale que

$$F(\lambda\Gamma) = \lambda^{-k} F(\Gamma).$$

Ahora, una tal F define una función $\widehat{F}$ saliendo de X de modo que $\widehat{F}(z_1, z_2) = F(\Gamma)$ donde Γ es el retículo generado por z_1 y z_2. Observemos que esta función es invariante por la acción de G en X y cumple que para todo $\lambda \in \mathbb{C}^\times$:

$$\widehat{F}(\lambda z_1, \lambda z_2) = \lambda^{-k} \widehat{F}(z_1, z_2).$$

En particular, la función $z_2^k \widehat{F}(z_1, z_2)$ solo depende del valor de z_1/z_2, por lo tanto si definimos $f : \mathfrak{h} \to \mathbb{C}$ como $f(\omega) = \widehat{F}(\omega, 1)$ se tiene

$$\begin{gathered} z_2^k \widehat{F}(z_1, z_2) = f(z_1/z_2) \\ \Updownarrow \\ \widehat{F}(z_1, z_2) = z_2^{-k} f(z_1/z_2). \end{gathered}$$

Si ahora usamos que $\widehat{F}$ es invariante por la acción de G obtenemos que para todo $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$,

$$f(\omega) = \widehat{F}(\omega, 1) = \widehat{F}(a\omega + b, c\omega + d) = (c\omega + d)^{-k} f(g\omega),$$

es decir, f satisface la ecuación funcional que define a las formas modulares.

Es importante notar que esta construcción es reversible. Dada f una forma modular de peso k, podemos definir una función F en ∇ como $F(\Gamma) = z_2^{-k} f(z_1/z_2)$ con $\{z_1, z_2\}$ alguna base orientada de $\Gamma \in \nabla$. La ecuación funcional que satisface f garantiza que F está bien definida y es de peso k. Así, las formas modulares pueden identificarse con algunas funciones de retículos. Esto, como toda interpretación alternativa, simplifica algunas cuentas, presentamos un ejemplo en la próxima sección.

2.1.3. Ejemplos

Los primeros ejemplos de formas modulares son los dados por las series de Eisenstein. La idea de la construcción es usar que dado un retículo Γ, la serie

$$\sum_{\gamma \in \Gamma^*} 1/|\gamma|^k,$$

donde $\Gamma^* = \Gamma - \{0\}$ es convergente para todo $k > 2$. Esto se puede probar comparando la serie con la integral $\iint_{\mathbb{C}-B} 1/|w|^k dw$, donde B es una bola alrededor del origen que no contiene ningún elemento de Γ^*.

Ahora, si $2k$ es un entero par mayor a 2 definimos la función de retículos $\widehat{E}_{2k}$ como

$$\widehat{E}_{2k}(\Gamma) = \sum_{\gamma \in \Gamma^*} \frac{1}{\gamma^{2k}}.$$

Afirmamos que la función de $\mathfrak{h}$ en $\mathbb{C}$ asociada a $\widehat{E}_{2k}$ es una forma modular. Veamos primero cuál es esta función. Siguiendo la sección anterior definimos

$$E_{2k}(z) = \widehat{E}_{2k}(z, 1) = \sum_{m,n} \frac{1}{(mz+n)^{2k}},$$

donde m y n recorren todo $\mathbb{Z} \times \mathbb{Z} - \{(0,0)\}$.

Ya sabemos que E_{2k} cumple la ecuación funcional, resta ver que es holomorfa en $\mathfrak{h}$ y en ∞.

Para lo primero, veamos que sucede en D. Si $z \in D$, se tiene que

$$|mz+n|^2 = m^2|z|^2 + n^2 + 2\langle mz, n\rangle = m^2|z|^2 + n^2 + 2mn\mathrm{Re}(z),$$

que como $\mathrm{Re}(z) \geq -1/2$ y $|z| \geq 1$, esto es mayor que

$$m^2 - mn + n^2 = |mP - n|^2,$$

donde P es el punto de D definido en la Proposición 2.1.1.

Tenemos entonces que E_{2k} está definida en D por una serie de funciones holomorfas f_i acotadas por $E_{2k}(P)$. Esto nos dice que dicha serie converge normalmente (es decir, converge la serie de término $\sup_{z \in D} f_i(z)$) lo que implica convergencia uniforme sobre compactos y nos dice que E_{2k} es holomorfa en el interior D.

Para ver que existe un entorno de D en el que E_{2k} es holomorfa, observemos que podemos aplicar exactamente el mismo argumento en un dominio D' un poco más amplio. Por ejemplo en $D' = \{z \in \mathbb{C} : |z| \geq 3/4$ y $|\mathrm{Re}(z)| \geq 2/3\}$ la misma cuenta funciona, reemplazando P con el punto de D' con módulo igual a $3/4$ y parte real igual a $2/3$. Razonando de manera análoga obtenemos que E_{2k} es holomorfa en el interior de D' que es un entorno de D.

Finalmente, queremos probar que E_{2k} es holomorfa en todo $\mathfrak{h}$. Para eso, veamos que dado $g \in G$ vale que

$$E_{2k}(gz) = (cz + d)^{-2k} E_{2k}(z)$$

es una función holomorfa en un entorno de D. Esto nos dice que E_{2k} es holomorfa en un entorno de gD para todo $g \in G$, pero estos entornos cubren $\mathfrak{h}$ por lo que E_{2k} debe ser holomorfa allí.

Para completar la demostración solo resta chequear que nuestras series de Eisenstein son holomorfas en infinito. Es decir, debemos ver que E_{2k} vista como función de $q = e^{2\pi iz}$ puede continuarse de manera holomorfa en $q = 0$, lo que es equivalente a comprobar que existe el límite de $E_{2k}(z)$ cuando $\mathrm{Im}(z) \to \infty$. Además, como E_{2k} es invariante por traslaciones, podemos calcular este límite recorriendo los $z \in D$.

Ahora, recordemos que nuestra función está definida como una serie, cuya convergencia en D es uniforme, por lo que al calcular el límite podemos intercambiarlo con la sumatoria, precisamente se tiene

$$\lim_{\mathrm{Im}(z)\to\infty} E_{2k}(z) = \lim_{\mathrm{Im}(z)\to\infty} \sum_{m,n} \frac{1}{(mz+n)^{2k}} = \sum_{m,n} \lim_{\mathrm{Im}(z)\to\infty} \frac{1}{(mz+n)^{2k}}.$$

Para los términos con $m \neq 0$ el límite da 0. Con lo que nuestra suma se transforma en

$$\sum_{n\in\mathbb{Z}-\{0\}} \frac{1}{n^{2k}},$$

que es convergente, más aún es igual a $2\zeta(2k)$ donde ζ es la función zeta de Riemann.

Así hemos construido para cada entero $k > 1$ una forma modular de peso $2k$. Con esto podemos, por ejemplo, construir nuestra primera forma cuspidal. Teniendo en cuenta que

$$E_4(\infty) = 2\zeta(4) = \frac{1}{45}\pi^4 \quad \text{y} \quad E_6(\infty) = 2\zeta(6) = \frac{2}{945}\pi^6.$$

podemos llamar $g_4 = 60E_4$ y $g_6 = 140E_6$ y definir

$$\Delta = g_4^3 - 27g_6^2$$

y así obtenemos una forma cuspidal de peso 12. En general, las series de Eisenstein son un complemento para las formas cuspidales en M_k. Como veremos más adelante esto es cierto en un sentido más amplio. En este caso tenemos el siguiente lema.

Lema 2.1.6. *Dado un entero par $k > 2$ vale que*

$$M_k = S_k \oplus \mathbb{C}.E_k.$$

Demostración. Esto es consecuencia de que S_k es el núcleo de la aplicación lineal

$$\phi : M_k \to \mathbb{C}$$

definida como $\phi(f) = f(\infty)$. De esto se deduce que S_k es un subespacio de codimensión 1 en M_k. Por otro lado, se tiene que $E_k \in M_k - S_k$, pues $E_k(\infty) = 2\zeta(k) \neq 0$, por lo tanto

$$M_k = S_k \oplus \langle E_k \rangle$$

como queríamos. □

Como comentario final de la sección, destaquemos que los espacios M_k tienen todos dimensión finita sobre $\mathbb{C}$. Esto se puede demostrar, en este caso, calculando una integral a lo largo del borde de un dominio fundamental (como se hace en [Ser73]), pero esta idea no se traslada bien a situaciones de mayor generalidad.

La idea más útil consiste en dotar a $(\mathfrak{h}/G)^* := \mathfrak{h}/G \cup \{\infty\}$ de una estructura de variedad compleja y utilizar el hecho de que los espacios de funciones meromorfas sobre variedades compactas con polos y ceros prescriptos tienen dimensión finita. Esta prueba puede encontrarse en [Bum98, 1.3.].

Más aún, utilizando en este mismo marco un resultado más fuerte (el Teorema de Riemann-Roch) es posible calcular explícitamente las dimensiones de los M_k. Esto se encuentra desarrollado a lo largo del capítulo 3 de [DS05] y en [Shi71, 2.3.].

2.1.4. Los operadores de Hecke

Los operadores de Hecke son ciertos operadores que actúan en los espacios de formas modulares. En la clase de problemas que nos interesan, estas aplicaciones juegan un rol fundamental. Al estudiar las correspondencias entre el mundo de las formas modulares, el de las representaciones de Galois y el de los objetos geométricos como curvas elípticas o variedades abelianas, los objetos que aparecen naturalmente son autofunciones para estos operadores.

Haremos entonces una pequeña introducción a la teoría relativa al caso que estamos estudiando (formas modulares de nivel 1) con el objetivo final

de entender como funcionan en general.

Comenzaremos definiendo una función en los retículos de $\mathbb{C}$. Sea $\mathfrak{L}$ el grupo abeliano libre generado por ∇ el conjunto de retículos de $\mathbb{C}$, es decir las combinaciones lineales formales $\sum n_i\Gamma_i$ de elementos de ∇ con coeficientes enteros. Para definir un morfismo saliendo de $\mathfrak{L}$ alcanza con especificar su valor en los elementos de ∇ y extender linealmente. Definimos para cada $n \in \mathbb{Z}_{>0}$

$$T_n : \mathfrak{L} \to \mathfrak{L}$$

como

$$T_n(\Gamma) = \sum_{[\Gamma:\Gamma']=n} \Gamma',$$

es decir, la suma de los subretículos de índice n. Definimos otro operador, para cada $\lambda \in \mathbb{C}$, R_λ como

$$R_\lambda(\Gamma) = \lambda\Gamma.$$

Una observación valida es que los operadores T_n están bien definidos, pues un retículo tiene una cantidad finita de subretículos con un índice fijo. Esto se debe a que cualquier Γ' de índice n debe contener a $n\Gamma$ (pues sumar un elemento n veces en el cociente da 0), y su imagen en $\Gamma/n\Gamma$ es un subgrupo de n elementos que lo determina. Por lo tanto, hay tantos retículos de índice n en Γ como subgrupos de n elementos de $\Gamma/n\Gamma \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

Además, observemos que los operadores T_n y R_λ conmutan cualquiera sea el par n, λ. Esto es porque los subretículos de índice n de Γ están en correspondencia con los de $\lambda\Gamma$ vía la multiplicación por λ. También resulta evidente que los R_λ conmutan entre sí. Lo que no es tan sencillo es entender la interacción entre los propios T_n, para eso enunciamos la siguiente proposición.

Proposición 2.1.7. *Las aplicaciones T_n satisfacen*

- $T_m T_n = T_{mn} = T_n T_m$ *para todo par n, m coprimos.*
- $T_{p^n} T_p = T_{p^{n+1}} + pT_{p^{n-1}} R_p$ *para todo p primo.*

Demostración. Para la primera afirmación, basta con observar que para cada par de retículos Γ_1 de índice m y Γ_2 de índice n en Γ, existe un único retículo de índice mn contenido en ambos: su intersección, que tiene el índice correcto en virtud del teorema chino del resto (aquí estamos usando la hipótesis de coprimalidad al afirmar que al ser coprimos m y n, Γ_1 y Γ_2 generan todo Γ).

La segunda afirmación requiere un poco más de trabajo. Queremos probar una igualdad entre aplicaciones de retículos. Tenemos tres operadores involucrados, que dado un retículo Γ nos devuelven una combinación lineal de retículos de índice p^{n+1} en Γ. Bastará entonces con chequear, que para cada tal retículo Γ', el coeficiente con el que aparece en cada lado de la igualdad es el mismo. Notemos que en la expresión de $T_{p^{n+1}}$ todos aparecen con coeficiente 1. Además, $T_{p^{n-1}}R_p$ devuelve la suma de los retículos de índice p^{n-1} en $p\Gamma$, es decir la suma de los retículos de índice p^{n+1} en Γ que están contenidos en $p\Gamma$. Tenemos entonces dos casos:

a. $\Gamma' \subseteq p\Gamma$. En este caso, el lado derecho nos da $1 + p$. Para calcular el lado izquierdo, observemos que todos los retículos de índice p en Γ contienen a $p\Gamma$ y por lo tanto a Γ'. Por lo tanto estamos contando a Γ' una vez por cada retículo de índice p en Γ. Esta cantidad es igual a la cantidad de subgrupos de orden p en $(\mathbb{Z}/p\mathbb{Z})^2$ que es precisamente $p + 1$.

b. $\Gamma' \nsubseteq p\Gamma$. Aquí, el lado derecho da 1. Si el lado izquierdo da mayor que 1, entonces Γ' está contenido en al menos dos retículos de índice p en Γ y por lo tanto en su intersección. Pero esta intersección es justamente $p\Gamma$ (pues la intersección de dos subgrupos de orden p en $\Gamma/p\Gamma$ es $\{0\}$). Por lo tanto el lado izquierdo también da 1. □

Este resultado nos permite probar que los operadores T_n también conmutan entre sí. Observemos que de la segunda afirmación se deduce que para todo n, T_{p^n} es un polinomio en los T_{p^i} con $i < n$ y R_p, con lo que por un argumento inductivo, resulta un polinomio en T_p y R_p. Esto nos dice que los T_{p^i} conmutan entre sí y junto con el primer ítem implica que los T_n conmutan.

Otra observación referente a la proposición que acabamos de probar es que nos dice que el álgebra generada por los T_p y los R_λ contiene a todos los T_n.

La acción en los retículos que acabamos de definir puede trasladarse a las funciones a valores complejos que salen de ∇ de la siguiente manera, dada $F : \nabla \to \mathbb{C}$ definimos T_nF como $T_nF(\Gamma) = F(T_n\Gamma)$, considerando la extensión lineal de F a todo $\mathfrak{L}$. Así, podemos finalmente definir los operadores de Hecke T_n en los espacios M_k. Recordemos que toda forma modular f tiene asociada una función $F : \nabla \to \mathbb{C}$ que cumple $f(z) = F(\langle z, 1\rangle)$. Definimos entonces para todo n y toda forma modular f de peso k al operador de

Hecke T_n como

$$T_n(f)(z) = n^{k-1} T_n F(\langle z, 1\rangle),$$

es decir, como la función asociada a $n^{k-1}T_nF$ (aquí F es la función de retículos asociada a f).

Lema 2.1.8. *Los operadores T_n definidos en M_k satisfacen*

- $T_m T_n = T_{mn}$ *para todos m, n coprimos.*
- $T_{p^n} T_p = T_{p^{n+1}} + p^{k-1} T_{p^{n-1}}$

Demostración. Ambas se deducen de la Proposición 2.1.7, trasladando primero la relación que satisfacen a funciones de retículos y luego agregando el coeficiente n^{k-1}. □

Al definir los operadores de Hecke de esta forma, tenemos asegurado que $T_n(f)$ satisface la ecuación funcional. Para probar que efectivamente es una forma modular debemos estudiar como este operador afecta a la q-expansión de f. Para eso, comencemos por describir a $T_n f$ en función de f.

El hecho que utilizaremos para dar esta descripción es que dado un retículo Γ, cada matriz M de coeficientes enteros y determinante n define un retículo $\Gamma' \subset \Gamma$ de índice n: el generado por el par obtenido al aplicar M a una base orientada de Γ. Además, dos matrices tienen asociado el mismo retículo si y solo si difieren en la multiplicación por un elemento de $\mathrm{SL}_2(\mathbb{Z})$

Si llamamos $\mathcal{M}^n$ al conjunto de matrices de determinante n y tomamos representantes $\alpha_1, \ldots, \alpha_s$ de las órbitas de la acción de $\mathrm{SL}_2(\mathbb{Z})$ en $\mathcal{M}^n$ (por multiplicación a izquierda) tenemos el siguiente resultado:

Lema 2.1.9. *La acción de T_n en una forma modular f de peso k está dada por*

$$T_n f = n^{k-1} \sum_{i=1}^{s} f|_k[\alpha_i].$$

Demostración. El resultado es consecuencia de un simple cálculo, si

$$\alpha_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix},$$

entonces

$$T_n F(\langle z, 1\rangle) = \sum_{i=1}^{s} F(\langle \alpha_i(z, 1)\rangle) = \sum_{i=1}^{s} F(\langle a_i z + b_i, c_i z + d_i\rangle) =$$

$$= \sum_{i=1}^{s} (c_i z + d_i)^{-k} f\left(\frac{a_i z + b_i}{c_i z + d_i}\right) = \sum_{i=1}^{s} f|_k[\alpha_i].$$

Esto concluye la demostración, una aclaración útil es que en la anteúltima igualdad utilizamos el hecho de que F, la función de retículos asociada a f, cumple $F(\langle z_1, z_2\rangle) = z_2^{-k} f(z_1/z_2)$. □

Para terminar de darle forma a la fórmula de $T_n f$, encontremos un conjunto de representantes α_i adecuado.

Lema 2.1.10. *Las matrices de la forma*

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

con $a \geq 0$, $ad = n$ y $0 \leq b < d$ forman un conjunto de representantes de las órbitas de la acción de $\mathrm{SL}_2(\mathbb{Z})$ en $\mathcal{M}^n$.

Demostración. Comencemos con una matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de determinante n y probemos que existe $g \in \mathrm{SL}_2(\mathbb{Z})$ tal que gA es de la forma buscada. Tomando x e y coprimos tales que $ax + cy = 0$ y w, z tales que $zy - wx = 1$, multiplicar a A por $\begin{pmatrix} z & w \\ x & y \end{pmatrix}$ nos da una matriz en la órbita de A de la forma $\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$.

Finalmente, escribamos $b' = d'.q + r$ con $0 \leq r < d'$, entonces la multiplicación por $\begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}$ devuelve la matriz $\begin{pmatrix} a' & r \\ 0 & d' \end{pmatrix}$ que es de la forma buscada.

Resta ver que dos matrices de este tipo nunca están en la misma órbita. Supongamos que existe $g \in \mathrm{SL}_2(\mathbb{Z})$ y A en nuestro conjunto tales que

$$gA = \begin{pmatrix} x & y \\ w & z \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}.$$

Debe valer, primero que $aw = 0$, de donde $w = 0$ pues $a \neq 0$. Luego, $1 = \det g = xy$, lo que implica $x = z = \pm 1$. Pero además $d' = dz$ y tanto d como d' son positivos, por lo que $x = z = 1$.

Finalmente, $b' = b + yd$, pero tanto b como b' son números entre 0 y $d - 1$, por lo que deben ser iguales e $y = 0$. □

Combinando los dos lemas previos obtenemos la siguiente expresión para los operadores de Hecke:

$$T_n f = n^{k-1} \sum_{ad=n,\ 0\leq b<d} d^{-k} f\left(\frac{az+b}{d}\right).$$

Con esta descripción, es posible estudiar el efecto de los T_n en la q-expansión. Sea entonces f una función modular con q-expansión $f(z) = \sum_{m=-M}^{\infty} b_m q^m$, se tiene la siguiente

Proposición 2.1.11. *$T_n f$ es una función modular con q-expansión*

$$T_n f(z) = \sum_{m\in\mathbb{Z}} c_m q^m,$$

donde

$$c_m = \sum_{d|(m,n),\, d>0} d^{k-1} b_{mn/d^2}.$$

Demostración. Por nuestra última observación,

$$T_n f(z) = n^{k-1} \sum_{ad=n,\, 0\leq b<d} d^{-k} \left(\sum_{m\in\mathbb{Z}} b_m e^{2\pi i m(az+b)/d}\right).$$

Notemos que la suma

$$\sum_{0\leq b<d} e^{2\pi i m b/d}$$

de raíces de la unidad, da 0 cuando $d \nmid m$ y d en caso contrario. Utilizando esto y agrupando términos para cada a, d y m fijos obtenemos, si $m = m'd$, que

$$T_n f(z) = n^{k-1} \sum_{ad=n,\, m'\in\mathbb{Z}} d^{1-k} b_{dm'} q^{am'}.$$

Ahora, agrupamos las potencias de q e incorporamos el término n^{k-1} a la suma para obtener la q-expansión

$$T_n f(z) = \sum_{r\in\mathbb{Z}} q^r \sum_{a|(n,r),\, a\geq 1} (n/d)^{k-1} b_{rd/a},$$

que es igual a la q-expansión que buscamos. □

Observemos que si los b_m son cero para todo $m < 0$, entonces los c_m también, pues en la fórmula aparecen solo coeficientes con índice negativo. Si además $b_0 = 0$, resulta que

$$c_0 = \sum_{a|n} a^{k-1} b_0 = 0.$$

Deducimos entonces que los operadores T_n actúan en los espacios M_k y S_k. Ahora queremos entender sus autofunciones. Consideremos una forma modular f que sea autofunción de todos los T_n con autovalores λ_n. Se tiene el siguiente teorema.

Lema 2.1.12. *Si llamamos b_n a los coeficientes de la q-expansión de f, vale que:*

- $b_1 \neq 0$.
- $\forall n,\ b_n = \lambda_n b_1$.

Demostración. La fórmula para la q-expansión de $T_n f$ nos dice que el coeficiente que acompaña a q es

$$\sum_{a|(n,1)} a^{k-1} b_{n/a^2} = b_n.$$

Por otro lado, como f es autofunción de T_n de autovalor λ_n, este coeficiente es igual a $\lambda_n b_1$. Tenemos entonces que para todo n vale que

$$b_n = \lambda_n b_1.$$

Esto implica que $b_1 \neq 0$ pues, en caso contrario, tendríamos $b_n = 0$ para todo n con lo que debería ser $f = 0$. □

Corolario 2.1.13. *Los coeficientes b_n de la q-expansión de una forma modular f como en el Lema 2.1.12 y normalizada para que $b_1 = 1$ cumplen*

- $b_n b_m = b_{nm}$ *para todo par de m, n coprimos.*
- $b_p b_{p^n} = b_{p^{n+1}} + p^{k-1} b_{p^{k-1}}$ *para todo p primo.*

Demostración. Se deduce de las relaciones correspondientes para los T_n. □

Notemos que estos resultados nos dicen que dos formas modulares del mismo peso, que son autofunciones para todos los T_n y tienen los mismos autovalores, deben diferir en un escalar.

Algunos ejemplos de autofunciones de los operadores de Hecke son las series de Eisenstein E_4, E_6, E_8 y E_{10} y la forma cuspidal Δ. En todos los casos, el espacio al que pertenecen tiene dimensión 1 y es por eso que al aplicar cualquier operador T_n obtenemos un múltiplo escalar de la forma original.

Una consecuencia de esto es que los coeficientes de sus q-expansiones (que se pueden calcular, la cuenta puede encontrarse en [Ser73]) cumplen las relaciones del Corolario 2.1.13.

El producto de Petersson

Otra propiedad importante de los operadores de Hecke es que son diagonalizables tanto en S_k como en M_k. Más aún, un resultado de álgebra lineal nos dice que dada una familia de operadores lineales diagonalizables que conmutan entre sí, existe una base en la que todos son diagonales.

Para probar que los T_n son diagonalizables, se define el siguiente producto interno en S_k

$$\langle f, g\rangle = \int_D f(z)\overline{g(z)}y^{k-2}dxdy$$

donde $z = x + iy$ y D es un dominio fundamental para la acción de G en $\mathfrak{h}$. Este producto es conocido como el producto de Petersson. La integral que lo define es convergente siempre que f (o g) sea una forma cuspidal y se puede probar que la forma bilineal que queda definida es hermitiana ([Lan76, III-4]). Además, su definición no depende del dominio D elegido y es invariante por la acción de G.

Finalmente, es posible probar que los operadores T_n son autoadjuntos para el producto de Petersson [Lan76, III Teorema 4.2.], con lo que son diagonalizables en S_k. Para probar que también lo son en M_k es posible comprobar que las series E_k que definimos con anterioridad son ortogonales a todas las formas cuspidales ([DS05, 5.11.]). Por lo tanto, el espacio generado por E_k también es invariante, completando así una base de autofunciones de M_k.

2.2. El caso de nivel N

Para dar lugar a las formas modulares de nivel N lo que haremos es relajar el cumplimiento de la ecuación funcional a ciertos subgrupos de $\mathrm{SL}_2(\mathbb{Z})$. Al mismo tiempo, debemos modificar la condición en infinito de manera adecuada. Comenzamos estudiando la acción de los subgrupos que nos interesan en $\mathfrak{h}$.

2.2.1. Subgrupos de congruencia de $\mathrm{SL}_2(\mathbb{Z})$

Comencemos definiendo algunos subgrupos de $\mathrm{SL}_2(\mathbb{Z})$. Para cada $N \in \mathbb{N}$, definimos

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

y otros dos subgrupos,

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

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : \, a \equiv 1 \,(mod\, N) \right\}.$$

Observemos que para todo $N \in \mathbb{N}$, $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$. Llamamos "subgrupo de congruencia de nivel N" a cualquier subgrupo Θ de $\mathrm{SL}_2(\mathbb{Z})$ tal que $\Gamma(N) \subseteq \Theta$.

Con el trabajo que hicimos hasta ahora, resulta sencillo construir un dominio fundamental para cualquier subgrupo de congruencia Θ.

Lema 2.2.1. *Sea D un dominio fundamental para G. Dado un subgrupo de congruencia $\Theta \subset \mathrm{SL}_2(\mathbb{Z})$, y $\alpha_1, \ldots, \alpha_r \in \mathrm{SL}_2(\mathbb{Z})$ representantes de las coclases a izquierda de Θ en $\mathrm{SL}_2(\mathbb{Z})$, el conjunto*

$$D' = \bigcup_{1 \leq i \leq r} \alpha_i^{-1} D$$

es un dominio fundamental para Θ.

Notemos antes de demostrar el lema que el índice $[\mathrm{SL}_2(\mathbb{Z}) : \Theta]$ es finito, pues es menor que el de $\Gamma(N)$, que es finito pues existe un monomorfismo

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \hookrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

inducido por la proyección de $\mathbb{Z}$ a $\mathbb{Z}/N\mathbb{Z}$. Así, el enunciado tiene sentido.

Demostración. La demostración es sencilla. Dado $z \in \mathfrak{h}$, existe $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\alpha z \in D$. Además, $\alpha = \alpha_i \theta$ para algún $\theta \in \Theta$, con lo que $\alpha_i \theta z \in D$ implicando $\theta z \in \alpha_i^{-1} D \subset D'$.

Por otro lado, si dos elementos de D' están en la misma órbita por la acción de Θ tenemos, $z = \theta w$ con $\alpha_i z$, $\alpha_j w \in D$. Es decir, $\alpha_i \theta w$ y $\alpha_j w$ están en D, de donde $\alpha_i \theta = \alpha_j$, lo que implica $i = j$ y por lo tanto $\theta = Id$, como queríamos probar. □

Para las definiciones que siguen, será útil ampliar $\mathfrak{h}$ agregando los puntos racionales y un punto en ∞. Llamaremos a este conjunto $\tilde{\mathfrak{h}}$ y a los elementos de $\mathbb{Q} \cup \{\infty\}$ cúspides. La acción de G en $\mathfrak{h}$ puede extenderse a $\tilde{\mathfrak{h}}$ de la siguiente forma, si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ y $q \in \mathbb{Q}$, definimos

$$gq = \begin{cases} \infty & \text{si} \quad cq + d = 0; \\ \frac{aq+b}{cq+d} & \text{si} \quad cq + d \neq 0. \end{cases}$$

Además, $g\infty = a/c$ si $c \neq 0$ y $g\infty = \infty$ en caso contrario.

2.2.2. Formas modulares para subgrupos de congruencia

Como dijimos en un principio, daremos una definición más amplia de formas modulares relajando la ecuación funcional. Para ser más precisos.

Definición 2.2.2. *Dado un subgrupo de congruencia Θ de nivel N, decimos que una función meromorfa $f : \mathfrak{h} \to \mathbb{C}$ es una función modular de peso k para Θ si*

- $f|_k[\gamma] = f$ *para todo* $\gamma \in \Theta$.
- *Para todo* $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, $f|_k[\alpha]$ *tiene un desarrollo en serie de la forma*

$$f|_k[\alpha](z) = \sum_{n=-M}^{\infty} a_n e^{2\pi i n/N}.$$

Al igual que en el caso $N = 1$, decimos que f es una forma modular si el desarrollo en serie empieza en $n = 0$ para todo α y una forma cuspidal si además $a_0 = 0$.

Observemos que cualquier subgrupo de congruencia Θ de nivel N contiene al elemento $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$. Resulta entonces que una función f que satisface la ecuación funcional para Θ cumple que $f(z + N) = f(z)$ para todo z,

por lo que se puede escribir como una función de $q_N := e^{2\pi iz/N}$. Más aún, dada $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, $f|_k[\alpha]$ cumple la ecuación funcional para todas las matrices $\gamma \in \alpha^{-1}\Theta\alpha$, grupo que, al ser $\Gamma(N)$ normal, contiene a $\Gamma(N)$. Resulta entonces que $f|_k[\alpha]$ también es invariante por $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ y por lo tanto se puede escribir como función de q_N.

La segunda condición que impusimos a una función modular usualmente es conocida como "ser meromorfa en las cúspides". A pesar de que a simple vista estamos ante una cantidad infinita de condiciones (una por cada elemento de $\mathrm{SL}_2(\mathbb{Z})$), veremos a continuación que basta chequear que se cumplen finitas. Precisamente, que $f|_k[\alpha]$ sea meromorfa en infinito solo depende de la órbita de $\alpha\infty$ respecto de la acción de Θ.

Proposición 2.2.3. *Sean α y β en $\mathrm{SL}_2(\mathbb{Z})$ tales que que $\alpha\infty$ y $\beta\infty$ están en la misma órbita por la acción de Θ. Vale que la primera potencia de q_N que aparece con coeficiente no nulo en la expansión en infinito de $f|_k[\alpha]$ y $f|_k[\beta]$ es la misma. Más aún, si esa potencia es 0, los coeficientes coinciden si k es par y pueden diferir a lo sumo en el signo si k es impar.*

Demostración. Por nuestra hipótesis existe $\theta \in \Theta$ tal que $\theta\alpha\infty = \beta\infty$. Esto nos dice que $\beta^{-1}\theta\alpha$ deja fijo a ∞ y por lo tanto debe ser una traslación. Luego $\beta^{-1}\theta\alpha = \pm T^j$, con lo cual $\alpha = \pm\theta^{-1}\beta T^j$. Resulta entonces que

$$f|_k[\alpha] = f|_k[\pm Id][\theta^{-1}][\beta]_k[T^j] = (\pm 1)^k f|_k[\beta][T^j].$$

Ahora, si tenemos la q-expansión $f|_k[\beta](z) = \sum a_n q_N^n$ vale que

$$f|_k[\alpha](z) = (\pm 1)^k f|_k[\beta](z+j) = (\pm 1)^k \sum a_n e^{2\pi inj/N} q_N^n.$$

De aquí se deduce lo que queremos probar. □

Los primeros ejemplos de formas modulares con nivel mayor que 1 también provienen de series de Eisenstein. El espíritu de la construcción es el mismo pero hay que hacer pequeñas modificaciones.

Dado $a = (a_1, a_2)$ un par de elementos de $\mathbb{Z}/N\mathbb{Z}$ definimos la serie de Eisenstein de nivel N y peso $k > 2$ correspondiente a a como

$$E_k^a(z) = \sum_{\substack{m=(m_1,m_2) \\ m \equiv a \,(mod\, N)}} \frac{1}{(m_1 z + m_2)^k}.$$

Con argumentos similares a los de nivel 1 se puede probar que siempre $E_k^a \in M_k(\Gamma(N))$ y si $a = (0, a_2)$ entonces $E_k^a \in M_k(\Gamma_1(N))$. Esta cuenta puede encontrarse en [Kob93, III-21].

En cuanto a los espacios $M_k(\Theta)$ y $S_k(\Theta)$, resultan ser de dimensión finita para cualquier subgrupo de congruencia. Esto se prueba de la misma forma que en el caso de nivel 1. En este caso, se le puede dar estructura de variedad al conjunto $(\mathfrak{h}/\Theta)^*$ definido como el cociente de $\tilde{\mathfrak{h}}$ por la acción de G (recordemos que $\tilde{\mathfrak{h}}$ era el conjunto formado por $\mathfrak{h}$ y las cúspides). Otra vez vale que mediante el Teorema de Riemann-Roch, estas dimensiones pueden calcularse explícitamente. Las mismas referencias que para el caso de nivel 1 son útiles ([Shi71, 2.23.] y [DS05, capítulo 3]).

2.2.3. Particularidades de $\Gamma_0(N)$ y $\Gamma_1(N)$

Haremos una pequeña pausa para estudiar ciertas relaciones que hay entre formas modulares para Γ_0 y Γ_1. Básicamente, estos son los casos importantes para lo que deseamos estudiar.

Antes que nada, observemos que para todo N, $\Gamma_1(N)$ es el núcleo de la aplicación

$$\phi : \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$$

definida por

$$\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \overline{d}.$$

Este morfismo es claramente sobreyectivo, lo que nos permite deducir que $\Gamma_1(N)$ es un subgrupo normal de $\Gamma_0(N)$ y el cociente $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$.

Ahora, dada $f \in M_k(\Gamma_1(N))$ y $\alpha \in \Gamma_0(N)$, notemos que la función $f|_k[\alpha]$ es una forma modular para $\alpha^{-1}\Gamma_1(N)\alpha = \Gamma_1(N)$. Tenemos entonces para cada $\alpha \in \Gamma_0(N)$ un automorfismo de espacios vectoriales en $M_k(\Gamma_1(N))$ definido como $\phi_\alpha(f) = f|_k[\alpha]$. En otras palabras, podemos definir una representación ρ de $\Gamma_0(N)$ en $M_k(\Gamma_1(N))$. Observemos que esta representación ρ es trivial en $\Gamma_1(N)$, lo que nos da una representación de $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$.

Por otro lado, es un hecho conocido que cualquier representación de un grupo abeliano se descompone como suma de caracteres (representaciones de dimensión 1), en otras palabras, $M_k(\Gamma_1(N))$ es isomorfo como $\mathbb{Z}/N\mathbb{Z}$-módulo a una suma de espacios de dimensión 1, con lo cual la acción de $\Gamma_0(N)$ es diagonalizable.

Esto nos dice que hay una base $f_1, \ldots, f_r$ de $M_k(\Gamma_1(N))$ tal que para todo $\alpha \in \Gamma_0(N)$, $f_i|_k[\alpha] = \lambda_{\alpha,i} f_i$, donde el escalar $\lambda_{\alpha,i}$ solo depende de la clase de α módulo $\Gamma_1(N)$ y respeta la multiplicación, con lo que realmente tenemos para cada f_i un caracter ϵ_i de $\mathbb{Z}/N\mathbb{Z}$ tal que $f|_k[\alpha] = \epsilon_i(\overline{\alpha}) f_i$.

Poniendo estos hechos en otras palabras, podemos primero definir

$$M_k(N, \epsilon) = \{f \in M_k(\Gamma_1(N)) : \ f(\alpha) = \epsilon(d) f\}$$

para toda $\alpha \in \Gamma_0(N)$. Aquí d es la entrada inferior derecha de α y ϵ es un caracter de $\mathbb{Z}/N\mathbb{Z}$. De manera análoga definimos $S_k(N, \epsilon)$.

Con esta notación, lo que acabamos de probar no es otra cosa que

$$M_k(\Gamma_1(N)) \cong \bigoplus_{\epsilon} M_k(N, \epsilon),$$

donde ϵ recorre todos los caracteres de $\mathbb{Z}/N\mathbb{Z}$. Cuando $f \in M_k(N, \epsilon)$ llamamos a ϵ el caracter o *nebentypus* de f.

2.2.4. Operadores de Hecke en nivel N

Al igual que en el caso de nivel 1 los operadores de Hecke pueden definirse de diversas formas. En este caso, daremos una definición similar a la caracterización del Lema 2.1.9 y enunciaremos las propiedades que satisfacen.

Vale la pena mencionar que en este caso también existe una interpretación de las formas modulares como ciertas funciones de retículos. En este espíritu, los operadores de Hecke pueden definirse de forma similar al caso de nivel 1 y derivar varias propiedades de simples cálculos combinatorios. Este tratamiento es dado en [Kob93, III-5].

Definiremos los operadores de Hecke para algunos subgrupos de congruencia, que entre otros incluyen a $\Gamma_0(N)$ y $\Gamma_1(N)$ para todo N.

Sean S^+ un subgrupo de $\mathbb{Z}$ y $S^\times$ la preimagen en $\mathbb{Z}$ de un subgrupo de $\mathbb{Z}/N\mathbb{Z}$. Definimos el subgrupo

$$\Delta^n(N, S^+, S^\times) = \{\alpha \in M_{2\times 2}(\mathbb{Z}) : N|c,\ a \in S^\times,\ b \in S^+ \text{ y } \det(\alpha) = n\},$$

donde $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Observemos que por ejemplo, para $n = 1$, $S^+ = \mathbb{Z}$ y $S^\times = 1 + N\mathbb{Z}$ obtenemos $\Gamma_1(N)$ y para $n = 1$ y $S^+ = S^\times = \mathbb{Z}$ obtenemos $\Gamma_0(N)$. En general,

siempre que $n = 1$, el grupo que se tiene es un subgrupo de congruencia de nivel N.

Al igual que en el caso de nivel 1, se tiene una acción de $\Delta^1(N, S^+, S^\times)$ en $\Delta^n(N, S^+, S^\times)$ por multiplicación a izquierda. Si consideramos elementos $\alpha_1, \ldots, \alpha_s$ en $\Delta^n(N, S^+, S^\times)$ representantes de las órbitas de esta acción, definimos los operadores de Hecke para $\Delta^1(N, S^+, S^\times)$ como sigue.

Definición 2.2.4. *Dado $\Theta = \Delta^1(N, S^+, S^\times)$ un subgrupo de congruencia y $f \in M_k(\Theta)$ definimos*

$$T_n(f) = n^{k/2-1} \sum_{1 \leq i \leq s} f|_k[\alpha_i].$$

Observemos que con esta definición, nuestros operadores coinciden con los previamente definidos para el caso de nivel 1.

Enunciamos a continuación los resultados análogos a los probados para nivel 1, la demostración puede encontrarse en [Lan76, VII-2] o [Kob93, III-5].

Lema 2.2.5. *Los operadores T_n actúan en los espacios $M_k(\Theta)$, $S_k(\Theta)$. Más aún, en el caso de los grupos $\Gamma_0(N)$ y $\Gamma_1(N)$ la acción se restringe a los espacios $M_k(N, \epsilon)$ y $S_k(N, \epsilon)$.*

Lema 2.2.6. *Los operadores de Hecke actuando en $M_k(N, \epsilon)$ satisfacen:*

- *$T_{mn} = T_m T_n$ para todo m y n coprimos.*
- *$T_{p^n} = (T_p)^n$ para todo primo $p|N$.*
- *$T_{p^n} = T_{p^{n-1}} T_p - \epsilon(p) p^{k-1} T_{p^{n-2}}$ para todo primo $p \nmid N$.*

En particular, esto nos dice que el álgebra generada por los T_n está generada por los T_p y es conmutativa.

Lema 2.2.7. *Dada $f \in M_k(N, \epsilon)$ con q-expansión en una cúspide $f(z) = \sum_{n=0}^{\infty} a_n q^n$, los coeficientes b_n de la q-expansión de $T_m(f)$ están dados por*

$$b_n = \sum_{d|(m,n)} \epsilon(d) d^{k-1} a_{mn/d^2}.$$

Aquí, si d no es coprimo con N convenimos que $\epsilon(d) = 0$.

Nuevamente, este resultado tiene como consecuencia que si f es una autofunción de autovalor λ_m para T_m, entonces mirando el coeficiente b_1 de la q-expansión de $T_m(f)$ obtenemos

$$\lambda_m a_1 = b_1 = \sum_{d|(m,1)} \epsilon(d) d^{k-1} a_{m/d^2} = a_m.$$

La última pregunta que podemos hacernos, inspirados en el caso de nivel 1, es si los operadores que definimos son diagonalizables o no. En general, esto no es cierto, pero siempre podemos restringirnos a ciertos subespacios en los que los operadores pueden ser diagonalizados.

Comenzamos definiendo el producto de Petersson para este caso. Nuevamente, nos interesarán las formas modulares para $\Gamma_0(N)$ y $\Gamma_1(N)$ pero podemos dar una definición general. Sea $\Theta = \Delta^n(N, S^+, S^\times)$ un subgrupo de congruencia y f y g formas cuspidales de peso k para Θ. Definimos

$$\langle f, g\rangle = \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \Theta]} \int_D f(z)\overline{g(z)}y^{k-2}dxdy$$

donde $z = x + iy$ y D es un dominio fundamental para Θ.

Este producto está bien definido y define una forma hermitiana en S_k. Más aún, si dos funciones f y g son formas cuspidales para subgrupos distintos Θ y Θ', el valor de $\langle f, g\rangle$ no depende del subgrupo respecto del que se calcule la integral.

Ahora sí, volvemos nuestra atención a las formas modulares para $\Gamma_1(N)$. En este caso, no es cierto que todos los operadores de Hecke sean autoadjuntos para este producto interno. Pero se tiene el siguiente resultado similar.

Proposición 2.2.8. *Sea para cada $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ una matriz σ_d tal que $\sigma_d \equiv \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} (mod\, N)$.*

Para todo n coprimo con N, vale que dadas f y g en $S_k(\Gamma_1(N))$

$$\langle T_n f, g\rangle = \langle f|_k[\sigma_n], T_n g\rangle.$$

En particular, si $f \in S_k(N, \epsilon)$, resulta $\langle T_n f, g\rangle = \epsilon(n)\langle f, T_n g\rangle$.

Una demostración puede encontrarse en [Kob93, III-5 Prop 48]. Este resultado tiene como consecuencia

Corolario 2.2.9. *Sea n coprimo con N y tomemos c_n una raíz cuadrada de $\overline{\epsilon(n)}$. Entonces $c_n T_n$ es autoadjunto en $S_k(N, \epsilon)$.*

Demostración. Es un cálculo sencillo:

$$\langle c_n T_n f, g\rangle = c_n\epsilon(n)\langle f, T_n g\rangle = c_n\overline{c_n}^2\langle f, T_n g\rangle = \langle f, c_n T_n g\rangle$$

donde el último paso vale pues $c_n\overline{c_n} = |c_n|^2 = |\epsilon(n)| = 1$. □

Lo que nos dice este resultado es que los operadores T_n para n coprimo con N son diagonalizables en $S_k(\Gamma_1(N))$, más aún, como en el caso de nivel 1 existe una base de $S_k(\Gamma_1(N))$ compuesta por autofunciones de todos los T_n.

La principal diferencia con el caso inicial es que aquí no podemos diagonalizar a todos los operadores de Hecke. En un caso ideal en el que los autoespacios de los T_n para n coprimo con N tuvieran dimensión 1, valdría que todos los operadores son diagonalizables. Esto sería consecuencia de que al conmutar T_m y T_n para cualquier par de naturales m y n, los autoespacios para T_n son invariantes para T_m.

Afortunadamente, existe un subespacio de $S_k(\Gamma_1(N))$ en el que estos autoespacios tienen dimensión uno. Procedemos a dar las definiciones correspondientes.

Observemos que si $M \mid N$, cualquier forma modular para $\Gamma_1(M)$ es también una forma modular para $\Gamma_1(N)$. Más aún, si tenemos $f \in S_k(\Gamma_1(M))$ y $r|\frac{N}{M}$ entonces $g(z) = f(rz) \in S_k(\Gamma_1(N))$, pues $\Gamma_1(N) \subset \alpha^{-1}\Gamma_1(M)\alpha$, donde $\alpha = \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$.

Así, tenemos varios morfismos

$$S_k(\Gamma_1(M)) \rightrightarrows S_k(\Gamma_1(N)),$$

uno por cada $r|\frac{N}{M}$.

Llamamos subespacio viejo al subespacio generado por las imágenes de todas estas aplicaciones, cuando M recorre todos los divisores propios de N. Definimos el subespacio nuevo como el complemento ortogonal del subespacio viejo respecto del producto de Petersson. Llamamos *newforms* o formas nuevas a las autofunciones de los operadores de Hecke en el subespacio nuevo. Notamos a estos espacios $S_k^{\text{old}}(\Gamma_1(N))$ y $S_k^{\text{new}}(\Gamma_1(N))$.

Los operadores de Hecke preservan estos espacios y tenemos el siguiente resultado, conocido como Teorema de Multiplicidad uno. Un desarrollo más profundo de estas ideas puede encontrarse en [Lan76, VIII].

Teorema 2.2.10 (Multiplicidad uno)**.** *Valen los siguientes resultados.*

- *Sean $f, g \in S_k(\Gamma_1(N))$ autofunciones para todos los T_n con n y N coprimos tales que f y g tienen los mismos autovalores. Si f es una forma nueva entonces existe una constante c tal que $g = cf$.*

- *El espacio nuevo es la suma de los autoespacios de los T_n con $(n, N) = 1$ de dimensión uno. El espacio viejo es la suma de los autoespacios de dimensión mayor a 1.*

Este teorema tiene tres consecuencias importantes:

- En $S_k^{\text{new}}(\Gamma_1(N))$, una autofunción de los T_n con $(n, N) = 1$ queda determinada por sus autovalores.

- Si $f \in S_k^{\text{new}}(\Gamma_1(N))$ es autofunción de los operadores T_n con $(n, N) = 1$ entonces lo es para todos los T_n.

- Si f es una forma nueva, entonces $a_1 \neq 0$. En caso contrario tendríamos $a_m = \lambda_m a_1 = 0$ para todo m.

Para finalizar el capítulo, citamos un resultado de Shimura que habla de los autovalores de los operadores de Hecke.

Teorema 2.2.11 (Shimura)**.** *Dada $f \in S_k^{new}(\Gamma_1(N))$ una autofunción para los operadores de Hecke, sus autovalores son enteros algebraicos sobre $\mathbb{Q}$. Más aún, están todos contenidos en una extensión finita de $\mathbb{Q}$ a la que llamaremos $\mathbb{Q}_f$.*

Observemos que si f esta normalizada (es decir, si $a_1(f) = 1$) la extensión $\mathbb{Q}_f$ es la generada por los coeficientes de la q-expansión. Una prueba de este teorema puede encontrarse en [DS05, 6.5.].

Capítulo 3

La conjetura de Serre

3.1. Representaciones asociadas a formas modulares

Antes de poder enunciar la conjetura de Serre, debemos asociar a toda forma modular una representación de Galois. Este trabajo no es sencillo y fue realizado en primer lugar por Eichler-Shimura en peso 2 y luego por Deligne para los pesos $k > 1$ y por Deligne y Serre en peso 1.

La construcción utiliza herramientas de geometría algebraica que están fuera del alcance de este trabajo por lo que solo enunciaremos los resultados que fueron probados.

En el caso de peso 2, también es posible asociar a f un objeto geométrico (en ciertos casos curvas elípticas y en general variedades abelianas) y obtener a partir de éste la representación buscada.

Teorema 3.1.1 (Eichler-Shimura)**.** *Toda $f \in S_2^{new}(\Gamma_0(N))$ autofunción para los operadores de Hecke normalizada y tal que $\mathbb{Q}_f = \mathbb{Q}$ tiene asociada una curva elíptica E_f que satisface:*

- *E_f tiene mala reducción exactamente en los primos $p|N$.*
- *El coeficiente a_p de la q-expansión de f es igual a $p+1-\#E[\mathbb{F}_p]$ para todo $p \nmid N$.*

En general, a cualquier forma nueva f de peso 2 se le puede asociar un objeto geométrico similar a una curva elíptica con las propiedades garantizadas por el teorema. Estos objetos son las llamadas variedades abelianas. Se trata de variedades algebraica compactas definidas sobre $\mathbb{Q}$ provistas

de una estructura de grupo algebraico (es decir, variedades compactas no-singulares definidas sobre $\mathbb{Q}$ dotadas de una ley de grupo definida por funciones racionales). Vale que la variedad abeliana asociada a una forma nueva f de peso 2 tiene dimensión (como variedad algebraica) $[\mathbb{Q}_f : \mathbb{Q}]$.

La construcción de estos objetos (y de las representaciones asociadas a f que pueden conseguirse a partir de ellos) es realizada con detalle en el capítulo 9 de [DS05].

En el caso de peso $k > 2$, también es posible construir una representación asociada a f, aunque en este caso no proviene directamente de un objeto geométrico como los que introducimos. La construcción hecha por Deligne en [Del71] cumple con el siguiente teorema.

Teorema 3.1.2 (Deligne)**.** *Sean $f \in S_k(N, \epsilon)$ una forma nueva normalizada con $k > 1$ y $\lambda \in \mathbb{Q}_f$ un primo. Entonces existe una representación*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_{f,\lambda})$$

tal que:

- *$\rho_{f,\lambda}$ ramifica exactamente en los primos $p|N$ y $\ell = \lambda \cap \mathbb{Q}$.*
- *Para todo $p \nmid \ell N$, el polinomio característico de $\rho_{f,\lambda}(Frob_p)$ es*

$$x^2 - a_p x + \epsilon(p)p^{k-1}.$$

Aquí, $\mathbb{Q}_{f,\lambda}$ es la completación de $\mathbb{Q}_f$ respecto de λ.

Para poder interpretar los coeficientes del característico de $\rho_{f,\lambda}(Frob_p)$, hagamos la siguiente

Observación 3.1.3. *Sea $f \in S_k(N, \epsilon)$ una forma nueva normalizada y llamemos O_f al anillo de los coeficientes de la q-expansión de f en infinito, entonces $Im(\epsilon) \subset O_f$.*

Demostración. Según probamos en el Lema 2.2.7., el coeficiente b_p de la q-expansión de $T_p(f)$, donde f es una forma nueva de peso k y caracter ϵ, cumple

$$(a_p)^2 = \lambda_p a_p = b_p = a_{p^2} + p^{k-1}\epsilon(p),$$

implicando que $\epsilon(p) \in O_f$. Como los primos que no dividen a N recorren todo $(\mathbb{Z}/N\mathbb{Z})^\times$ esto nos dice que la imagen de ϵ está en O_f. □

Sabiendo esto, podemos pensar a ϵ como un caracter de $G_{\mathbb{Q}}$ de la siguiente forma

$$G_{\mathbb{Q}} \xrightarrow{\pi} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^{\times} \xrightarrow{\epsilon} \mathbb{Q}_f^{\times} ,$$

donde ζ_N es una raíz N-ésima primitiva de la unidad.

Al pensarlo así, el Teorema de Deligne nos dice que $\det(\rho_{f,\lambda})$ coincide con $\epsilon\chi_\ell^{k-1}$ en todos los $Frob_p$ para $p \nmid \ell N$. Recordemos que χ_ℓ es el caracter ciclotómico definido en $\mathbb{Q}_\ell$. Como estos elementos son densos en $G_{\mathbb{Q}}$, deducimos que

$$\det(\rho_{f,\lambda}) = \epsilon\chi_\ell^{k-1},$$

como caracteres de $G_{\mathbb{Q}}$.

A partir de esta igualdad podemos probar una propiedad característica de las representaciones asociadas a formas modulares, la llamada condición de paridad. Observemos primero que si ϵ es el caracter de una forma nueva no nula de peso k debe valer que $\epsilon(-1) = (-1)^k$ pues vale que

$$(-1)^k f(z) = f|_k[-Id] = \epsilon(-1)f(z),$$

con lo que $\epsilon(-1) \neq (-1)^k$ implica que $f = 0$.

Ahora, si evaluamos el determinante de ρ en el morfismo $c \in G_{\mathbb{Q}}$ dado por la conjugación compleja obtenemos:

$$\det(\rho_{f,\lambda}(c)) = \epsilon(c)\chi_\ell^{k-1}(c) = \epsilon(-1)(-1)^{k-1} = (-1)^{2k-1} = -1.$$

Aquí, usamos que para toda raíz de la unidad ζ vale que $c(\zeta) = \zeta^{-1}$ con lo que $\chi_\ell(c) = -1$.

Definición 3.1.4. *Diremos que una representación de Galois ρ es* impar *si* $\det(\rho(c)) = -1$.

Observemos además que mediante esta construcción, podemos asociar una representación módulo ℓ a f, que será la reducción de $\rho_{f,\lambda}$. Estas son las representaciones que entran en juego en la conjetura de Serre.

Finalmente, para peso $k = 1$ la situación es levemente distinta. En este caso las formas modulares tienen asociadas representaciones de Artin. En [DS74] se prueba el siguiente teorema.

Teorema 3.1.5 (Deligne-Serre)**.** *Si $f \in S_1(N, \epsilon)$ es una forma nueva normalizada entonces existe una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ tal que:*

- $\det(\rho) = \epsilon$. *En particular* ρ *es impar.*

- $N(\rho) = N$.

- $Tr(\rho(Frob_p)) = a_p$ *para todo* $p \nmid N$.

3.2. La conjetura de Serre

La conjetura de Serre es una suerte de resultado recíproco a todas estas construcciones. En su versión débil, asegura que cualquier representación de Galois módulo p, impar e irreducible proviene de una forma modular. En otras palabras, se tiene el siguiente enunciado.

Teorema 3.2.1 (Conjetura débil de Serre)**.** *Sea* $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ *una representación de Galois impar e irreducible. Entonces* ρ *es modular, es decir existe una forma nueva* $f \in S_k(\Gamma_1(N))$ *y un primo* $\lambda \in \mathbb{Q}_f$ *arriba de* p *tal que*

$$\overline{\rho}_{f,\lambda} \cong \rho,$$

donde $\overline{\rho}_{f,\lambda}$ *es la reducción módulo* λ *de* $\rho_{f,\lambda}$.

Enunciamos este resultado como teorema pues recientemente fue probado. Primero se demostró el caso de nivel 1, independientemente por Dieulefait en [Die07] y por Khare y Wintenberger en [KW09a] y unos años después fue probado el caso general por Khare y Wintenberger en [KW09b] y [KW09c] siguiendo las ideas de la prueba para nivel 1.

Una observación respecto del enunciado es que la forma f que da lugar a ρ no es única. Sucede que siempre existen infinitas formas cuyas representaciones son congruentes modulo p a ρ. En este sentido el resultado puede refinarse. En su versión fuerte, la conjetura no solo afirma que la representación proviene de una forma modular sino que además da una receta para calcular a partir de características de la representación el nivel $N(\rho)$, el peso $k(\rho)$ y el caracter $\epsilon(\rho)$ de una forma modular de la que ρ proviene (más aún, se trate de un peso y nivel *mínimos*), daremos estas recetas en las próximas secciones. El enunciado es el siguiente.

Teorema 3.2.2 (Conjetura fuerte de Serre)**.** *Sea* $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ *una representación de Galois impar e irreducible y* $p > 3$ *un primo. Entonces existe una forma nueva* $f \in S_{k(\rho)}(N(\rho), \epsilon(\rho))$ *y un primo* $\lambda \in \mathbb{Q}_f$ *arriba de* p *tal que*

$$\overline{\rho}_{f,\lambda} \cong \rho.$$

Más aún, si f' es otra forma modular tal que la representación módulo p asociada a f' es ρ entonces $N(\rho)|N(f')$, $k(f') \geq k(\rho)$ y $\epsilon(f') = \pi \circ \epsilon(\rho)$ donde $\pi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N(\rho)\mathbb{Z}$ es la proyección.

Es en esta versión que la conjetura resulta mucho más poderosa, pues permite catalogar las representaciones de Galois a partir de la clasificación de formas modulares en espacios de dimensión finita, uno por cada par peso-nivel. Sin embargo, y fundamentalmente gracias al trabajo de Ribet, las dos versiones de la conjeturas fueron probadas equivalentes, incluso antes de conocerse una prueba de la versión débil.

En los casos de $p = 2$ y 3 existen problemas en casos particulares. Estos son tratados en las Proposiciones 1.10. y 1.11. y el Teorema 1.12. de [Edi97].

Remarquemos que existe una conjetura análoga para el caso de representaciones con imagen en $\mathrm{GL}_2(\mathbb{C})$. Esta afirma que toda representación de Artin irreducible e impar proviene de alguna forma modular de peso 1 mediante la construcción de Deligne-Serre. En [Kha97] se prueba que este resultado se sigue como consecuencia de la conjetura de Serre, al probar que una representación de Artin impar da lugar a una familia estrictamente compatible de representaciones p-ádicas impares.

En lo que queda del trabajo, daremos la receta de Serre para $N(\rho)$, $k(\rho)$ y $\epsilon(\rho)$.

3.2.1. El nivel

Para dar esta definición, el trabajo que hay que hacer es el del final del capítulo 1. El nivel de Serre $N(\rho)$ es el conductor de Artin de ρ.

Una posible motivación para esta definición es un resultado de Carayol (se encuentra en [Car89]) que afirma que si $f \in S_k(N, \epsilon)$ es una forma nueva y $\lambda \in \mathbb{Q}_f$ un primo entonces el conductor de $\overline{\rho_{f,\lambda}}$ divide a N. Una forma de probar esto es demostrar primero que el conductor de la representación p-ádica $\rho_{f,\lambda}$ es exactamente N. Luego, la Proposición 1.5.2. nos dice que si llamamos $\tau = \rho_{f,\lambda}$ y $\overline{\tau} = \overline{\rho_{f,\lambda}}$ entonces

$$n_q(\overline{\tau}) = n_q(\tau) + \operatorname{codim} \overline{V}^{\overline{\tau}(G^0(\overline{\mathbb{Q}}/\mathbb{Q}))} - \operatorname{codim} V^{\tau(G^0(\overline{\mathbb{Q}}/\mathbb{Q}))},$$

donde $\overline{V}$ es el $G_{\mathbb{Q}}$-módulo asociado a $\overline{\tau}$.

Observemos ahora que $\dim \overline{V}^{\overline{\tau}(G^0(\overline{\mathbb{Q}}/\mathbb{Q}))} \geq \dim V^{\tau(G^0(\overline{\mathbb{Q}}/\mathbb{Q}))}$ pues

$$\pi\left(V^{\tau(G^0(\overline{\mathbb{Q}}/\mathbb{Q}))}\right) \subseteq \overline{V}^{\overline{\tau}(G^0(\overline{\mathbb{Q}}/\mathbb{Q}))},$$

donde π es el morfismo inducido por la proyección entre las representaciones. Esto nos dice que $n_q(\tau) \geq n_q(\overline{\tau})$ para todo $q \neq p$ por lo que $N(\overline{\tau})|N(\tau) = N$.

Lo que nos quiere decir esto es que si nuestra representación ρ proviene de una forma modular f, entonces f tiene nivel divisible por su conductor de Artin. Lo que asegura la conjetura es que siempre se puede encontrar una forma con nivel *igual* al conductor.

3.2.2. El caracter

La motivación para esta definición sale de la siguiente propiedad de las representaciones provenientes de formas modulares: si ρ_f proviene de una forma modular $f \in S_k(N, \epsilon)$ entonces $\det(\rho_f) = \epsilon\chi_p^{k-1}$ es un caracter de $(\mathbb{Z}/pN\mathbb{Z})^\times$.

Al partir de una representación ρ, podemos considerar

$$\det(\rho) : G_{\mathbb{Q}} \to \mathbb{F}^\times,$$

donde $\mathbb{F}$ es una extensión finita de $\mathbb{F}_p$. Notemos que este caracter tiene imagen abeliana, por lo que se factoriza por el grupo de Galois de una extensión abeliana (el cuerpo fijo por el núcleo). Como cualquier extensión abeliana está contenida en una extensión ciclotómica (este resultado se conoce como teorema de Kronecker-Webber) podemos factorizarlo por

$$\det(\rho) : \mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q}) \cong (\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{F}$$

donde ζ_M es una raíz M-ésima de la unidad.

Se puede probar (un posible argumento se encuentra en la página 213 de [Edi97]) que M siempre puede elegirse de forma tal que $M|pN(\rho)$ con lo que siempre podemos considerar que $\det(\rho)$ es un caracter de $\mathbb{Z}/pN(\rho)\mathbb{Z}$. Como $N(\rho)$ no es divisible por p, el teorema chino del resto nos asegura que $\det(\rho)$ es el producto de dos caracteres

$$\theta : \mathbb{Z}/p\mathbb{Z} \to \mathbb{F}^\times,$$

y

$$\omega : \mathbb{Z}/N(\rho)\mathbb{Z} \to \mathbb{F}^\times.$$

Lo que la conjetura de Serre afirma es que ρ proviene de una forma modular cuyo caracter $\epsilon(\rho)$ satisface que su reducción módulo p es ω.

Observemos que a partir de esta construcción también es posible decir algo sobre el peso. El caracter θ que aparece como factor de $\det(\rho)$ sale de

un grupo de orden $p-1$ lo que implica que los elementos de su imagen tienen orden divisible por $p-1$, es decir, θ tiene imagen en $\mathbb{F}_p^\times$.

A partir de esto podemos escribir a θ como una potencia $\overline{\chi_p}^d$ de la reducción del caracter ciclotómico χ_p. Según la construcción de Deligne, cuando la representación proviene de una forma modular esta potencia es $k-1$. Teniendo en cuenta esto, el peso $k(\rho)$ que definimos cumplirá que $k(\rho) \equiv d+1 \,(\mathrm{mod}\, p-1)$.

3.2.3. El peso

Finalmente, trataremos la construcción más delicada de las tres: el peso. La definición del peso depende de como ρ se comporta en el primo p. Recordemos que para cada primo $\wp|p$ tenemos definido el subgrupo de inercia $I_\wp$ y que estos son todos conjugados. Notaremos I_p a alguno de estos grupos y probaremos resultados que valen para este objeto definido salvo conjugación.

Probemos primero un lema sobre el comportamiento de la restricción de ρ a I_p.

Lema 3.2.3. *Llamemos $W_p \subset I_p$ al subgrupo de inercia salvaje definido en 1.4.1. Sea τ una representación de $G_\mathbb{Q}$ semisimple, entonces $W_p \subset \mathrm{Ker}(\tau)$.*

Demostración. Trabajaremos con la restricción de τ al grupo de descomposición D_p, como $I_p \subset D_p$ alcanza con analizar ese caso. De todos modos, seguiremos llamando τ a esta representación.

Notemos además que si dos representaciones ω_1 y ω_2 cumplen con el lema entonces su suma $\omega_1 \oplus \omega_2$ también lo hace. En virtud de esto, podemos suponer que τ es irreducible.

Sea V un $G_\mathbb{Q}$-módulo asociado a τ. V es un $\mathbb{F}$-espacio vectorial, donde $\mathbb{F}$ es la extensión finita de $\mathbb{F}_p$ en la que la imagen de τ tiene coeficientes. Consideremos entonces el subespacio V^{W_p} formado por los elementos de V que se quedan fijos por todos los morfismos de W_p.

Notemos primero que este espacio satisface que $\tau(g)(V^{W_p}) \subseteq V^{W_p}$ para todo $g \in D_p$ pues W_p es un subgrupo normal de D_p y por lo tanto si $v \in V^{W_p}$ y $g \in D_p$ se tiene que para todo $h \in W_p$ existe un $h' \in W_p$ tal que

$$\tau(hg)(v) = \tau(gh')(v) = \tau(g)(v),$$

implicando que $\tau(g)(v) \in V^{W_p}$.

Afirmamos que $V^{W_p} \neq \{0\}$. Para probar esto consideremos la acción de W_p en V dada por τ. Como W_p es límite de p grupos y V es finito, cada

órbita de esta acción tiene como cardinal una potencia de p, es decir, es 1 o múltiplo de p. Por otro lado, la órbita de 0 es puntual y como V tiene cardinal potencia de p tiene que existir otro elemento tal que el cardinal de su órbita no sea múltiplo de p. Un tal elemento debe tener órbita puntual y por lo tanto estar en V^{W_p}.

Para finalizar, notemos que hemos probado que V^{W_p} es un D_p-módulo no trivial incluido en V y al ser V irreducible debemos tener $V^{W_p} = V$ y por lo tanto $W_p \subset \mathrm{Ker}(\tau)$. □

A partir de ahora, llamaremos τ a la semisimplificación de $\rho|_{I_p}$. Si pensamos a τ saliendo del subgrupo de inercia I_{p_L} de $\mathrm{Gal}(L/\mathbb{Q})$ para una extensión finita L de $\mathbb{Q}$ (podemos tomar L como el cuerpo fijo por $\mathrm{Ker}(\tau)$) el lema anterior nos asegura que se factoriza por I_{p_L}/W_{p_L}, que por el Lema 1.4.6. es isomorfo a un subgrupo de $\mathbb{F}_{p_L}^{\times}$. Hemos probado que la imagen de τ es abeliana. Como además τ es semisimple, deducimos que es suma de dos caracteres, pues las representaciones irreducibles de grupos abelianos tienen todas dimensión 1. Llamemos $\tau = \alpha \oplus \beta$.

Los caracteres fundamentales

Como acabamos de probar, la representación τ puede pensarse saliendo del cociente I_p/W_p; llamemos I_t a ese cociente. Definiremos ciertos caracteres de I_t a los que llamaremos caracteres fundamentales.

Para eso, tomemos el cuerpo $\mathbb{Q}_p$. Como probamos en la Proposición 1.1.3. vale que $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \cong D_p$. Podemos considerar entonces $\mathbb{Q}_p^{\mathrm{unr}}$ el cuerpo fijo por I_p en $\overline{\mathbb{Q}_p}$ y $\mathbb{Q}_p^{\mathrm{tm}}$ el cuerpo fijo por W_p.

Observemos que $\mathbb{Q}_p^{\mathrm{unr}}$ es la máxima extensión no ramificada de $\mathbb{Q}_p$ y $\mathbb{Q}_p^{\mathrm{tm}}$ contiene a todas las extensiones con grupo de inercia salvaje trivial. De acuerdo a estas definiciones, resulta que $I_t \cong \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tm}}/\mathbb{Q}_p^{\mathrm{unr}})$.

Para definir los caracteres fundamentales necesitamos pasar por las extensiones $\mathbb{Q}_p^{\mathrm{unr}}(\sqrt[n]{p})/\mathbb{Q}_p^{\mathrm{unr}}$ donde n es coprimo con p. Dediquemos un párrafo a hablar de sus propiedades.

Recordemos primero que en $\mathbb{Q}_p^{\mathrm{unr}}$ se encuentran todas las raíces n-ésimas de la unidad, por lo que en $\mathbb{Q}_p^{\mathrm{unr}}(\sqrt[n]{p})$ tenemos a todas las raíces del polinomio minimal de $\sqrt[n]{p}$. Esto nos dice que estas extensiones son de Galois. Además, según la teoria de Kummer podemos identificar a su grupo de Galois con el

grupo de raíces n-ésimas de la unidad de $\mathbb{Q}_p^{\mathrm{unr}}$ mediante

$$\begin{aligned} \psi : \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}(\sqrt[n]{p})/\mathbb{Q}_p^{\mathrm{unr}}) &\to \mu_n(\mathbb{Q}_p^{\mathrm{unr}}) \\ \sigma &\mapsto \frac{\sigma(\sqrt[n]{p})}{\sqrt[n]{p}}, \end{aligned}$$

donde $\mu_n(K)$ es la notación para las raíces n-ésimas de la unidad de K. Finalmente, es posible chequear que el subgrupo de inercia salvaje de $\mathbb{Q}_p^{\mathrm{unr}}(\sqrt[n]{p})/\mathbb{Q}_p$ es trivial, razón por la cual $\mathbb{Q}_p^{\mathrm{unr}}(\sqrt[n]{p}) \subset \mathbb{Q}_p^{\mathrm{tm}}$.

Una vez dicho esto, la proyección entre los grupos de Galois nos da un morfismo

$$I_t \to \mathrm{Gal}\left(\mathbb{Q}_p^{\mathrm{unr}}(\sqrt[n]{p})/\mathbb{Q}_p^{\mathrm{unr}}\right) \cong \mu_n(\mathbb{Q}_p^{\mathrm{unr}}).$$

Poniendo $n = p^r - 1$ y utilizando el hecho de que $\mathbb{Q}_p^{\mathrm{unr}}$ tiene todas las raíces n-ésimas de la unidad, y por lo tanto $\mu_n(\mathbb{Q}_p^{\mathrm{unr}}) \cong \mu_n(\overline{\mathbb{F}_p})$ obtenemos un caracter

$$I_t \to \mu_{p^r-1}(\overline{\mathbb{F}_p}) = \mathbb{F}_{p^r}^{\times},$$

y componiendo con los r elementos de $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$ conseguimos los r caracteres fundamentales de nivel r. El único caracter fundamental de nivel 1 es el caracter ciclotómico y llamamos ψ y ψ' a los dos caracteres fundamentales de nivel 2. Estos satisfacen que $\psi^p = \psi'$ y $\psi\psi' = \chi_p$.

A continuación, probaremos que tanto α como β tienen imagen en $\mathbb{F}_{p^2}^{\times}$.

Lema 3.2.4. *Los caracteres α y β satisfacen una de las siguientes dos afirmaciones:*

(a) $\alpha^p = \alpha$ *y* $\beta^p = \beta$, *ó*

(b) $\alpha^p = \beta$ *y* $\beta^p = \alpha$.

En el primer caso ambos tienen imagen en $\mathbb{F}_p^{\times}$, en el segundo en $\mathbb{F}_{p^2}^{\times}$.

Demostración. Comencemos por considerar el grupo $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}/\mathbb{Q}_p)$. Este es canónicamente isomorfo al grupo de Galois de la extensión residual y por lo tanto está topológicamente generado por un elemento distinguido (el que corresponde al Frobenius vía el isomorfismo). Sea $g \in \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tm}}/\mathbb{Q}_p)$ una extensión de ese elemento a $\mathbb{Q}_p^{\mathrm{tm}}$.

Por otro lado, recordemos que $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}(\sqrt[n]{p})/\mathbb{Q}_p^{\mathrm{unr}}) \cong \mu_n(\mathbb{Q}_p^{\mathrm{unr}})$ mediante el morfismo que envía σ a $\sigma(\sqrt[n]{p})/\sqrt[n]{p}$ (que no depende de la elección de

$\sqrt[n]{p}$). Si consideramos entonces un elemento σ que corresponde a una raíz de la unidad h, tenemos

$$\frac{g\sigma g^{-1}(\sqrt[n]{p})}{\sqrt[n]{p}} = g\left(\frac{\sigma(g^{-1}(\sqrt[n]{p}))}{g^{-1}(\sqrt[n]{p})}\right) = g(h) = h^p,$$

pues la acción de Frobenius en las raíces de la unidad de $\mathbb{Q}_p^{\mathrm{unr}}$ es elevar a la p. Esto quiere decir que $g\sigma g^{-1} = \sigma^p$ para todo $\sigma \in \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}(\sqrt[n]{p})/\mathbb{Q}_p^{\mathrm{unr}})$, más aún, como $\mathbb{Q}_p^{\mathrm{tm}}$ es la unión de estas extensiones esto vale para todo $\sigma \in \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tm}}/\mathbb{Q}_p^{\mathrm{unr}})$. Aplicando ρ obtenemos que

$$\rho = \rho(g)^{-1}\rho^p\rho(g),$$

lo que quiere decir que ρ y ρ^p son conjugadas, en particular isomorfas. Deducimos de esto que τ y τ^p también son conjugadas a partir de lo que se obtiene el resultado. □

Diremos que estamos en el caso ordinario cuando los caracteres satisfacen (a) y en el caso supersingular cuando se cumple (b).

En el caso supersingular, los caracteres α y β tienen imagen en $\mathbb{F}_{p^2}^{\times}$, por lo que podemos escribir a α como una potencia de un caracter fundamental ψ de nivel 2. Sean $a < b$ ambos entre 0 y $p-1$ tales que $\alpha = \psi^{a+pb}$. Siempre se puede hacer esto pues si α no cumple que $a < b$ entonces β sí y podemos intercambiarlos. Además, si $a = b$ entonces α resulta ser una potencia de ψ^{p+1} que es de nivel 1, es decir, estamos en el caso ordinario.

Como $\beta = \alpha^p$ resulta que $\beta = \psi'^{a+pb} = \psi^{b+pa}$. Tenemos entonces que $\det(\tau) = \psi^{a+pb}\psi'^{a+pb} = \chi_p^{a+pb}$ lo que nos motiva a definir $k(\rho) = 1 + a + pb$.

En el caso ordinario hay que hacer ciertas distinciones que provienen de identificar en τ propiedades de representaciones provenientes de objetos geométricos con distintos tipos de reducción en p. Una motivación más adecuada puede encontrarse en [RS01] y [RS10].

Resulta en este caso, que si χ es el caracter ciclotómico módulo p entonces

$$\rho_{|I_p} \sim \begin{pmatrix} \chi^a & * \\ 0 & \chi^b \end{pmatrix}.$$

Para definir correctamente el peso hace falta hablar de una condición técnica que no introduciremos: que una representación sea finita en p. La definición se puede encontrar en [Edi97] o en [RS10, 21.7.2.]. La receta de Serre es:

- Si $* = 0$, reacomodamos a y b para que $0 \leq a \leq b \leq p-2$. Ponemos $k(\rho) = 1 + ap + b$.
- Si $* \neq 0$, tomemos $0 \leq a \leq p-2$ y $1 \leq b \leq p-1$. Sea $a' = \text{mín}\{a, b\}$ y $b' = \text{máx}\{a, b\}$. Si $\chi^{a-b} = \chi$ y $\rho \otimes \chi^{-a}$ no es finita en p entonces definimos $k(\rho) = 1 + pa' + b' + p - 1$. En caso contrario, tomamos $k(\rho) = 1 + pa' + b'$.

3.2.4. Una generalización a cuerpos totalmente reales

Para finalizar este trabajo, enunciaremos una generalización de la conjetura de Serre en la que remplazamos el cuerpo de base $\mathbb{Q}$ por un cuerpo F totalmente real.

Para esto, daremos un breve definición del objeto modular que debemos considerar: las formas modulares de Hilbert.

Definición 3.2.5. *Sea F un cuerpo totalmente real de grado m sobre $\mathbb{Q}$ y O_F su anillo de enteros. Consideremos los m morfismos $\sigma_1, \ldots, \sigma_m$ de F en $\mathbb{R}$. Tenemos entonces una acción de $\mathrm{GL}_2^+(O_F)$ sobre $\mathfrak{h}^m$ el producto de m semiplanos complejos superiores dada por*

$$\gamma(z_1, \ldots, z_m) = (\sigma_1(\gamma)z_1, \ldots, \sigma_m(\gamma)z_m).$$

Las formas modulares de Hilbert son en cierta forma el análogo de las formas modulares para varias variables sobre cuerpos totalmente reales. Para hacer más cómoda la notación definamos para una matriz $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$

$$j(\alpha, z) = \det \alpha^{-1/2}(cz + d).$$

Definición 3.2.6. *Una forma modular de Hilbert de peso $(k_1, \ldots, k_m)$ para F es una función analítica de $\mathfrak{h}^m$ tal que para todo $\gamma \in \mathrm{GL}_2^+(O_F)$ vale que*

$$f(\gamma z) = \prod_{i=1}^{m} j(\sigma_i(\gamma), z)^{k_i} f(z).$$

Al igual que en el caso de las formas modulares existe una versión con nivel y estos objetos vienen equipados con una acción de un álgebra de Hecke de operadores $T_{\mathfrak{m}}$ que conmutan entre sí y están indexados por los ideales no nulos de O_F.

Vale remarcar que a diferencia de la versión en dimensión 1, en este caso no es necesario pedir una condición en infinito pues esta se deduce de la ecuación funcional (el llamado Principio de Koecher).

Además, una construcción finalizada por Taylor (que se encuentra en [Tay89]) asocia a cada forma modular de Hilbert f una representación de Galois

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

que ramifica solo en p y en los primos de F que dividen al nivel de f. Nuevamente, podemos considerar la representación reducida con imagen en $\mathrm{GL}_2(\overline{\mathbb{F}_p})$. Estas representaciones resultan ser totalmente impares, es decir, $\det(\rho_f(c)) = -1$ para cualquier morfismo c proveniente de la conjugación compleja.

Es entonces natural conjeturar lo siguiente.

Conjetura 3.2.7. *Sea $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ una representación continua, irreducible y totalmente impar. Entonces ρ es isomorfa a $\overline{\rho_f}$ para alguna forma modular de Hilbert f.*

Poco se sabe de esta conjetura. En este caso también existe una versión fuerte y la mayor parte de los progresos hechos hasta ahora fueron en dirección a probar la equivalencia entre ambas. Detalles y referencias sobre estos avances pueden encontrarse en [BDJ10].

Bibliografía

[BDJ10] Kevin Buzzard, Fred Diamond, and Frazer Jarvis. On Serre's conjecture for mod ℓ Galois representations over totally real fields. *Duke Mathematical Journal*, 155(1):105–161, 2010.

[Bum98] Daniel Bump. *Automorphic Forms and Representations*. Cambridge University Press, 1998.

[Car89] Henri Carayol. Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires. *Duke Mathematical Journal*, 59(3):785–801, 1989.

[Con78] John B. Conway. *Functions of One Complex Variable*. Springer, 1978.

[Del71] Pierre Deligne. Formes modulaires et représentations l-adiques. *Seminaire Bourbaki*, (exposé 355), 1971.

[Die04] Luis Dieulefait. Existence of compatible families and new cases of the Fontaine-Mazur conjecture. *Journal fur die Reine und Angewandte Mathematik*, (577):147–151, 2004.

[Die07] Luis Dieulefait. The level 1 weight 2 case of Serre's conjecture. *Revista Matemática Iberoamericana*, 23(3):1115–1124, 2007.

[DS74] Pierre Deligne and Jean-Pierre Serre. Formes modulaires et poids 1. *Annales scientifiques de l'E.N.S.*, (4):507–530, 1974.

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Springer, 2005.

[Edi97] Bas Edixhoven. *Modular Forms and Fermat's Last Theorem*, chapter VII, pages 209–239. Springer, 1997.

[Kha97] Chandrashekar Khare. Remarks on mod p forms of weight one. *International Mathematics Research Notices*, (3):127–133, 1997.

[Kob93] Neal I. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Springer, 1993.

[KR01] Chandrashekar Khare and C.S. Rajan. The density of ramified primes in semisimple p-adic Galois representations. *International Mathematics Research Notices*, (12):601–607, 2001.

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger. On Serre's conjecture for 2-dimensional mod p representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Annals of Mathematics*, 169(1):229–253, 2009.

[KW09b] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture (i). *Inventiones Mathematicae*, 178(3):485–504, 2009.

[KW09c] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture (ii). *Inventiones Mathematicae*, 178(3):505–586, 2009.

[Lan76] Serge Lang. *Introduction to Modular Forms*. Springer, 1976.

[Lan02] Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer, 2002.

[Mar77] Daniel A. Marcus. *Number Fields*. Universitext. Springer, 1977.

[Mil08] James S. Milne. Fields and Galois theory (v4.21), 2008. Available at www.jmilne.org/math/.

[Neu99] Jürgen Neukirch. *Algebraic number theory*. Springer, 1999.

[Ram99] Ravi Ramakrishna. Lifting Galois representations. *Inventiones mathematicae*, (138):537–562, 1999.

[RS01] Kenneth A. Ribet and William A. Stein. Lectures on Serre's conjectures. In *Arithmetic algebraic geometry*, volume 9, pages 143–232. Park City, UT, 2001.

[RS10] Kenneth A. Ribet and William A. Stein. Lectures on modular forms and Hecke operators, 2010. Available at http://wstein.org.

[Ser73] Jean-Pierre Serre. *A Course in Arithmetic*. Springer, 1973.

[Ser79] Jean-Pierre Serre. *Local Fields*. Graduate Texts in Mathematics. Springer, 1979.

[Ser87] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Mathematical Journal*, 54(1):179–230, 1987.

[Ser89] Jean-Pierre Serre. *Abelian ℓ-adic representations and elliptic curves*. The advanced book program. Addison-Wesley publishing company, 1989.

[Shi71] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Forms*. Princeton University Press, 1971.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, second edition, 2009.

[Tay89] Richard Taylor. On Galois representations associated to Hilbert modular forms. *Inventiones Mathematicae*, 98(2):265–280, 1989.

[TS92] John Tate and Joseph H. Silveman. *Rational Points on Elliptic Curves*. Springer, 1992.

[Wei03] Steven H. Weintraub. *Representation Theory of Finite Groups: Algebra and Arithmetic*. Graduate Studies in Mathematics. American Mathematical Society, 2003.

[Wie08] Gabor Wiese. Galois representations, 2008. Available at http://www.uni-due.de/ hx0037/.