0.1 Representaciones de Galois

0.1.1 Definiciones Preliminares

En esta sección vamos a fijar la siguiente notación: ℓ y p siempre son números primos, $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ es el grupo de Galois absoluto de $\mathbb{Q}$ (muchos resultados de esta sección se pueden generalizar a cualquier grupo de Galois $G_{L|K} = \mathrm{Gal}(L \mid K)$) que, con la topología de Krull [**?**, capítulo IV, §1], es un grupo topológico compacto y Hausdorff, de hecho:

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

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

Definición 1. Sea A un anillo topológico. Una *representación de Galois* es un homomorfismo de grupos topológicos $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(A)$. Decimos que dos representaciones de Galois ρ y ρ' son isomorfas, denotado por $\rho \cong \rho'$, si existe una matriz $M \in \mathrm{GL}_n(A)$ tal que $\rho(\sigma) = M\rho'(\sigma)M^{-1}$ para toda $\sigma \in G_{\mathbb{Q}}$. Decimos que ρ es *impar* si $\det \rho(c) = -1$ donde $c \in G_{\mathbb{Q}}$ es la conjugación compleja.

Nota. Como $G_{\mathbb{Q}}$ es compacto, ρ satisface muchas de las mismas propiedades de las representaciones de grupos finitos como el lema de Schur [**?**, parte I, §4].

Nosotros vamos a estar interesados en tres casos de representaciones de Galois:

1. A es una extensión de campos finita sobre $\mathbb{Q}_\ell$. Recuerde que todo campo de esta forma se obtiene al completar un campo numérico $K|\mathbb{Q}$ con respecto de un valor absoluto $| * |_\lambda$ que está canónicamente asociado a un ideal primo $\lambda \subset \mathcal{O}_K$ sobre ℓ. Esta completación, denotada por K_λ, también se puede obtener como el campo de cocientes del límite inverso $\mathcal{O}_{K,\lambda} := \varprojlim_n \mathcal{O}_K/\lambda^n$, donde $\mathcal{O}_K$ es el anillo de enteros de K.

2. A es un *anillo de coeficientes.* Un anillo de coeficientes es un anillo local completo noetheriano con campo residual k finito. A es naturalmente un anillo topológico con la topología $\mathfrak{m}$-ádica donde $\mathfrak{m}$ es el ideal maximal de A. Una base para esta topología es la familia de abiertos $\{a + \mathfrak{m}^N \mid a \in A, N > 0\}$. Además, como A es completo, tenemos que $A \cong \varprojlim A/\mathfrak{m}^N$. De esta manera, la topología $\mathfrak{m}$-ádica de A induce una topología profinita en $\mathrm{GL}_n(A)$ dado por el isomorfismo $\mathrm{GL}_n(A) \cong \varprojlim \mathrm{GL}_n(A/\mathfrak{m}^N)$. En este caso, A casi siempre va a ser el anillo de enteros de una extensión finita de $\mathbb{Q}_\ell$.

3. A es una extensión finita de $\mathbb{F}_\ell$. En este caso, a A y a $\mathrm{GL}_n(A)$ les damos la topología discreta.

Una de las propiedades esenciales de las representaciones de Galois es la ramificación, pero para poder discutirla necesitamos estudiar $G_{\mathbb{Q}}$ con más cuidado; en particular estudiamos los grupos de Galois de extensiones finitas.

Para cualquier extensión finita de Galois $K \mid \mathbb{Q}$ con anillo de enteros $\mathcal{O}_K$, si $\mathfrak{P} \subset \mathcal{O}_K$ es un ideal primo sobre p (i.e. $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$) entonces el grupo de descomposición de $\mathfrak{P} \mid p$ se define como

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

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

$$\frac{D_{p,\mathfrak{P}}}{I_{p,\mathfrak{P}}} \cong \mathrm{Gal}(\mathcal{O}_K/\mathfrak{P} \mid \mathbb{F}_p). \tag{1}$$

El grupo de Galois $\mathrm{Gal}(\mathcal{O}_K/\mathfrak{P} \mid \mathbb{F}_p)$ es generado por el automorfismo de Frobenius definido por $x \mapsto x^p$. A cualquier preimagen $\sigma \in D_{p,\mathfrak{P}}$ de φ_p bajo $D_{p,\mathfrak{P}} \twoheadrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{P} \mid \mathbb{F}_p)$ se le llama un *elemento de Frobenius* sobre p. Entonces σ está bien definido módulo el grupo de inercia $I_{p,\mathfrak{P}}$.

En el caso de la extensión $\overline{\mathbb{Q}} \mid \mathbb{Q}$, si $\mathfrak{p} \subset \overline{\mathbb{Z}}$ es un ideal maximal de la cerradura entera de $\mathbb{Z}$ en $\overline{\mathbb{Q}}$, entonces definimos el grupo de descomposición de $\mathfrak{p}$ como:

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

Este grupo de descomposición es el límite inverso de los grupos de descomposición de las subextensiones finitas de Galois, es decir

$$D_{\mathfrak{p}} \cong \varprojlim_K D_{p,\mathfrak{p}\cap\mathcal{O}_K}$$

donde $K \subset \overline{\mathbb{Q}}$ corre sobre todas las subextensiones finitas de Galois y $\mathcal{O}_K$ es el anillo de enteros de K, además p es el número primo que cumple $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. En efecto, el isomorfismo está dado por $\sigma \mapsto \{\sigma|_K\}_K$ donde estamos identificando a $\varprojlim D_{p,\mathfrak{p}\cap\mathcal{O}_K}$ como subconjunto del producto $\prod_K \mathrm{Gal}(K \mid \mathbb{Q})$.

Ahora, como $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, entonces la inclusión $\mathbb{Z} \hookrightarrow \overline{\mathbb{Z}}$ induce la inclusión $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \overline{\mathbb{Z}}/\mathfrak{p}$. Por lo tanto $\overline{\mathbb{Z}}/\mathfrak{p}$ es una extensión (de campos) de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. De hecho es la cerradura algebráica de $\mathbb{F}_p$ porque cualquier elemento $\alpha + \mathfrak{p} \in \overline{\mathbb{Z}}/\mathfrak{p}$ satisface un polinomio mónico con coeficientes en $\mathbb{F}_p$ que es la reducción módulo p del polinomio mónico que satisface $\alpha \in \overline{\mathbb{Z}}$ y porque cualquier extensión algebraica propia de $\overline{\mathbb{Z}}/\mathfrak{p}$ induciría una extensión entera de $\overline{\mathbb{Z}}$ en $\overline{\mathbb{Q}}$ y esto no puede suceder porque $\overline{\mathbb{Z}}$ es la cerradura entera de $\mathbb{Z}$ en $\overline{\mathbb{Q}}$. Por lo tanto tenemos un isomorfismo $\overline{\mathbb{Z}}/\mathfrak{p} \cong \overline{\mathbb{F}}_p$ y gracias a esto identificamos $\overline{\mathbb{Z}}/\mathfrak{p}$ con $\overline{\mathbb{F}}_p$. Por lo tanto obtenemos un epimorfismo $\overline{\mathbb{Z}} \twoheadrightarrow \overline{\mathbb{F}}_p$ con nucleo $\mathfrak{p}$.

De esta manera, cualquier $\sigma \in D_{\mathfrak{p}}$ induce un homomorfismo $\tilde{\sigma}$ definido por el siguiente diagrama conmutativo:

$$\begin{tikzcd}
\overline{\mathbb{Z}} \arrow[r, "\sigma"] \arrow[d, two heads] & \overline{\mathbb{Z}} \arrow[d, two heads] \\
\overline{\mathbb{F}}_p \arrow[r, dashed, "\tilde{\sigma}"] & \overline{\mathbb{F}}_p
\end{tikzcd}$$

Más precisamente hay un homomorfismo $D_{\mathfrak{p}} \to G_{\mathbb{F}_p}$ definido por $\sigma \mapsto \tilde{\sigma}$ donde $\tilde{\sigma}(\alpha + \mathfrak{p}) = \sigma(\alpha) + \mathfrak{p}$.

El nucleo de $D_{\mathfrak{p}} \to G_{\mathbb{F}_p}$ se llama el grupo de inercia de $\mathfrak{p}$ y se denota por $I_{\mathfrak{p}}$. Análogamente al caso de $D_{\mathfrak{p}}$, el grupo de inercia de $\mathfrak{p}$ es el límite inverso de los grupos de inercia $I_{p,\mathfrak{p}\cap\mathcal{O}_K}$ donde K corre sobre todas las subextensiones finitas de Galois, i.e.

$$I_{\mathfrak{p}} \cong \varprojlim_K I_{p,\mathfrak{p}\cap\mathcal{O}_K}$$

donde $\mathcal{O}_K$ es el anillo de enteros de K.

Recuerde que $G_{\mathbb{F}_p} \cong \widehat{\mathbb{Z}}$, la completación profinita† de $\mathbb{Z}$ (c.f. [**?**, capítulo IV, §2, ejemplo 5]). Entonces el *automorfismo de Frobenius* $\varphi_p : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ definido por $\varphi_p(x) = x^p$ corresponde al

†Formalmente $\widehat{\mathbb{Z}}$ se define como el límite inverso $\widehat{\mathbb{Z}} = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})$ donde el sistema proyectivo se define con el orden de divisibilidad, más precisamente, cuando $n \mid m$ entonces usamos la proyección módulo n y así la familia de morfismos $\{\mathbb{Z}/m\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}\}_{n|m}$ forman un sistema proyectivo; su límite inverso es $\widehat{\mathbb{Z}}$

elemento $1 \in \widehat{\mathbb{Z}}$ y el subgrupo generado por φ_p corresponde al subgrupo denso $\mathbb{Z} \subset \widehat{\mathbb{Z}}$. A cualquier preimagen de φ_p en $D_{\mathfrak{p}}$ bajo el homomorfismo $D_{\mathfrak{p}} \to G_{\mathbb{F}_p}$ se le llama un *elemento de Frobenius absoluto sobre p.*

Con todo esto podemos definir la ramificación:

Definición 2. Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(A)$ una representación de Galois. Entonces ρ es *no-ramificado* en p si cumple $I_{\mathfrak{p}} \subseteq \ker \rho$ para algún (y por lo tanto todo, ver la siguiente nota) ideal maximal $\mathfrak{p} \subset \overline{\mathbb{Z}}$ sobre p. En general decimos que ρ es *no-ramificado casi donde sea* si ρ es no-ramificado para todo primo p salvo posiblemente un conjunto finito de números primos.

Nota. Si elegimos otro ideal primo $\mathfrak{p}'$ sobre p, entonces existe un $\sigma \in G_{\mathbb{Q}}$ tal que $\sigma(\mathfrak{p}) = \mathfrak{p}'$ (esto es porque $G_{\mathbb{Q}}$ actúa transitivamente sobre el conjunto de ideales primos sobre p). De esta manera $\sigma D_{\mathfrak{p}} \sigma^{-1} = D_{\sigma(\mathfrak{p})} = D_{\mathfrak{p}'}$ y en particular los grupos de inercia, $I_{\mathfrak{p}}$ y $I_{\mathfrak{p}}$, son conjugados. Por lo tanto, como $\ker \rho$ es un subgrupo normal, $I_{\mathfrak{p}} \subseteq \ker \rho$ si y solamente si $I_{\mathfrak{p}'} \subseteq \ker \rho$. Es decir la definición anterior no depende del ideal primo $\mathfrak{p}$ sobre p.

Nota. Si $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ es una representación compleja, entonces se factoriza a través de una representación $\rho' : \mathrm{Gal}(K_\rho \mid \mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ donde K_ρ es una extensión finita igual al campo fijo de $\ker \rho \subset G_{\mathbb{Q}}$. Entonces ρ es no-ramificado en p si y solamente si K_ρ es no ramificado en p[†]. buscar cita

Ejemplo 1. Sea $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ un caracter de Dirichlet primitivo. Sabemos que $\mathrm{Gal}(\mathbb{Q}(\mu_N)|\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^*$ y es la imagen de la proyección $\pi : G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_n) \mid \mathbb{Q})$ definida por la restricción $\sigma \mapsto \sigma|_{\mathbb{Q}(\mu_N)}$. Juntamos estos comentarios en el siguiente diagrama conmutativo:

Determinar cuando pasa esto, ademas del caso complejo.

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r, "\pi"] \arrow[rrr, dashed, bend right, "\rho_\chi"'] & \mathrm{Gal}(\mathbb{Q}(\mu_N) \mid \mathbb{Q}) \arrow[r, "\cong"] & (\mathbb{Z}/N\mathbb{Z})^* \arrow[r, "\chi"] & \mathbb{C}^* \end{tikzcd}$$

Por lo tanto obtenemos una representación ρ_χ asociado a χ. Afirmamos que ρ_χ es no-ramificado cuando $p \nmid N$. En efecto, $\ker \rho_\chi = \ker \pi$ y así su campo fijo es $\mathbb{Q}(\mu_N)$ donde la ramificación de primos es bien conocido: p es no-ramificado cuando $p \nmid N$.

Ahora estudiemos más a fondo qué sucede cuando ρ es no-ramificado en un primo p. En este caso elige un ideal primo $\mathfrak{p} \subset \overline{\mathbb{Z}}$ sobre p y un elemento de Frobenius absoluto $\sigma \in D_{\mathfrak{p}} \subset G_{\mathbb{Q}}$. Resulta que el valor $\rho(\sigma)$ es independiente de la elección de σ. En efecto, si σ' es otro elemento de Frobenius absoluto entonces $\sigma' = \sigma\tau$ para alguna $\tau \in I_{\mathfrak{p}}$ y así $\rho(\sigma') = \rho(\sigma\tau) = \rho(\sigma)$ ya que $I_{\mathfrak{p}} \subseteq \ker \rho$ por hipótesis.

Ahora, si elegimos otro ideal maximal $\mathfrak{p}'$ sobre p, entonces $\tau D_{\mathfrak{p}} \tau^{-1} = D_{\mathfrak{p}'}$ para alguna $\tau \in G_{\mathbb{Q}}$ y así cualquier elemento de Frobenius absoluto $\sigma' \in D_{\mathfrak{p}'}$ es de la forma $\tau\sigma\tau^{-1}$ donde $\sigma \in D_{\mathfrak{p}}$ es un elemento de Frobenius absoluto. Por lo tanto cambiar de ideal maximal sobre p conjuga al elemento de Frobenius absoluto. Esto quiere decir que el valor $\rho(\sigma)$ cambia por conjugación (por $\rho(\tau)$ en este caso). Por lo tanto la clase de conjugación $[\sigma] = \{\tau\sigma\tau^{-1} \mid \tau \in G_{\mathbb{Q}}\}$ de un elemento de Frobenius absoluto no depende de la elección de $\mathfrak{p}$, solamente de p. Este hecho nos sugiere la siguiente definición:

[†]i.e. la factorización del ideal $p\mathcal{O}_\rho$ del anillo de enteros de K_ρ es un producto lineal de ideales primos distintos, todos con índice de ramificación 1.

Definición 3. Sea $\sigma \in D_{\mathfrak{p}} \subset G_{\mathbb{Q}}$ un elemento de Frobenius absoluto para algún ideal maximal $\mathfrak{p} \subset \overline{\mathbb{Z}}$ sobre p. La clase de conjugación $[\sigma] \subset G_{\mathbb{Q}}$ se llama la *clase de conjugación de Frobenius* sobre p y se denota por Frob_p.

Recuerde que el polinomio característico de la matriz $\rho(\sigma)$ (para alguna $\sigma \in \mathrm{Frob}_p$) es invariante bajo conjugación. Por lo tanto el polinomio característico

$$\det(\rho(\mathrm{Frob}_p) - T\mathrm{Id}) := \det(\rho(\sigma) - T\mathrm{Id}) \quad \text{para alguna } \sigma \in \mathrm{Frob}_p$$

está bien definido y lo denotamos por $f_{\rho,p}$. Similarmente la traza $\mathrm{tr}\rho(\mathrm{Frob}_p)$ está bien definido.

Los primeros ejemplos de representaciones de Galois son los caracteres ciclotómicos y sus propiedades de ramificación son sencillas.

El grupo de Galois $G_{\mathbb{Q}}$ actúa sobre $\mu_N \subset \overline{\mathbb{Q}}$ de manera natural, entonces hay un homomorfismo de grupos $G_{\mathbb{Q}} \to \mathrm{Aut}(\mu_N)$. Recuerde que $\mathrm{Aut}(\mu_N) \cong (\mathbb{Z}/N\mathbb{Z})^*$, bajo el isomorfismo $f \mapsto n$ donde n es el entero que cumple $f(\zeta) = \zeta^n$ para alguna raiz primitiva de la unidad $\zeta \in \mu_N$ (observe que este isomorfismo no es canónico). Por lo tanto obtenemos una representación

$$\bar{\chi}_N : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_1(\mathbb{Z}/N\mathbb{Z}) = (\mathbb{Z}/N\mathbb{Z})^*,$$

que llamamos el *caracter ciclotómico módulo N*. Esta representación es caracterizada por las siguientes dos propiedades (cf. [**?**, §5.2 proposición 5.12 y §8.1 teorema 8.7]):

1. $\bar{\chi}_N$ es no-ramificada en todo primo $p \nmid N$.

2. $\bar{\chi}_N(\mathrm{Frob}_p) \equiv p \pmod N$.

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

$$\begin{tikzcd} & (\mathbb{Z}/\ell^{n+1}\mathbb{Z})^* \arrow[d, "\mathrm{mod}\ \ell^n"] \\ G_{\mathbb{Q}} \arrow[ur, "\bar{\chi}_{\ell^{n+1}}"] \arrow[r, "\bar{\chi}_{\ell^n}"'] & (\mathbb{Z}/\ell^n\mathbb{Z})^* \end{tikzcd}$$

Entonces podemos pasar al límite inverso. Sabemos que $\varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^* \cong \mathbb{Z}_\ell^*$, entonces si denotamos por χ_ℓ al morfismo inducido por la propiedad universal del límite inverso, obtenemos una representación

$$\chi_\ell : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_\ell^*.$$

La representación χ_ℓ se llama el *caracter ciclotómico ℓ-ádico*. Similarmente a $\bar{\chi}_N$, la representación χ_ℓ cumple:

Teorema 1. *El caracter ciclotómico χ_ℓ cumple, y es caracterizado por, las siguientes propiedades:*

1. *χ_ℓ es no-ramificada para todo primo $p \neq \ell$.*

2. *$\chi_\ell(\mathrm{Frob}_p) = p$ cuando $p \neq \ell$.*

0.1.2 Representaciones asociadas a curvas elípticas

Sea E una curva elíptica sobre $\mathbb{Q}$ y $E[N] \subset E(\overline{\mathbb{Q}})$ sus puntos de orden N. Observa que el grupo de Galois absoluto $G_{\mathbb{Q}}$ actúa sobre $E(\overline{\mathbb{Q}})$ y en particular actúa sobre $E[N]$. Esta acción está bien definida porque la acción de $G_{\mathbb{Q}}$ conmuta con la suma de E. En efecto, si P y Q son dos puntos de E, entonces las coordenadas de $P+Q$ son funciones racionales en las coordenadas de P y Q [**?**, §III.2, Group Law Algorithm]. Por lo tanto

$$O = O^\sigma = ([N]P)^\sigma = (P + \cdots + P)^\sigma = P^\sigma + \cdots + P^\sigma = [N]P^\sigma$$

y así $P^\sigma \in E[N]$ siempre que $P \in E[N]$. De esta manera cada σ induce un automorfismo de $E[N]$, es decir, tenemos una representación $G_{\mathbb{Q}} \to \mathrm{Aut}(E[N])$. Por otro lado, sabemos que $E[N] \cong (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ (c.f. la proposición **??** de la sección **??**), entonces $\mathrm{Aut}(E[N])$ es simplemente $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Así definimos:

Definición 4. La representación de Galois de los puntos de N-torsión de una curva elíptica $E/\mathbb{Q}$ se denota por

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

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

$$\begin{tikzcd}
 & \mathrm{GL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \arrow[r, dash, "\cong"] \arrow[d, "\bmod \ell^n"] & \mathrm{Aut}(E[\ell^{n+1}]) \arrow[d] \\
G_{\mathbb{Q}} \arrow[ur, "\bar{\rho}_{E,\ell^{n+1}}"] \arrow[r, "\bar{\rho}_{E,\ell^n}"'] & \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \arrow[r, dash, "\cong"] & \mathrm{Aut}(E[\ell^n])
\end{tikzcd}$$

Por lo tanto (como en el caso del caracter ciclotómico ℓ-ádico) existe naturalmente una representación de $G_{\mathbb{Q}}$ en $\varprojlim \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \cong \varprojlim \mathrm{Aut}(E[\ell^n]) = \mathrm{Aut}(T_\ell(E))$, es decir, tenemos:

Definición 5. Sea E una curva elíptica sobre $\mathbb{Q}$, entonces la *representación de Galois ℓ-ádica* asociada a E, es la representación

$$\bar{\rho}_{E,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \cong \mathrm{Aut}(T_\ell(E))$$

Esta representación cumple dos propiedades muy importantes:

Teorema 2. *Sea E una curva elíptica sobre $\mathbb{Q}$ con buena reducción en p, entonces*

1. *$\rho_{E,\ell}$ es no-ramificado en p para todo primo ℓ distinto de p.*
2. *El polinomio característico de $\rho_{E,\ell}$ es*

$$\det(\rho_{E,\ell}(\mathrm{Frob}_p) - T\mathrm{Id}) = p - a_p(E)T + T^2 \qquad (\forall \ell \neq p).$$

*donde $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$ (comparar con el teorema **??**)*

Proof. (c.f. [**?**, §3.3, proposición 3.15]) □

Del polinomio característico de $\rho_{E,\ell}(\mathrm{Frob}_p)$ podemos leer el determinante y la traza de $\rho_{E,\ell}(\mathrm{Frob}_p)$. En particular, el caracter $\det \rho_{E,\ell} : G_{\mathbb{Q}} \to \mathbb{Z}_\ell^*$ obtenido de la composición $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell) \xrightarrow{\det} \mathbb{Z}_\ell^*$, cumple que $\det \rho_{E,\ell}(\mathrm{Frob}_p) = p$ para toda p distinta de ℓ; cumple la mitad de las propiedades que caracterizan al caracter ciclotómico ℓ-ádico. Por otro lado, como toda curva elíptica sobre $\mathbb{Q}$ solamente tiene una cantidad finita de primos donde hay reducción mala, entonces $\rho_{E,\ell}$ es no-ramificado casi donde sea. Con estos dos hechos tenemos:

Corolario 3. *Sea E una curva elíptica sobre $\mathbb{Q}$ y $\rho_{E,\ell}$ su representación de Galois ℓ-ádica asociada. Entonces:*

$$\det \rho_{E,\ell} = \chi_\ell \quad y \quad \mathrm{tr}\rho_{E,\ell}(\mathrm{Frob}_p) = a_p(E) \qquad (\forall p \neq \ell).$$

0.1.3 La modularidad de representaciones de Galois

En esta sección estudiamos las representaciones de Galois que surgen de las formas modulares. Como en la sección **??**, denotamos por $S_2(\Gamma_0(N))$ al espacio de formas cuspidales de peso 2 y sea $f \in S_2(\Gamma_0(N))$ una forma primitiva (véase la definición **??**). Recuerde que el campo numérico de f, denotado por K_f, es la extensión finita de $\mathbb{Q}$ generada por los valores propios de f bajo los operadores de Hecke (c.f. la proposición **??**). Denotamos por $\mathcal{O}_f$ al anillo de enteros de K_f.

Gracias al trabajo de Eichler y Shimura, cada forma primitiva tiene asociado una representación de Galois:

Teorema 4. *(Eichler-Shimura) Sea $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ una forma primitiva y ℓ un número primo. Para todo ideal primo $\lambda \subset \mathcal{O}_f$ sobre ℓ escribimos $K_{f,\lambda}$ como la completación de K_f con respecto del valor absoluto asociado a λ. Bajo estas condiciones, existe una representación de Galois*

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

que satisface las siguientes propiedades:

1. *$\rho_{f,\lambda}$ es no-ramificado en p para todo primo $p \nmid N\ell$.*
2. *$\det \rho_{f,\lambda} = \chi_\ell$ el caracter ciclotómico $\ell-$ádico.*
3. *$\mathrm{tr}(\rho_{f,\lambda}(\mathrm{Frob}_p)) = a_p(f)$ para todo primo $p \nmid N\ell$.*

Nota. Para justificar la notación de la propiedad 2, primero observamos que $\det \rho_{f,\lambda}$ es la representación definida por la composición:

$$G_{\mathbb{Q}} \xrightarrow{\rho_{f,\lambda}} \mathrm{GL}_2(K_{f,\lambda}) \xrightarrow{\det} K_{f,\lambda}^*.$$

Pero $K_{f,\lambda}$ es una extensión finita de $\mathbb{Q}_\ell$, por lo tanto $\mathbb{Z}_\ell^* \subset K_{f,\lambda}^*$. Entonces identificamos el caracter ciclotómico $\ell-$ádico χ_ℓ con la composición

$$G_{\mathbb{Q}} \xrightarrow{\chi_\ell} \mathbb{Z}_\ell^* \hookrightarrow K_{f,\lambda}^*,$$

para poder hablar de la igualdad $\det \rho_{f,\lambda} = \chi_\ell$.

Proof. c.f. el teorema 9.5.4, §9.5 de [**?**] ó véase §7.6 de [**?**]. □

Este teorema tiene una generalización a pesos más grandes que 2 (c.f. el teorema 9.6.5 de [?]), pero para este trabajo solamente nos enfocaremos en peso 2 para definir modularidad.

Las representaciones de Galois asociadas a formas primitivas nos determinan una clase muy importante de representaciones. Para definirla, necesitamos separar en casos según qué anillo topológico A tomamos:

Definición 6. Sea ℓ un primo y sea $A = L$ una extensión finita de $\mathbb{Q}_\ell$. Sea $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(L)$ una representación de Galois no-ramificada casi donde sea. Decimos que ρ es *modular* si existe una forma primitiva $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ y un ideal primo $\lambda \subset \mathcal{O}_f$ sobre ℓ tales que $K_{f,\lambda} \hookrightarrow L$ y $\rho \cong \rho_{f,\lambda}$ (donde estamos identificando $\rho_{f,\lambda}$ con la composición $G_\mathbb{Q} \xrightarrow{\rho_{f,\lambda}} \mathrm{GL}_2(K_{f,\lambda}) \hookrightarrow \mathrm{GL}_2(L)$).

Proposición 1. *Sean ρ y $\rho_{f,\lambda}$ representaciones irreducibles e impares. Entonces si $a_p(f) = \mathrm{tr}(\rho(\mathrm{Frob}_p))$ y $\det(\rho(\mathrm{Frob}_p)) = p$ para casi todo primo p, entonces $\rho \cong \rho_{f,\lambda}$.*

Proof. Las dos igualdades, junto con los teoremas **??** y 3 nos dicen que los polinomios característicos $\det(\rho(\mathrm{Frob}_p) - T\,\mathrm{Id})$ y $\det(\rho_{f,\lambda}(\mathrm{Frob}_p) - T\mathrm{Id})$ son iguales para casi todo p. Como la traza y el determinante son funciones continuas y como $\{\mathrm{Frob}_p\}_p$ es denso en $G_\mathbb{Q}$, entonces los polinomios característicos $\det(\rho(\sigma) - T\,\mathrm{Id})$ y $\det(\rho_{f,\lambda}(\sigma) - T\mathrm{Id})$ son iguales para toda $\sigma \in G_\mathbb{Q}$. Si además asumimos que ρ y $\rho_{f,\lambda}$ son irreducibles e impares entonces podemos concluir que $\rho \cong \rho_{f,\lambda}$ (c.f. ejercicio 9.6.1 de [?]). $\square$ definir impar

Para definir modularidad para representaciones sobre extensiones finitas de $\mathbb{F}_\ell$, retomamos la representación de Galois $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(A)$, donde A es una extensión finita de $\mathbb{Q}_\ell$. Bajo estas condiciones, ρ se factoriza a través de la inclusión $\mathrm{GL}_n(\mathcal{O}_A) \hookrightarrow \mathrm{GL}_n(A)$ donde $\mathcal{O}_A$ es el anillo de enteros de A. Más precisamente, existe una representación de Galois $\rho' : G_\mathbb{Q} \to \mathrm{GL}_n(\mathcal{O}_A)$ tal que ρ es isomorfa a la composición

$$G_\mathbb{Q} \xrightarrow{\rho'} \mathrm{GL}_n(\mathcal{O}_A) \hookrightarrow \mathrm{GL}_n(A).$$

Este hecho se sigue de que $\mathcal{O}_A^n$ es una retícula de A^n (c.f. la proposición 9.3.5 de [?]).

Por lo tanto, en el caso $A = K_{f,\lambda}$ para alguna forma primitiva $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ y un ideal primo $\lambda \subset \mathcal{O}_f$ sobre ℓ, cada representación de Galois $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(K_{f,\lambda})$ tiene asociada una representación $\rho' : G_\mathbb{Q} \to \mathrm{GL}_n(\mathcal{O}_{f,\lambda})$ donde $\mathcal{O}_{f,\lambda}$ es el anillo de enteros de $K_{f,\lambda}$. Definimos la representación $\bar\rho_{f,\lambda} : G_\mathbb{Q} \to \mathrm{GL}_n(\mathcal{O}_{f,\lambda}/\mathfrak{m}_{f,\lambda})$ obtenida por la composición de ρ' con la proyección módulo $\mathfrak{m}_{f,\lambda} = \lambda\mathcal{O}_{f,\lambda}$. Resumimos estos dos párrafos con el siguiente diagrama conmutativo:

$$\begin{tikzcd} & \mathrm{GL}_n(K_{f,\lambda}) & \\ G_\mathbb{Q} \arrow[ur, "\rho_{f,\lambda}"] \arrow[r, "\rho'"] \arrow[rr, dashed, bend right, "\exists\,\bar\rho_{f,\lambda}"'] & \mathrm{GL}_n(\mathcal{O}_{f,\lambda}) \arrow[u, hook] \arrow[r, two heads, "\bmod \mathfrak{m}_{f,\lambda}"] & \mathrm{GL}_n(\mathcal{O}_{f,\lambda}/\mathfrak{m}_{f,\lambda}). \end{tikzcd} \tag{2}$$

Recuerde que $\mathcal{O}_{f,\lambda}/\mathfrak{m}_{f,\lambda}$ es una extensión finita de $\mathbb{F}_\ell$. Por lo tanto la asignación $\rho_{f,\lambda} \mapsto \bar\rho_{f,\lambda}$ asocia a cada representación $\rho_{f,\lambda} : G_\mathbb{Q} \to \mathrm{GL}_2(K_{f,\lambda})$ una representación $\bar\rho_{f,\lambda} : G_\mathbb{Q} \to \mathrm{GL}_2(F)$ donde F es una extensión finita de $\mathbb{F}_\ell$.

Ahora definimos la modularidad de representaciones de Galois sobre $\bar{\mathbb{F}}_\ell$.

Definición 7. Una representación de Galois $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$ es *modular* si existe una forma primitiva $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ y un ideal primo $\lambda \subset \mathcal{O}_f$ sobre ℓ tales que $\rho \cong \bar{\rho}_{f,\lambda}$.

Nota. Si F es una extensión finita de $\mathbb{F}_\ell$, entonces $F \subset \bar{\mathbb{F}}_\ell$. Así podemos extender la definición anterior a la representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$ simplemente considerando la composición $G_{\mathbb{Q}} \xrightarrow{\rho} \mathrm{GL}_2(F) \hookrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$. Conversamente, si tenemos una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$, la imagen de ρ es finito por ser un subconjunto compacto del espacio discreto $\bar{\mathbb{F}}_\ell$ (ya que $G_{\mathbb{Q}}$ es compacto y ρ es continua). Por lo tanto la imagen de ρ está contenido en $\mathrm{GL}_2(F)$ para alguna extensión finita F de $\mathbb{F}_\ell$, es decir, ρ se factoriza a través de la inclusión $\mathrm{GL}_2(F) \hookrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$. En conclusión, una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$ induce una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$ donde $[F : \mathbb{F}_\ell] < \infty$ y vice versa. Por lo tanto la definición anterior realmente es una definición de modularidad de representaciones sobre extensiones finitas de $\mathbb{F}_\ell$.

La modularidad de una curva elíptica está codificada en la modularidad de las representaciones ℓ-ádicas asociadas a la curva:

Teorema 5. *Sea $E/\mathbb{Q}$ una curva elíptica. Entonces las siguientes afirmaciones son equivalentes:*

1. *E es modular.*
2. *$\rho_{E,\ell}$ es modular para todo primo ℓ.*
3. *Existe un primo ℓ tal que $\rho_{E,\ell}$ es modular.*

Proof. c.f. [**?**, §3.4, proposición 3.23] □

Este teorema es un paso fundamental en la prueba de STW semiestable (véase la segunda figura de la introducción).