AGRA II: Aritmética, grupos y análisis
An ICTP-CIMPA Research School

Curvas de Shimura

Michael Harris

Columbia University

harris@math.columbia.edu

UNIVERSIDAD S. ANTONIO ABAD, CUSCO, PERÚ, del 8 al 22 de agosto de 2015

Índice

1. Grupos cuaterniónicos como grupos Fuchsianos

1.1. Grupos discretos de cuaterniones y plano superior de Poincaré. Sea D un álgebra de cuaterniones sobre un cuerpo totalmente real F. Sea Σ el conjunto de primos arquimedianos de F. Sea G el grupo multiplicativo de D. Para cada primo v de F (arquimediano o no) tenemos la completación D_v sobre el cuerpo topológico F_v, y ponemos $G_v = D_v^\times$. El álgebra de adèles de D es el producto restringido $D(\mathbf{A}) = \prod_v' D_v$ sobre todos los primos de F, definido exactamente como en el caso de un cuerpo de números. Es decir, en cada primo no arquimediano v, D_v contiene una subálgebra compacta maximal $\mathcal{O}_{D_v} \subset D_v$; si $D_v \xrightarrow{\sim} M(2, F_v)$ entonces $\mathcal{O}_{D_v} = M(2, \mathcal{O}_v)$. El álgebra $D(\mathbf{A})$ es el subconjunto de $(x_v) \in \prod_v D_v$ donde $x_v \in \mathcal{O}_{D_v}$ salvo en un número finito de primos. Además hay un homomorfismo inyectivo $F_{\mathbf{A}} := \mathbf{A}_F \to D(\mathbf{A})$ y la imagen es igual al centro de $D(\mathbf{A})$.

Del mismo modo, definimos el grupo de ideles de D como el producto restringido $D^\times(\mathbf{A}) = \prod_v' D_v^\times = \prod_v' G_v$. Escribimos $D^\times(\mathbf{A}) = D_\infty^\times \times D^\times(\mathbf{A}_f)$, donde $D_\infty^\times = \prod_{v\in\Sigma} D_v^\times$ y $D^\times(\mathbf{A}_f) = \prod_{v finito}' D_v^\times$. La

norma reducida $\nu : D \to F$ es un mapeo multiplicativo y así define homomorfismos locales y globales:

$$\nu_v : G_v \to F_v^\times,\ \nu : G \to F^\times, \nu_{\mathbf{A}} : D^\times(\mathbf{A}) \to F_{\mathbf{A}}^\times.$$

La norma local ν_v es suryectiva si v es un primo finito o si $D_v \simeq M(2,\mathbb{R})$; si $D_v \simeq \mathbb{H}$, el álgebra de cuaterniones de Hamilton, la imagen de la norma local ν_v es el grupo de números reales *positivos*.

Escribimos $D_F^\times$ para los elementos globales, es decir el grupo multiplicativo del álgebra D de dimensión 4 sobre F. Podemos considerar $D_F^\times$ como subgrupo de $D^\times(\mathbf{A})$. El *grupo de congruencia de nivel* K $\Gamma_K \subset D_F^\times$ es la intersección en $D^\times(\mathbf{A})$ de $D_F^\times$ con un subgrupo compacto abierto $K \subset D^\times(\mathbf{A}_f)$.

Sea $\Sigma_D \subset \Sigma$ (resp. $\Sigma'_D \subset \Sigma$) el subconjunto de los v no ramificados (resp. ramificados), para los cuales $D_v \simeq M(2,\mathbb{R})$ (resp. $D_v \simeq \mathbb{H}$). Sea $\mathfrak{H}^\pm = \mathbb{C} \setminus \mathbb{R}$, la unión de los semiplanos superior e inferior. Hay una acción del grupo $D_\infty^\times = \prod_{v\in\Sigma} D_v^\times$ sobre $\mathfrak{H}^{\pm,\Sigma_D} = \prod_{v\in\Sigma_D} \mathfrak{H}_v^\pm$: si $v \in \Sigma_D$ el factor $D_v^\times \xrightarrow{\sim} GL(2,\mathbb{R})$ actúa sobre el factor $\mathfrak{H}_v^\pm$ y los factores $D_v^\times$ con $v \in \Sigma'_D$ actúan trivialmente. Sea $\Gamma_K \subset D_F^\times$ el grupo de congruencia de nivel K. Via la inclusión $\Gamma_K \hookrightarrow D_\infty^\times$ tenemos una acción de Γ_K sobre $\mathfrak{H}^{\pm,\Sigma_D}$.

Fijamos un punto $h \in \mathfrak{H}^{\pm,\Sigma_D}$ y definimos $\tilde{K}_\infty = \tilde{K}_h \subset D_\infty^\times$ [con virgulilla] como el estabilizador de h:

$$\tilde{K}_\infty = \{g \in D_\infty^\times \mid g(h) = h\}. \tag{1.1}$$

El grupo $\tilde{K}_\infty$ contiene el centro $Z_\infty = \prod_{v\in\Sigma} F_v^\times$ de $D_\infty^\times$, y el cociente $\tilde{K}_\infty/Z_\infty$ es compacto. Sea $K_\infty = K_h$ el subgrupo compacto maximal de $\tilde{K}_\infty$ (hay solo uno), que además es compacto maximal conexo en $D_\infty^\times$. La definición de formas modulares sobre $D^\times(\mathbf{A})$ (ver más abajo) depende de la elección de un subgrupo compacto maximal $K_\infty \in D_\infty^\times$, pero distintos K_∞ dan teorías equivalentes (espacios isomorfos) de formas modulares.

Proposición 1.2. *La acción de* Γ_K *sobre* $\mathfrak{H}^{\pm,\Sigma_D}$ *es propiamente discontinua. Si* D *es un álgebra de división, entonces el cociente* $\Gamma_K\backslash\mathfrak{H}^{\pm,\Sigma_D}$ *es compacto.*

La propia discontinuidad se muestra como en el caso del semiplano superior.

Ejercicio 1.1. Demostrar la propia discontinuidad.

Para mostrar la compacidad, utilizamos el teorema siguiente del libro *Basic Number Theory* de Weil (Theorem IV.3.4) :

Teorema 1.3. *Sea D un álgebra de división de dimensión finita sobre F. Para cada número real $\mu \geq 1$, sea*

$$D_\mu = \{d \in D^\times(\mathbf{A}) \mid ||d||_{\mathbf{A}} \leq \mu, ||d||^{-1} \geq \mu^{-1}\}$$

Entonces D_μ es un conjunto cerrado en $D^\times(\mathbf{A})$ y la imagen de D_μ en $D^\times \backslash D^\times(\mathbf{A})$ es compacta.

Si $D = F$, el enunciado sigue del argumento de la geometría de números utilizado para demostrar la finitud del número de clases y el teorema de Dirichlet. El caso de un álgebra no conmutativa es exactamente lo mismo. En particular, si $D_1 = \ker || \bullet || : D^\times(\mathbf{A}) \to \mathbb{R}^\times$, el teorema de Weil implica que $D^\times \backslash D_1 / K \cdot K_\infty$ es compacto.

El cociente $\Gamma_K \backslash \mathfrak{H}^{\pm, \Sigma_D}$ es un ejemplo de una *variedad de Shimura conexa* de dimensión $|\Sigma_D|$. Cuando $|\Sigma_D| = 1$, es una *curva de Shimura conexa*. (Es un abuso escribir eso; esa curva no es necesariamente conexa, porque $\mathfrak{H}^\pm$ tiene 2 componentes conexas. Pero es más sencillo no separar las componentes conexas de $\mathfrak{H}^\pm$.) Resulta de la proposición que el subgrupo de Γ_K que estabiliza una componente conexa $\mathfrak{H}^+$ de $\mathfrak{H}^\pm$ es un grupo Fuchsiano, de modo que $\Gamma_K \backslash \mathfrak{H}^{\pm, \Sigma_D}$ es isomorfa a la unión de uno o dos cocientes de $\mathfrak{H}^+$ por un grupo Fuchsiano. Todavia no es ese el objeto que nos interesa. Cuando el grupo de clases h_F es de orden > 1 no se pueden definir operadores de Hecke de modo natural sobre esas variedades conexas. Para eso tenemos que trabajar con las variedades de Shimura adélicas. Además, para las aplicaciones aritméticas, hay que construir modelos de las variedades de Shimura sobre cuerpos de números.

En el resto del curso, siempre vamos a suponer que $|\Sigma_D| = 1$; entonces la variedad es una curva de Shimura. Para evitar dificultades técnicas es mejor en este curso trabajar con el grupo $PD = D^\times / F^\times$, y con los grupos locales $PD_\infty = D_\infty^\times / F_\infty^\times$ y adélicos $PD(\mathbf{A}) = D^\times(\mathbf{A}) / F_{\mathbf{A}}^\times$, $PD(\mathbf{A}_f) = D^\times(\mathbf{A}_f) / F^\times(\mathbf{A}_f)$. Eso tiene sentido porque el centro $F_\infty^\times$ de $D_\infty^\times$ actúa trivialmente sobre $\mathfrak{H}^{\pm, \Sigma_D} = \mathfrak{H}^\pm$. Una curva de Shimura adélica de nivel $K \subset PD(\mathbf{A}_f) = D^\times(\mathbf{A}_f) / F^\times(\mathbf{A}_f)$ es el cociente

$$_K S(D) = PD \backslash [\mathfrak{H}^{\pm, \Sigma_D} \times PD(\mathbf{A}_f) / K].$$

Exactamente como en el caso de la variedad modular de Hilbert, hay un conjunto finito $U = \{u_i, i \in I\}$ y una descomposición

$$PD(\mathbf{A}) = D^\times(\mathbf{A}) / F_{\mathbf{A}}^\times = \coprod_{i \in I} PD u_i [PD_\infty \times K].$$

Pero esa descomposición es más sencilla que en el caso de $GL(2, F)$ cuando D es un álgebra de división; como Weil muestra en su libro

Basic Number Theory, la demostración de la finitud del número de clases se aplica sin cambio a un tal cociente. Entonces, si escribimos (1.4)

$$_KS(D) = PD\backslash[\mathfrak{H}^{\pm,\Sigma_D} \times (PD(\mathbf{A}_f)/K)] = PD\backslash[\coprod_{i\in I} \mathfrak{H}^{\pm,\Sigma_D} \times PDu_iK/K]$$

se puede escribir

$$\coprod_{i\in I}[PD \cap u_iKu_i^{-1}\backslash\mathfrak{H}^{\pm,\Sigma_D}] = \coprod_{i\in I} \Gamma_i\backslash\mathfrak{H}^{\pm,\Sigma_D}$$

donde hemos escrito

$$\Gamma_i = PD \cap u_iKu_i^{-1} = \Gamma_{u_iKu_i^{-1}}$$

en nuestra notación anterior.

En efecto, si $x, x' \in \mathfrak{H}^{\pm,\Sigma_D}$, entonces las imágenes de xu_i y $x'u_j$ en el cociente

$$PD\backslash[\coprod_{i\in I} \mathfrak{H}^{\pm,\Sigma_D} \times PDu_i \times K]/K$$

coinciden si, y solamente si, $u_i = u_j$ y hay $d \in PD$, $k \in K$, con

$$dxu_ik = x'u_i \Leftrightarrow x' = dx[u_iku_i^{-1}].$$

Pero como $x', x \in \mathfrak{H}^{\pm,\Sigma_D}$ y $u_iku_i^{-1} \in D^\times(\mathbf{A}_f)/F^\times(\mathbf{A}_f)$, eso quiere decir que $d[u_iku_i^{-1}] = 1 \in D^\times(\mathbf{A}_f)/F^\times(\mathbf{A}_f)$; de modo que $d \in \Gamma_i$. Asi la imagen de xu_i en $\mathfrak{H}^{\pm,\Sigma_D}$ es bien determinada en $\Gamma_i\backslash\mathfrak{H}^{\pm,\Sigma_D}$.

Ya hemos demostrado esa proposición:

Proposición 1.5. *El cociente adélico*

$$_KS(D) = (D^\times/F^\times)\backslash[\mathfrak{H}^{\pm,\Sigma_D} \times (D^\times(\mathbf{A}_f)/F^\times(\mathbf{A}_f))/K]$$

es una unión finita de curvas de Shimura conexas.

1.2. Curvas de Shimura: teoría analítica de formas modulares. Todas las consideraciones en esta sección son válidas para cualquier álgebra cuaterniónica de división D. Pero como ya hemos dicho, siempre vamos a suponer que $|\Sigma_D| = 1$, y escribiremos $\mathfrak{H}^\pm$ en vez de $\mathfrak{H}^{\pm,\Sigma_D}$.

Sea v el único primo arquimediano en Σ_D, y sea $\tilde{K}_v = \tilde{K}_\infty \cap D_v^\times$. Entonces $D_v \simeq M(2,\mathbb{R})$, y tenemos un isomorfismo $D_v^\times/\tilde{K}_v = \mathfrak{H}^\pm$: entonces $\tilde{K}_v$ es el estabilizador de h y el mapeo

$$p_h : D_v^\times/\tilde{K}_v \to \mathfrak{H}^\pm : d \mapsto d(h)$$

es un isomorfismo C^∞. El estabilizador $\tilde{K}_\infty$ de h es entonces igual a $\tilde{K}_v \times \prod_{w\neq v} D_w^\times$, y tenemos también un isomorfismo C^∞

$$p_{h,\infty} : \prod_w D_w^\times/(\tilde{K}_v \times \prod_{w\neq v} D_w^\times) \xrightarrow{\sim} \mathfrak{H}^\pm. \tag{1.6}$$

El grupo $\tilde{K}_v$ estabiliza el punto h y por esta razón actúa sobre el espacio tangente complexificado $T_{\mathfrak{H}^\pm,h,\mathbb{C}} = T_{\mathfrak{H}^\pm,h} \otimes \mathbb{C}$ de $\mathfrak{H}^\pm$ en h. Sabemos además que la acción de $D_v^\times$ sobre $\mathfrak{H}^\pm$ conserva la estructura analítica del espacio. Así la acción $\tilde{K}_v$ sobre $T_{\mathfrak{H}^\pm,h,\mathbb{C}}$ conserva la descomposición en subespacios holomorfa y anti-holomorfa, cada uno de dimensión uno:

$$T_{\mathfrak{H}^\pm,h,\mathbb{C}} \xrightarrow{\sim} T_h^{hol} \oplus \bar{T}_h^{hol}.$$

El diferencial del mapeo p_h es un mapeo suryectivo

$$dp_h : T_{D_v^\times,1,\mathbb{C}} \to T_{\mathfrak{H}^\pm,h,\mathbb{C}}.$$

Ponemos $\mathfrak{g}_v$ el álgebra de Lie del grupo de Lie $D_v^\times \xrightarrow{\sim} GL(2,\mathbb{R})$, e identificamos $\mathfrak{g}_v$ con $M(2,\mathbb{R})$. Como $T_{D_v^\times,1} = \mathfrak{g}_v$, el diferencial es un mapeo suryectivo

$$M(2,\mathbb{C}) \to T_{\mathfrak{H}^\pm,h,\mathbb{C}}$$

que además es un homomorfismo de representaciones del grupo $\tilde{K}_v$. Aquí la acción de $\tilde{K}_v$ sobre $M(2,\mathbb{C})$ es dada por conjugación (representación adjunta):

$$ad(k)(X) = kXk^{-1}, k \in \tilde{K}_v, X \in M(2,\mathbb{C}).$$

De aquí en adelante, h designa el punto $i \in \mathfrak{H}^+$. Con esta convención, el estabilizador $\tilde{K}_v$ en $GL(2,\mathbb{R})$ es nada más que el subgrupo de matrices $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ con $a, b \in \mathbb{R}$ y $a^2+b^2 \neq 0$. (Y el mapeo $a+bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ define un isomorfismo $\mathbb{C}^\times \xrightarrow{\sim} \tilde{K}_v$). Es fácil descomponer $M(2,\mathbb{C})$ en espacios propios para la acción de $\tilde{K}_v$: si

$$\tilde{\mathfrak{k}}_v = Lie(\tilde{K}_v) \otimes \mathbb{C} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix},\ a, b \in \mathbb{C} \right\},$$

entonces

$$M(2,\mathbb{C}) = \tilde{\mathfrak{k}}_v \oplus \mathfrak{p}^+ \oplus \mathfrak{p}^-$$

con

$$\mathfrak{p}^+ = \mathbb{C}X^+, \mathfrak{p}^- = \mathbb{C}X^-, X^+ = \begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}, X^- = \begin{pmatrix} 1 & -i \\ -i & -1 \end{pmatrix}.$$

Resulta de un cálculo fácil que

Lema 1.7. *El diferencial dp_h identifica $\mathfrak{p}^+ \xrightarrow{\sim} T_h^{hol}$, $\mathfrak{p}^- \xrightarrow{\sim} \bar{T}_h^{hol}$. Una función $\phi : \mathfrak{H}^{\pm} \to \mathbb{C}$ es holomorfa si y solamente si la función compuesta $\Phi = \phi \circ p_h : D_v^{\times} \to \mathbb{C}$ es una solución de la ecuación diferencial $X^- \Phi = 0$.*

Ejercicio 1.2. Demostrar el Lema 1.7.

Más generalmente, ponemos $\tilde{\mathfrak{k}} = Lie(\tilde{K}_\infty) = \tilde{\mathfrak{k}}_v \oplus \oplus_{w \neq v} Lie(D_w^{\times})$.

1.2.1. Formas modulares y funciones adélicas. Una *forma modular clásica* sobre la curva (no conexa) ${}_K S(D)$ es una función holomorfa sobre $\mathfrak{H}^{\pm, \Sigma_D} \times (D^{\times}(\mathbf{A}_f)/K)$ que satisface una ecuación funcional que corresponde a sus pesos, que en nuestra situación son enteros pares (porque todas nuestras formas son supuestas invariantes por la acción de $F^{\times}(\mathbf{A})$). Pero como la componente $D_w^{\times}$, con $w \neq v$, es compacta módulo $F_w^{\times}$, no podemos definir un factor como $c_w z_w + d_w$ en la coordenada w. En vez de eso, tenemos que utilizar las representaciones irreducibles del grupo $D_w^{\times}$, que generalmente son de dimensión superior a 1; es decir, tenemos que introducir *formas modulares con valores vectoriales*.

Podemos tratar todos los primos arquimedianos de manera homogénea. Sea $\rho : \tilde{K}_\infty / (\prod_{w|\infty} F_w^{\times}) \to GL(W)$ una representación irreducible, con $W = W_\rho$ un espacio vectorial complejo de dimensión finita. Una tal representación admite una factorización

$$\rho = \rho_v \otimes_{w \neq v} \rho_w, \rho_v : \tilde{K}_v / F_v^{\times} \to \mathbb{C}^{\times}, \rho_w : \tilde{K}_w / F_w^{\times} \xrightarrow{\sim} \mathbb{H}^{\times} / \mathbb{R}^{\times} \to GL(W_w)$$

donde todos los ρ_w son irreducibles. Definimos el *factor de automorfía*

$$j_\rho : D_v^{\times} \times \prod_{w \neq v} D_w^{\times} \times \mathfrak{H}^{\pm} \to GL(W) = GL(\otimes_{w \neq v} W_w);$$

$$j_\rho \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, (g_w), z \right) = \rho_v(cz + d) \cdot \otimes_{w \neq v} \rho_w(g_w). \tag{1.8}$$

Ejercicio 1.3. Demostrar que j_ρ satisface la ecuación funcional de factores de automorfía:

$$j_\rho(g_v g_v', (g_w)(g_w'), z) = j_\rho(g_v, (g_w), g_v'(z)) j_\rho(g_v', (g_w'), z).$$

Vamos a escribir $j_\rho(g, z)$ con $g = (g_v, (g_w)) \in D_\infty^{\times}$.

Así podemos definir una *forma modular clásica de peso ρ* por la fórmula habitual:

Definición 1.9. Sea $K \subset D^{\times}(\mathbf{A}_f)$ un subgrupo abierto compacto. Una forma modular de peso ρ y de nivel K para $D^{\times}$ es una función holomorfa

$$f : \mathfrak{H}^{\pm} \times D^{\times}(\mathbf{A}_f)/K \to W$$

que satisface la ecuación funcional

$$f(d(z), \iota_f(d) \cdot g_f) = j_\rho(\iota_\infty(d))f(z), z \in \mathfrak{H}^{\pm}, d \in D^\times.$$

Aquí hemos designado por ι_∞ (respectivamente ι_f) la inclusión

$$\iota_\infty : D^\times \hookrightarrow D_\infty^\times (\text{ respectivamente } \iota_f : D^\times \hookrightarrow D^\times(\mathbf{A}_f).$$

Vamos a designar por $M_\rho(D^\times, K)$ el espacio de formas modulares clásicas de peso ρ y de nivel K. Si ρ_v es el homomorfismo $x \mapsto x^2$ y si ρ_w es la representación trivial para $w \neq v$, escribimos $M_{(2,2,\ldots,2)}(D^\times, K)$ en vez de $M_\rho(D^\times, K)$. Como en el caso de formas modulares de Hilbert, tenemos la descripción siguiente de $M_{(2,2,\ldots,2)}(D^\times, K)$:

Proposición 1.10. *Hay un isomorfismo natural*

$$M_{(2,2,\ldots,2)}(D^\times, K) \xrightarrow{\sim} \Omega^1({}_K S(D))$$

donde $\Omega^1({}_K S(D))$ *designa el espacio de diferenciales holomorfos sobre* ${}_K S(D)$.

2. Formas modulares cuaterniónicas y curvas de Shimura

Antes de presentar las definiciones formales, quisiera explicar que una forma modular sobre el grupo $G = D^\times$ admite una descomposición como combinación lineal de autoformas para operadores de Hecke, exactamente como las formas modulares de Hilbert, con algunas modificaciones naturales. El aspecto más importante de la teoría es que una autoforma sobre el grupo multiplicativo de D contiene la misma información que una autoforma modular de Hilbert. Hay una *correspondencia* entre autoformas modulares sobre $D^\times$ y autoformas modulares de Hilbert. La correspondencia es inyectiva: todas las autoformas (más precisamente, sistemas de autovalores) sobre $D^\times$ tienen realizaciones como autoformas modulares de Hilbert, pero no todas las autoformas de Hilbert surgen de esta manera de $D^\times$. La correspondencia se llama *correspondencia de Jacquet-Langlands* y es una motivación principal para el estudio de formas modulares sobre $D^\times$. La propiedad principal de esta correspondencia es la preservación de funciones L.

2.1. Definiciones. En esta sección, D es un álgebra de cuaterniones *de división* sobre el cuerpo totalmente real F. Escribimos $D^\times(\mathbf{A}) = D_\infty^\times \times D^\times(\mathbf{A}_f)$ como en la sección precedente.

Definición 2.1. Una forma modular (forma automorfa) sobre $D^\times$ es una función $f : D^\times(\mathbf{A}) \to \mathbb{C}$ con las propiedades siguientes:

1. Para cualquier $g_f \in D^\times(\mathbf{A}_f)$, $g_\infty \mapsto f(g_\infty, g_f)$ es una función C^∞ sobre $D_\infty^\times$.

2. Para cualquier $g_\infty \in D_\infty^\times$, $g_f \mapsto f(g_\infty, g_f)$ es una función localmente constante sobre $D^\times(\mathbf{A}_f)$.
3. Para cualquier $\gamma \in D^\times$ y $g \in D^\times(\mathbf{A})$, $f(\gamma \cdot g) = f(g)$.
4. Existe un subgrupo $K_f \subset D^\times(\mathbf{A}_f)$, abierto y compacto, tal que $f(gk) = f(g)$ para cualquier $g \in D^\times(\mathbf{A})$ y $k \in K_f$.
5. Sea $C(D^\times(\mathbf{A}))$ el espacio de funciones continuas complejas sobre $D^\times(\mathbf{A})$. El subespacio de $C(D^\times(\mathbf{A}))$ generado por las funciones $g \mapsto f(gk_\infty z)$, con $k_\infty \in K_\infty$, y con $z \in F^\times(\mathbf{A})$ (el centro de $D^\times(\mathbf{A})$) es de dimensión finita.
6. Sea $v \in \Sigma_D$ un primo arquimediano de F con $D_v \simeq M(2, \mathbb{R})$. Sea $C_v \in U(Lie(D_v))$ el operador de Casimir (ver el curso de A. Pacetti). Entonces el subespacio de $C(D^\times(\mathbf{A}))$ generado por las funciones $\prod_{v \in \Sigma_D} C_v^{k_v} f$, $k_v = 0, 1, 2, 3, \ldots$, es de dimensión finita.

A diferencia de lo que pasa en el caso de formas modulares de Hilbert, el cociente $(D_\infty^\times \times D^\times(\mathbf{A}_f))/F^\times(\mathbf{A})$ es compacto (como ya hemos visto), y no es necesario imponer una condición de crecimiento moderado. Vamos a designar por $\mathcal{A}(D^\times)$ el espacio de formas modulares sobre $D^\times$; esta notación queda válida cuando $D = M(2, F)$ es el álgebra de matrices. Si W es un espacio vectorial complejo de dimensión finita, podemos definir una forma modular sobre $D^\times$ con valores en W como una función $f : D^\times(\mathbf{A}) \to W$ tal que, para toda forma lineal $\lambda : W \to \mathbb{C}$, $\lambda \circ f$ es una forma modular en el sentido de la Definición 2.1.

Como en el caso de formas modular de Hilbert, las formas modulares clásicas para $D^\times$ se identifican con formas modulares adélicas. Si $d = (d_\infty, d_f) \in D^\times(\mathbf{A})$, $f \in M_\rho(D^\times, K_f)$, definimos

(2.2)

$$\Phi = \Phi(f) : D^\times \backslash D^\times(\mathbf{A})/K_f \to W; \Phi(d_\infty, d_f) = j_\rho(d_\infty, i)^{-1} f(d_\infty(i), d_f).$$

Proposición 2.3. *El mapeo $f \mapsto \Phi(f)$ define un isomorfismo entre $M_\rho(D^\times, K_f)$ y el espacio $\mathcal{A}^{hol}(D^\times, K_f, \rho)$ de formas modulares $\Phi : D^\times \backslash D^\times(\mathbf{A})/K_f \to W$ tales que*

(i) $dr(X^-)\Phi = 0$, donde $r : D_\infty^\times \to Aut(\mathcal{A}(D^\times))$ es la representación regular de multiplicación por la derecha y $dr : Lie(D_\infty^\times) \to End(\mathcal{A}(D^\times))$ es su diferencial.

(ii) Para todo $k \in \tilde{K}_\infty$ y todo $d = (d_\infty, d_f) \in D^\times(\mathbf{A})$, $\Phi(d_\infty k, d_f) = \rho(k)^{-1}\Phi(d)$.

La demostración es idéntica a la del caso de formas modulares de Hilbert.

Para tratar todas las formas automorfas de manera uniforme, es más natural reemplazar el espacio $\mathcal{A}^{hol}(D^\times, K_f, \rho)$ de formas modulares

vectoriales por la imagen de $\mathcal{A}^{hol}(D^\times, K_f, \rho) \otimes Hom(W_\rho, \mathbb{C})$ en $\mathcal{A}(D^\times)$ bajo el mapeo natural

$$\mathcal{A}^{hol}(D^\times, K_f, \rho) \otimes Hom(W_\rho, \mathbb{C}) \hookrightarrow \mathcal{A}(D^\times(\mathbf{A}), W_\rho) \otimes Hom(W_\rho, \mathbb{C}) \to \mathcal{A}(D^\times),$$

donde $\mathcal{A}(D^\times, W_\rho)$ designa el espacio de funciones de $D^\times(\mathbf{A})$ con valores en W_ρ que satisfacen las condiciones de la Definición 2.1, y la última flecha es inducida por contracción del producto tensorial

$$W_\rho \otimes Hom(W_\rho, \mathbb{C}) \to \mathbb{C}.$$

Así vamos a trabajar únicamente con formas modulares adélicas con valores complejos.

Si $f \in \mathcal{A}(D^\times)$ y si $g \in D^\times(\mathbf{A})$ definimos $r(g)(f) \in \mathcal{A}(D^\times)$ por la fórmula

$$r(g)(f)(d) = f(dg)$$

(traslación por la derecha). La acción $g \mapsto r(g) \in Aut(\mathcal{A}(D^\times))$ define una representación de $D^\times(\mathbf{A})$ en el espacio $\mathcal{A}(D^\times)$.

Definición 2.4. Una representación automorfa de $D^\times(\mathbf{A})$ es una subrepresentación irreducible de $\mathcal{A}(D^\times)$.

Esta definición queda válida cuando $D = M(2, F)$. En este caso, $\mathcal{A}(GL(2, F))$ contiene el subespacio $\mathcal{A}^0(GL(2, F))$ de *formas cuspidales* como subrepresentación. Una *representación automorfa cuspidal* de $GL(2, F_\mathbf{A})$ es una subrepresentación irreducible de $\mathcal{A}^0(D^\times)$.

Comentario 2.5. Si trabajamos con el grupo $PD = D^\times/F^\times$ y consideramos el subespacio

$$\mathcal{A}(PD) = \mathcal{A}(D^\times) \cap C(D^\times(\mathbf{A})/F^\times(\mathbf{A}))$$

entonces $\mathcal{A}(PD)$ es también una representación de $D^\times(\mathbf{A})$ que además es isomorfa a una suma *numerable* de representaciones irreducibles, si D es un álgebra de división. (En el caso contrario, hay que considerar también los espacios de series de Eisenstein.)

2.2. Funciones L. Sea f una autoforma modular sobre $D^\times$. No es un grupo conmutativo, pero el método de la tesis de Tate se aplica casi sin cambio en esta situación para permitir la definición de una función L de f. Seguimos la versión de este método en el libro *Zeta Functions of Simple Algebras* de Godement y Jacquet [5].

Más precisamente, el grupo adélico multiplicativo $D^\times(\mathbf{A})$ está contenido en el grupo $D(\mathbf{A})$. Sea $\varphi : D^\times(\mathbf{A}) \to \mathbb{C}$ una forma modular y sea $\Phi : D(\mathbf{A}) \to \mathbb{C}$ una función con soporte compacto. (Suponemos que φ

es invariante bajo $F_{\mathbf{A}}^{\times}$ para simplificar las fórmulas.) Podemos definir una integral zeta:

$$Z(\varphi, \Phi, s) = \int_{D^{\times}(\mathbf{A})} \varphi(g)\Phi(g)||\nu(g)||^s d^{\times}g \tag{2.6}$$

que es absolutamente convergente para $Re(s) >> 0$. Suponemos que Φ tiene una factorización $\Phi = \otimes'_v \Phi_v$ donde $\Phi_v = 1_{\mathcal{O}_{D_v}}$ en casi todo primo no arquimediano v. Suponemos también que φ tiene una factorización análoga $\varphi = \otimes'_v \varphi_v$. Para interpretar esa condición es necesario utilizar la teoría de representaciones; tenemos que suponer que F es un vector en una subrepresentación irreducible Π de $L_2(F_{\mathbf{A}}^{\times} D^{\times} \backslash D^{\times}(\mathbf{A}))$. Entonces hay una factorización $\Pi \xrightarrow{\sim} \otimes'_v \Pi_v$, donde Π_v es una representación irreducible de $D_v^{\times}$. Entonces para $Re(s) >> 0$ la integral zeta tiene un producto de Euler convergente:

$$Z(\varphi, \Phi, s) = \prod_v Z_v(\varphi_v, \Phi_v, s)$$

Además, podemos definir la transformada de Fourier $\hat{\Phi}$ de Φ. Sea $\psi = \otimes \psi_v : F \backslash F_{\mathbf{A}} \to \mathbb{C}^{\times}$ un carácter aditivo no trivial, con $\psi_v : F_v \to \mathbb{C}^{\times}$. Ponemos

$$\hat{\Phi}(x) = \int_{D(\mathbf{A})} \Phi(y)\psi \circ Tr_D(xy)dy; \ \hat{\Phi}_v(x) = \int_{D_v} \Phi_v(y) Tr_D(xy)dy$$

donde $Tr_D : D \to F$ es la traza reducida y dy es una medida de Haar autodual. Si ponemos $\varphi^{\vee}(g) = \varphi(g^{-1})$, $\varphi_v^{\vee}(g_v) = \varphi(g_v^{-1})$, entonces

Teorema 2.7. *Para cada primo v se pueden definir factores locales $L_v(\Pi_v, s)$ y $\varepsilon(\Pi_v, \psi_v, s)$ como en la tesis de Tate con las propiedades siguientes:*

1. *Para toda Φ_v y toda $f_v \in \Pi_v$, el cociente*
$$\Xi(\varphi_v, \Phi_v, s) := \frac{Z_v(\varphi_v, \Phi_v, s + \frac{1}{2})}{L_v(\Pi_v, s)}$$
es una función entera de s.
2. *Si v es un primo no arquimediano, $q = Nv$, o sea $L_v(\Pi_v, s) = 1$, o sea $L_v(\Pi_v, s)$ es producto de uno o dos factores de Euler de la tesis de Tate, y la función $\Xi(\varphi_v, \Phi_v, s)$ es un polinomio en q^s y q^{-s}.*
3. *Si v es un primo arquimediano entonces $L_v(\Pi_v, s)$ es un producto de potencias de π y de factores Γ.*
4. *El factor $\varepsilon(\Pi_v, \psi_v, s)$ es una función entera de s, y hay una ecuación funcional local:*
$$\Xi(\varphi_v^{\vee}, \hat{\Phi}_v, 1 - s) = (-1)^{e_v} \varepsilon(\Pi_v, \psi_v, s) Z_v(\varphi_v, \Phi_v, s)$$

donde $e_v = 0$ *si* $D_v = M(2, F_v)$ *y* $e_v = 1$ *si* D_v *es un álgebra de división.*

Exactamente como en la tesis de Tate, hay también una ecuación funcional global:

Teorema 2.8. *Sea* φ *y* Φ*, y* $Z(F, \Phi, s)$ *como en* (2.6)*. Entonces*

$$Z(\varphi, \Phi, s) = Z(\varphi^\vee, \hat{\Phi}, 2 - s).$$

Finalmente, definimos la función L de Π como el producto de Euler

$$L(\Pi, s) = \prod_v L_v(\Pi_v, s). \tag{2.9}$$

El producto es convergente para $Re(s) >> 1$ (de hecho, para $Re(s) > 1$ con nuestras hipótesis). Definimos el factor epsilon del mismo modo:

$$\varepsilon(\Pi, s) = \prod_v \varepsilon_v(\Pi_v, \psi_v, s). \tag{2.10}$$

El producto es independiente del carácter ψ escogido. Como en la tesis de Tate, deducimos formalmente la ecuación funcional de la función L:

Corolario 2.11.

$$L(\Pi, s) = \varepsilon(\Pi, s) L(\Pi^\vee, 1 - s)$$

2.3. Operadores de Hecke. Fijamos un grupo de nivel abierto compacto $K \subset D^\times(\mathbf{A}_f)$. El álgebra de Hecke $\mathcal{H}(K)$ (respectivamente $\mathcal{H}(K)_\mathbb{Z}$) de nivel K es el álgebra $C_c(D^\times(\mathbf{A}_f)//K)$ (respectivamente $C_c(D^\times(\mathbf{A}_f)//K, \mathbb{Z})$) de funciones continuas sobre $D^\times(\mathbf{A}_f)$ con soporte compacto con valores en $\mathbb{C}$ (respectivamente en $\mathbb{Z}$), invariante bajo multiplicación por ambos lados por elementos de K. Es un álgebra para la convolución

$$\phi_1 \star \phi_2(g) = \int_{D^\times(\mathbf{A}_f)} \phi_1(h)\phi_2(gh^{-1})dh$$

donde tomamos la medida de Haar dh normalizada de tal forma que tenemos $\int_K dh = 1$. Entonces la función característica 1_K de K es el elemento neutro del álgebra $\mathcal{H}(K)$. Suponemos que $K = \prod_v K_v$ con K_v abierto compacto en $D_v^\times$. El álgebra local $\mathcal{H}(K_v)$ (respectivamente $\mathcal{H}(K_v)_\mathbb{Z}$) es el álgebra $C_c(D_v^\times//K_v)$ (respectivamente $C_c(D_v^\times//K_v, \mathbb{Z})$), definida de la misma manera.

2.3.1. Álgebra de Hecke no ramificada (esférica). Si v es un primo no ramificado para D y si $K_v = GL(2, \mathcal{O}_v)$, entonces $\mathcal{H}(K_v)$ es el álgebra de Hecke clásica. Tomamos la medida de Haar dh_v con $\int_{K_v} dh_v = 1$. El álgebra $\mathcal{H}(K_v)$ tiene como generadores $R_v = K_v \cdot \begin{pmatrix} \varpi_v & 0 \\ 0 & \varpi_v \end{pmatrix} K_v$, I_v^{-1}, y $T_v = K_v \cdot \begin{pmatrix} \varpi_v & 0 \\ 0 & 1 \end{pmatrix} K_v$, con ϖ_v un uniformizador de F_v.

2.3.2. Acción de operadores de Hecke sobre formas modulares. Sea $f \in M_\rho(D^\times, K_f)$ una forma modular clásica de peso ρ y de nivel K_f. Suponemos que v es un primo *no ramificado* para K_f: $K_f \supset K_v = GL(2, \mathcal{O}_v)$. Entonces el álgebra de Hecke esférica $\mathcal{H}(K_v)$ actua sobre el espacio $\mathcal{A}^{hol}(D^\times, K_f, \rho)$. Si $T \in \mathcal{H}(K_v)$, definimos $T^{class}(f)$ por la fórmula

$$\Phi(T^{class}(f)) = T(\Phi(f)) \tag{2.12}$$

En particular, si la forma automorfa $\Phi(f) \in \mathcal{A}^{hol}(D^\times, K_f, \rho)$ es un vector propio para el álgebra $\mathcal{H}(K_v)$, entonces f es también un vector propio para los operadores de $\mathcal{H}(K_v)$. Los operadores T^{class} coinciden con los operadores de Hecke clásicos, salvo multiplicación por factores escalares de normalización.

2.4. Teoría local de representaciones, caso no arquimediano.

En este párrafo k es un cuerpo p-ádico, con anillo de enteros $\mathcal{O}$ y valor absoluto $|\bullet|_k$. Los dos lemas siguientes son básicos.

Lema 2.13 (Lema de Schur)**.** *Sea π una representación lisa e irreducible de $GL(2, k)$. Sea $Z = k^\times \subset GL(2, k)$ el centro de $GL(2, k)$. Entonces existe un homomorfismo $\xi_\pi : Z \to \mathbb{C}^\times$, el carácter central de π, tal que, para todo $v \in \pi$ y todo $z \in Z$,*

$$\pi(z)v = \xi_\pi(z)v.$$

En el Lema de Schur, la hipótesis que π sea lisa es esencial.

Ejercicio 2.1. Demostrar el Lema de Schur: Sea $U \subset GL(2, k)$ un subgrupo abierto tal que el subespacio

$$\pi^U = \{v \in \pi \mid \pi(u)v = v \ \forall \ u \in U\}$$

es de dimensión positiva. Sea $z \in Z$. Mostrar que el grupo Z estabiliza el subespacio π^U y que existe un vector $v \in \pi^U$, $v \neq 0$, que es vector propio para todos los elementos de Z. Entonces utilizar la irreducibilidad de π para terminar la demostración.

Lema 2.14. *Sea π una representación lisa e irreducible de dimensión finita de $GL(2,k)$. Entonces* $\dim \pi = 1$ *y existe un carácter*continuo *(localmente constante) $\chi : k^\times \to \mathbb{C}^\times$ tal que $\pi = \chi \circ \det$ (el carácter se factoriza por medio del determinante).*

Ejercicio 2.2. (a) Demostrar que, si π es lisa y de dimensión finita, entonces hay un subgrupo abierto $U \subset GL(2,k)$ tal que $\pi^U = \pi$. En particular, existe $\varepsilon > 0$ tal que, si $a \in \mathcal{O}$, $|a|_k < \varepsilon$, entonces, para todo $v \in \pi$,

$$\pi\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\right) v = \pi\left(\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}\right) v = v.$$

(b) Demostrar el Lema 2.14.

Ahora pasamos a las tres clases de representaciones lisas de dimensión infinita.[1]

2.4.1. Serie principal. Sea (χ_1, χ_2) un par ordenado de caracteres de $k^\times$. Sea $G = GL(2,k)$, $B \subset G$ el subgrupo de Borel triangular superior, $B = A \cdot N$, con

$$A = \left\{ \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \right\}, \; N = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right\}.$$

Definimos

$$I(\chi_1, \chi_2) = \{f : G \to \mathbb{C} \mid f(ang) = \chi_1(a_1)|a_1|^{\frac{1}{2}} \chi_2(a_2)|a_2|^{-\frac{1}{2}} \cdot f(g)\}$$

(todas las funciones son supuestas continuas y localmente constantes). Eso es una representación inducida normalizada, y G actúa sobre $I(\chi_1, \chi_2)$ por traslación por la derecha:

$$r(g)f(h) = f(hg).$$

Las potencias $\frac{1}{2}$ de la norma garantizan que casi siempre tenemos un isomorfismo

$$I(\chi_1, \chi_2) \xrightarrow{\sim} I(\chi_2, \chi_1)$$

Más precisamente, tenemos una proposición:

Proposición 2.15. *(a) $I(\chi_1, \chi_2)$ es irreducible a menos que $\chi_1/\chi_2 = |\bullet|^{\pm 1}$.*

(b) Si $\chi_1/\chi_2 \neq |\bullet|^{\pm 1}$ entonces

$$I(\chi_1, \chi_2) \xrightarrow{\sim} I(\chi_2, \chi_1)$$

como representaciones irreducibles admissibles de $GL(2,F)$.

(c) Si $\chi_1/\chi_2 \neq |\bullet|^{\pm 1}$ entonces $I(\chi_1, \chi_2)^\vee \xrightarrow{\sim} I(\chi_1^{-1}, \chi_2^{-1})$.

[1] Las diapositivas de un seminario de Pilar Bayer, `http://www.icmat.es/seminarios/langlands/14.01.10/bayer.pdf`, contienen una buena introducción a este material.

Las representaciones $I(\chi_1, \chi_2)$ se llaman *representaciones de la serie principal*.

Sea $K = GL(2, \mathcal{O}) \subset G$, donde $\mathcal{O}$ es el anillo de enteros de k. Sea $\varpi \in \mathcal{O}$ un uniformizador, $q = |\mathcal{O}/\varpi\mathcal{O}|$. Suponemos χ_1 y χ_2 *no ramificados*. Entonces $I(\chi_1, \chi_2)$ contiene un vector K-invariante canónico f_0 definido por

$$f_0(k) = 1 \ \forall \ k \in K.$$

La descomposición de Iwasawa $G = B \cdot K$ implica que todos los valores de f_0 son determinados por este propiedad. Se puede definir un álgebra local de Hecke $H_{\mathbb{Z}}(G, K)$, la subálgebra del álgebra compleja $\mathcal{H}(K)$ definida antes, de funciones con valores en $\mathbb{Z}$; entonces por cualquier anillo A definimos $H_A(G, K) = H_{\mathbb{Z}}(G, K) \otimes_{\mathbb{Z}} A$. $H_A(G, K)$ es un álgebra conmutativa, y tiene como en el caso complejo dos generadores

$$T = K \cdot \begin{pmatrix} \varpi & 0 \\ 0 & 1 \end{pmatrix} \cdot K, \ R = K \cdot \begin{pmatrix} \varpi & 0 \\ 0 & \varpi \end{pmatrix} \cdot K;$$

$$H_A(G, K) = A[T, R, R^{-1}].$$

El álgebra de convolución $H(G)$ de todas la funciones localmente constantes y con soporte compacto opera sobre cualquier representación lisa de G, y la función f_0 es un autovector por su subálgebra $H_{\mathbb{C}}(G, K)$, con

$$T f_0 = q^{\frac{1}{2}}(\chi_1(\varpi) + \chi_2(\varpi)) f_0, \ R f_0 = \chi_1(\varpi)\chi_2(\varpi) f_0. \tag{2.16}$$

Una representación irreducible con un vector v_0 fijo por K es determinada, salvo isomorfismo, por sus autovalores t_0 y r_0 con $T(v_0) = t_0 v_0$, $R(v_0) = r_0 v_0$. Una tal representación se llama *esférica*.

Si $k = \mathbb{Q}_p$ entonces T es el operador clásico $T(p)$, y $R = T(p, p)$ (salvo normalización). La teoría clásica de los operadores de Hecke queda completamente sustituida por la teoría de representaciones esféricas.

2.4.2. Representaciones de Steinberg. Sea $\chi : k^\times \to \mathbb{C}^\times$ un carácter liso. Sea

$$\chi_1 = \chi \cdot | \bullet |^{-\frac{1}{2}}, \chi_2 = \chi \cdot | \bullet |^{\frac{1}{2}}.$$

En ese caso es fácil ver que la función $f_\chi(g) = \chi(det(g))$ pertenece a $I(\chi_1, \chi_2)$. Hay una sucesión exacta corta de representaciones admisibles

$$0 \to \mathbb{C} f_\chi \to I(\chi_1, \chi_2) \to St(\chi) \to 0$$

donde G actúa por $\chi \circ \det$ sobre $\mathbb{C} f_\chi$ y $St(\chi)$ es irreducible; las $St(\chi)$ son las representaciones de Steinberg. Cuando χ es el carácter trivial, llamamos $St(1)$ *la* representación de Steinberg.

La representación $I(\chi_2, \chi_1)$ es tambien reducible y tiene a $St(\chi)$ como subrepresentación, y a $\chi \circ \det$ como cociente.

2.4.3. Representaciones supercuspidales.

Definición 2.17. Sea π una representación irreducible de $GL(2,k)$. Decimos que π es *supercuspidal* si $Hom_{GL(2,F)}(\pi, I(\chi_1,\chi_2)) = 0$ para cualquier par (χ_1,χ_2) de caracteres.

No hay una construcción elemental de representaciones supercuspidales. La clasificación de estas representaciones más importante es la *correspondencia de Langlands*. Para explicar eso, necesitamos algunas definiciones suplementarias. Sea $\mathbb{F} = \mathcal{O}/\varpi\mathcal{O}$ el cuerpo residual de k, y $Frob : \bar{\mathbb{F}} \to \bar{\mathbb{F}}$ el automorfismo de Frobenius: $Frob(x) = x^q$. Sea W_k el grupo de Weil de F; lo podemos definir como el subgrupo de $\gamma \in Gal(\bar{k}/k)$ que actúan sobre $\bar{\mathbb{F}}$ como potencias enteras de $Frob$.

Teorema 2.18 (Tunnell, Kutzko)**.** *Hay una biyección entre las (clases de equivalencia de) representaciones supercuspidales de $GL(2,k)$ y (clases de equivalencia de) representaciones irreducibles de dimension 2 de W_k.*

La correspondencia de Langlands vale también para las representaciones supercuspidales de $GL(n,k)$ (Teorema de MH-Taylor y Henniart), pero la clasificación de representaciones no supercuspidales es técnicamente más complicada.

2.4.4. Representaciones discretas y temperadas.

Definición 2.19. Sea π una representación irreducible de $GL(2,k)$. Decimos que π es *discreta* si π es isomorfa, sea a una representación de Steinberg, sea a una representación supercuspidal. Decimos que π es *esencialmente temperada* si π es isomorfa, sea a una representación discreta, sea a una representación $I(\chi_1,\chi_2)$ de la seria principal con $|\chi_1(x)| = |\chi_2(x)|$ para $x \in k^\times$. Decimos que π es *temperada* si π es esencialmente temperada y con carácter central unitario.

Comentario 2.20. Las representaciones temperadas son las que contribuyen a la formula de Plancherel en análisis armónico sobre el grupo (descomposición del espacio $L^2(GL(2,k))$ como integral directa de representaciones irreducibles). Las representaciones discretas con carácter central unitario son las que contribuyen discretamente a la formula de Plancherel (con medida puntual positiva).

2.4.5. Representaciones del grupo multiplicativo de un álgebra de división. Ahora $G = D^\times$ con D un álgebra cuaterniónica de división sobre k. Sea π una representación lisa irreducible de G. Exactamente como en el caso de $GL(2,k)$, el centro $Z_G \simeq k^\times$ actúa sobre π por un carácter ξ_π. Como el cociente G/Z_G es un grupo compacto, eso implica que π es necesariamente de dimensión *finita*.

2.5. Teoría local de representaciones, caso arquimediano. En este párrafo vamos a estudiar algunas representaciones irreducibles de los grupos $GL(2,\mathbb{R})$ y $\mathbb{H}^\times$. Comenzamos por el grupo $\mathbb{H}^\times$. El Lema de Schur es todavía válido, y como el cociente $\mathbb{H}^\times/\mathbb{R}^\times$ es compacto y se identifica con el grupo $SO(3)$ de rotaciones de $\mathbb{R}^3$, toda representación irreducible y continua de $\mathbb{H}^\times$ es de dimensión finita.

Proposición 2.21. *Por todo entero impar $t = 1, 3, 5, \ldots$, existe una única clase de equivalencia de representaciones irreducibles $\pi_t^{\mathbb{H}}$ de $\mathbb{H}^\times/\mathbb{R}^\times$ de dimension t.*

Demostración. Sea G el grupo recubridor universal de $\mathbb{H}^\times/\mathbb{R}^\times \simeq SO(3)$; entonces G es isomorfo al grupo $SU(2)$.

Las representaciones irreducibles de un grupo de Lie compacto G simplemente conexo son clasificadas por las representaciones irreducibles de su álgebra de Lie (complexificada) $\mathfrak{g}$. Cuando $G = SU(2)$, el álgebra de Lie $\mathfrak{g}$ es isomorfa al álgebra de Lie

$$\mathfrak{sl}(2) = \{X \in M(2,\mathbb{C}) \mid Tr(X) = 0\}.$$

Un teorema básico de la teoría de álgebras de Lie es que las representaciones irreducibles de $\mathfrak{sl}(2)$ son clasificadas por enteros positivos $1, 2, 3, \ldots$; la representación trivial es la única de dimension 1, la representación natural $\mathfrak{sl}(2) \to End(\mathbb{C}^2)$ es la única de dimension 2, y para cualquier entero $t \geq 2$, la representación $\mathfrak{sl}(2) \to End(Sym^{t-1}(\mathbb{C}^2))$ es de dimension t (es la representación natural sobre los polinomios de grado $t-1$ en dos variables).

Si ponemos $\mathbb{C} = Sym^0(\mathbb{C}^2)$, con la representación trivial, entonces el grupo $SU(2)$ actúa también sobre $Sym^{t-1}(\mathbb{C}^2)$ por cualquier $t > 0$. El centro C de $SU(2)$ es el grupo $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; la acción de C sobre $Sym^{t-1}(\mathbb{C}^2)$ es trivial si y solamente si t es impar. En consecuencia, las representaciones irreducibles de $\mathbb{H}^\times/\mathbb{R}^\times = SU(2)/C$ son las $Sym^{t-1}(\mathbb{C}^2)$ con t impar. □

La teoría de representaciones de $G = GL(2,\mathbb{R})$ es más complicada. En realidad, en la teoría de formas automorfas, es más natural hablar de representaciones del álgebra de Lie (complexificada) $\mathfrak{g} = M(2,\mathbb{C})$ que tienen una estructura de $(\mathfrak{g}, K)$-*módulo* en el sentido de Harish-Chandra. Sea $K \subset G$ un grupo compacto maximal; cuando $G = GL(2,\mathbb{R})$, ponemos $K = O(2)$, el grupo ortogonal del producto escalar euclidiano.

Definición 2.22. Un $(\mathfrak{g}, K)$-módulo es un espacio vectorial V (sobre $\mathbb{C}$) que admite una acción lineal π de $\mathfrak{g}$ y una acción continua ρ de K que son compatibles:

1. La acción de $\mathfrak{g}$ sobre V, restringida al álgebra de Lie de K, coincide con el diferencial de ρ;
2. Si $k \in K$, $X \in \mathfrak{g}$, entonces $\rho(k)\pi(X)\rho(k)^{-1} = \pi(ad(k)X)$.

De un $(\mathfrak{g}, K)$-módulo obtenemos automaticamente una representación del *álgebra universal encapsulante* de $\mathfrak{g}$. Sin embargo, si

$$\pi : G \to Aut(V)$$

es una representación continua sobre un espacio vectorial topológico razonable, se puede definir el subespacio $V^\infty \subset V$ de vectores diferenciables; entonces V^∞ es denso en V (teorema de Gårding) y admite una estructura canónica de $(\mathfrak{g}, K)$-módulo. Eso se aplica, por ejemplo, a las representaciones de la serie principal de $GL(2, \mathbb{R})$, que son construidas exactamente como en el caso no arquimediano.

Para las aplicaciones a las formas modulares holomorfas, necesitamos solo la clase de *representaciones holomorfas* de $GL(2, \mathbb{R})$, o más bien los $(\mathfrak{g}, K)$-módulos holomorfos. Nos interesan solo las representaciones con carácter central trivial (es decir, las representaciones de $PGL(2, \mathbb{R}) = GL(2, \mathbb{R})/\mathbb{R}^\times$). Como en el caso de $\mathbb{H}^\times/\mathbb{R}^\times$, la clasificación de $(\mathfrak{g}, K)$-módulos con carácter central trivial se reduce a la clasificación de módulos sobre $\mathfrak{sl}(2)$. Como grupo compacto maximal de $SL(2, \mathbb{R})$ tomamos el grupo $SO(2) = O(2) \cap SL(2, \mathbb{R})$.

Ejercicio 2.3. Determinar el normalizador de $SO(2)$ en $SL(2, \mathbb{R})$.

Proposición 2.23. *Sea $t \geq 0$ un entero. Existe un único $(\mathfrak{sl}(2), SO(2))$-módulo π'_t irreducible generado por un vector v_t caracterizado por las dos propriedades siguientes:*

(i) $X^- v_t = 0$, con $X^- = \begin{pmatrix} 1 & -i \\ -i & -1 \end{pmatrix}$;

(ii) v_t es un vector propio de $SO(2)$ con carácter

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} v_t = \alpha_{t+1}(a + ib)v_t,$$

donde $\alpha_t(e^{i\theta}) = e^{it\theta}$.

Ejercicio 2.4. Sea $v_t \in \pi'_t$ el vector de la proposición. Sea $X^+ = \begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix} \in \mathfrak{sl}(2)$. Demostrar que, para todo entero $a \geq 0$, el vector $(X^+)^a v_t$ es un vector propio de $SO(2)$, y calcular su valor propio.

Definición 2.24. Una representación irreducible π de $GL(2,\mathbb{R})$ (es decir, un $(\mathfrak{gl}(2), O(2))$-módulo)) es de la serie discreta si contiene el $(\mathfrak{sl}(2), SO(2))$-módulo π'_t con $t > 0$. La representación irreducible π es un límite de la serie discreta si contiene el $(\mathfrak{sl}(2), SO(2))$-módulo π'_0.

La proposición siguiente es una aplicación fácil de la teoría de representaciones inducidas:

Proposición 2.25. *Sea τ_1 y τ_2 dos representaciones irreducibles de $GL(2,\mathbb{R})$ que contienen la misma representación π'_t de $SL(2,\mathbb{R})$. Entonces τ_1 y τ_2 son equivalentes.*

Así tenemos el derecho de hablar de *la* representación irreducible π_t de $GL(2,\mathbb{R})$ que contiene π'_t.

Comentario 2.26. Sea $F = \mathbb{Q}$ y sea f una forma modular clásica de peso $k > 0$ para un subgrupo de $SL(2,\mathbb{Z})$ de índice finito. Sea π la representación automorfa de $GL(2,\mathbf{A})$ que corresponde a f. Entonces la componente π_∞ de π al primo arquimediano es isomorfa a la representación π_{k-1}.

Más generalmente, si f es una forma modular de Hilbert de peso $(2, 2, \ldots, 2)$, con representación automorfa asociada π, entonces la componente π_v en cualquier primo arquimediano es isomorfa a la representación π_1.

2.6. Correspondencia de Shimizu y de Jacquet-Langlands. Para describir la correspondencia de Jacquet-Langlands entre formas modulares (automorfas) de Hilbert y formas modulares (automorfas) sobre $D^\times(\mathbf{A})$, lo más sencillo es de comenzar con la *correspondencia local de Jacquet-Langlands JL* entre representaciones de los grupos locales $D_v^\times$ y de $GL(2,F_v)$. Con las definiciones ya introducidas eso se hace bastante rapidamente y muy conceptualmente. Sin embargo, las demostracíones de la correspondencia local son basadas sobre la correspondencia global.

2.6.1. Correspondencias locales. Sea v un primo de F. Ponemos $G = GL(2,F_v)$, $J = H_v^\times$, donde H_v es un álgebra cuaterniónica de división de dimensión 4 sobre F_v. Las representaciones irreducibles de J son todas de dimension finita. Designamos por $Rep(J)$ (respectivamente $Rep(G)$) el conjunto de (clases de equivalencia de) representaciones irreducibles de J (respectivamente G).

Teorema 2.27 (Correspondencia (local) de Jacquet-Langlands)**.** *Existe una biyección canónica*

$$JL : Rep(J) \simeq Rep_{disc}(G) \subset Rep(G)$$

entre el conjunto $Rep(J)$ de representaciones irreducibles de J y el conjunto $Rep_{disc}(G)$ de representaciones (irreducibles) discretas de G. Esa biyección conserva los factores locales de la ecuación funcional: si $\Pi \in Rep(J)$, y $\psi : F_v \to \mathbb{C}$ es un carácter aditivo no trivial, entonces

$$L(\Pi, s) = L(JL(\Pi), s)\varepsilon(\Pi, \psi, s) = \varepsilon(JL(\Pi), \psi, s)$$

donde $L(\Pi, s)$ y $\varepsilon(\Pi, \psi, s)$ son los factores locales de Godement-Jacquet introducidos en el Teorema 2.7.

Las representaciones no discretas de $GL(n, F_v)$, en particular las representaciones de la serie principal, no tienen correspondentes en $Rep(J)$.

Le demostración depende de la formula de trazas y necesita la introducción de la teoría de caracteres de representaciones de grupos reductivos sobre cuerpos locales. El carácter de una representación irreducible π de J es nada más que la traza habitual, que tiene un sentido porque π es de dimensión finita. En cambio, el carácterde una representación de dimensión infinita es una distribución y su existencia y propiedades hacen parte de la teoría de Harish-Chandra. Con las buenas definiciones, se puede caracterizar la correspondencia JL por un relación explicita de caracteres. Sin embargo, la conservación de factores locales es suficiente para caracterizar la correspondencia.

En general, la determinación explicita de la correspondencia local de Jacquet-Langlands es difícil, porque no hay una descripción elemental de las representaciones supercuspidales. En ciertos casos hay una descripción directa de la correspondencia. Nos limitamos a las representaciones con carácter central trivial.

Proposición 2.28. *Sea v un primo arquimediano. Entonces para todo $t > 0$, $JL(\pi_t^{\mathbb{H}}) = \pi_t$.*

Por supuesto, no se puede separar la demostración de esta proposición de la demostración de la correspondencia en general.

Proposición 2.29. *Sea v un primo no archimediano, y sea $\chi : F_v^\times \to \mathbb{C}^\times$ un carácter liso. Sea $\pi(\chi) = \chi \circ \nu : J \to \mathbb{C}^\times$ una representación de dimensión 1 de J. Entonces $JL(\pi(\chi)) = St(\chi)$.*

2.6.2. La correspondencia global. Ahora sea D un álgebra de división global sobre F. Sea S'_D el conjunto de primos de F (arquimedianos o no) de ramificación para D: D_v es un álgebra de división sobre F_v si y solamente si $v \in S'_D$. Entonces Σ'_D es el subconjunto de primos arquimedianos en S'_D. La cardinalidad $|S'_D|$ de S'_D es un número *par*; como hemos supuesto que D es un álgebra de división, $|S'_D| \geq 2$.

La correspondencia global de Jacquet-Langlands es una biyección del conjunto $Aut(D^\times)$ de representaciones automorfas de $D^\times$ y un subconjunto del conjunto $Aut(GL(2,F))$ de representaciones automorfas de $GL(2,F_{\mathbf{A}})$.

Teorema 2.30. *Sea π una representación automorfa de $D^\times(\mathbf{A})/F_{\mathbf{A}}^\times$. Sea $\Pi = JL(\pi)$ la representación admisible de $GL(2,F_{\mathbf{A}})$ definida como producto tensorial restringido $\otimes_v \Pi_v$, donde*

1. *Si $v \notin S'_D$, $D_v^\times \simeq GL(2,F_v)$ y Π_v es equivalente de π_v;*
2. *Si $v \in S'_D$, Π_v es equivalente de $JL(\pi_v)$.*

Entonces Π es una representación automorfa de $GL(2,F_{\mathbf{A}})$; además, Π esta contenida en el espacio de formas cuspidales.

El mapeo $\pi \mapsto JL(\pi)$ define una biyección entre $Aut(D^\times)$ y el subconjunto de $Aut(GL(2,F))$ de representaciones automorfas Π de $GL(2,F_{\mathbf{A}})$ que satisfacen la condición que Π_v esta en la serie discreta para todo $v \in S'_D$.

La demostración de este teorema por Jacquet y Langlands es basada sobre la fórmula de trazas. Se puede leer un bosquejo de la demostración en la sección 2.2 de [6]. Ese bosquejo presupone la existencia de la correspondencia local, pero en la práctica, las correspondencias local y global son demostradas simultaneamente.

2.7. Formas modulares de Hilbert de peso (2,2,...,2). El Teorema 2.30 tiene una interpretación más elemental en terminos de formas modulares holomorfas. Sea ${}_KS(D)$ la curva de Shimura asociada al álgebra de división D con $\Sigma_D = \{v\}$. Sea (ρ, W_ρ) una representación irreducible de $\tilde{K}_\infty$ trivial en el centro de $D_\infty^\times$. Si $w \neq v$, designamos por t_w la dimensión de W_{ρ_w}, donde $\rho_w : D_w^\times/F_w^\times = \mathbb{H}^\times/\mathbb{R}^\times \to GL(W_{\rho_w})$ es la componente local de ρ en w. Sea ρ_v el carácter α^{-t_v} de $SO(2) \subset \tilde{K}_v$.

Si u es un primo no arquimediano, $u \notin S'_D$, entonces $D_u^\times \xrightarrow{\sim} GL(2,F_u)$. Así podemos identificar las álgebras de Hecke esféricas de $D_u^\times$ y de $GL(2,F_u)$, relativamente a sus subgrupos compactos maximales respectivos.

Corolario 2.31. *Sea S un conjunto finito de primos no arquimedianos que contiene todos los primos no arquimedianos en S'_D. Sea $K_f \subset D^\times(\mathbf{A}_f)$ un subgrupo compacto abierto que contiene $GL(2,\mathcal{O}_u)$ para todo primo no arquimediano $u \notin S$. Sea $f : \mathfrak{H}^\pm \times D^\times(\mathbf{A}_f)/K_f \to W$ una forma modular clásica que es autoforma para los operadores de Hecke en los primos fuera de S. Entonces existe una forma modular de Hilbert f^{Hilb} de peso t_v en v y de peso $t_w + 1$ en el primo arquimediano $w \neq v$,*

que es autoforma para los operadores de Hecke en los primos fuera de S con los mismos valores propios que f.

Para aplicaciones a las curvas elípticas, nos bastará enfocar nuestra atención en las formas modulares sobre curvas de Shimura que corresponden a las formas modulares de Hilbert de peso (2,2,...,2), es decir, con $t_v = 2$ y con $t_w = 0$ para todo $w \neq v$.

2.7.1. Formas nuevas. La teoría de *formas nuevas*, introducida por Atkin y Lehner y generalizada por Miyake y otros, permite de definir un espacio natural de dimensión uno en una representación automorfa de $GL(2, F_{\mathbf{A}})$. Esta teoría se generaliza fácilmente al caso de $D^\times(\mathbf{A})$ si nos limitamos a las representaciones automorfas associadas a formas de peso (2,2,...,2) cuyas componentes locales en los primos en S'_D son de dimensión uno.

Introducimos los más importantes grupos de nivel.

$$K(D) = \prod_{v \notin S'_D} GL(2, \mathcal{O}_v) \times \prod_{v \in S'_D} \mathcal{O}_{D_v}^\times \subset D^\times(\mathbf{A}_f) \tag{2.32}$$

(producto sobre primos no arquimedianos) es un grupo de nivel maximal. Sea $\mathfrak{n} \subset \mathcal{O}_F$ un ideal relativamente primo al conjunto S'_D, y definimos

(2.33)

$$K_0(\mathfrak{n}, D) = \{k = (k_v) \in K(D) \mid k_v \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{\mathfrak{n}}\ \forall v \notin S'_D\};$$

(2.34)

$$K_1(\mathfrak{n}, D) = \{k = (k_v) \in K(D) \mid k_v \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{n}}\ \forall v \notin S'_D\}.$$

Teorema 2.35. *Sea S un conjunto finito de primos no arquimedianos que contiene todos los primos no arquimedianos en S'_D. Sea $K_f \subset D^\times(\mathbf{A}_f)$ un subgrupo compacto abierto que contiene $GL(2, \mathcal{O}_u)$ para todo primo no arquimediano $u \notin S$. Sea $f : \mathfrak{H}^\pm \times D^\times(\mathbf{A}_f)/K_f \to W$ una forma modular clásica de peso (2,2,...,2) que es autoforma para los operadores de Hecke en los primos fuera de S. Sea Π la representación automorfa de $GL(2, F_{\mathbf{A}})$, associada a la forma modular clásica f. Suponemos que, en todo primo no arquimediano $v \in S$, la componente Π_v de Π es de dimensión uno.*

Entonces existe un ideal $\mathfrak{n} \subset \mathcal{O}_F$ relativamente primo al conjunto S'_D, el conductor *de Π (fuera de S'_D) tal que*

1. $\dim \Pi^{K_1(\mathfrak{n}, D)} = 1$;
2. *Si $\mathfrak{n}' \neq \mathfrak{n}$ es un ideal de $\mathcal{O}_F$, $\mathfrak{n}' \supset \mathfrak{n}$, entonces $\Pi^{K_1(\mathfrak{n}', D)} = \{0\}$.*

Cuando Π es una representación automorfa de $D^\times(\mathbf{A})$ como en el Teorema 2.7.1 con conductor $\mathfrak{n}$ (fuera de S'_D), llamemos los elementos de $\Pi^{K_1(\mathfrak{n},D)}$ *vectores nuevos*. Las formas modulares clásicas que corresponden a los vectores nuevos en Π se llaman *formas nuevas* (de nivel $K_1(\mathfrak{n},D)$). Una forma nueva de nivel $K_1(\mathfrak{n},D)$ que es invariante para la acción del grupo conmutativo $K_0(\mathfrak{n},D)/K_1(\mathfrak{n},D)$ se llama una *forma nueva* de nivel $K_0(\mathfrak{n},D)$. Sea

$$M_\rho(D^\times, K_1(\mathfrak{n},D))^{nuevo} \subset M_\rho(D^\times, K_1(\mathfrak{n},D))$$

(respectivamente

$$\mathcal{A}^{hol}(D^\times, K_1(\mathfrak{n},D),\rho)^{nuevo} \subset \mathcal{A}^{hol}(D^\times, K_1(\mathfrak{n},D),\rho))$$

los subespacios de formas nuevas (respectivamente de vectores nuevos), y definimos $M_\rho(D^\times, K_0(\mathfrak{n},D))^{nuevo}$ y $\mathcal{A}^{hol}(D^\times, K_0(\mathfrak{n},D),\rho)^{nuevo}$ de la misma manera. La principal propiedad del espacio de formas nuevas es expresado por el siguiente teorema (teorema de multiplicidad uno).

Teorema 2.36. *Sea $K = K_0(\mathfrak{n},D)$ o $K_1(\mathfrak{n},D)$. El espacio de formas nuevas de nivel K es un módulo semisimple sobre las álgebras de Hecke*

$$\mathbb{T}(K) \subset End(M_\rho(D^\times,K)), \mathbb{T}^{nuevo}(K) \subset End(M_\rho(D^\times,K)^{nuevo})$$

generada por los operadores T^{class} con $T \in \mathcal{H}(K_v)$, v relativamente primo al conjunto S'_D y al ideal $\mathfrak{n}$.

Además, si $\lambda : \mathbb{T}(K) \to \mathbb{C}$ es un carácter entonces el subespacio $M_\rho(D^\times,K)^{nuevo}[\lambda]$ de vectores propios de $\mathbb{T}(K)$ para el carácter λ es de dimensión ≤ 1. Si $\dim M_\rho(D^\times,K)^{nuevo}[\lambda] = 1$ entonces el carácter λ aparece con multiplicidad 1 en $M_\rho(D^\times,K)$ (es decir, la multiplicidad en el subespacio ortogonal al subespacio de formas nuevas, para el producto escalar de Petersson, es igual a 0).

El subespacio de $M_\rho(D^\times,K)$ ortogonal al subespacio $M_\rho(D^\times,K)^{nuevo}$ se llama el subespacio de *formas viejas*:

$$M_\rho(D^\times,K) = M_\rho(D^\times,K)^{nuevo} \oplus M_\rho(D^\times,K)^{viejo}. \tag{2.37}$$

En el caso de formas de peso (2,2,...,2), identificamos $M_{(2,2,\dots,2)}(D^\times,K) = \Omega^1({}_KS(D))$; entonces (2.37) se escribe

$$\Omega^1({}_KS(D)) = \Omega^1({}_KS(D))^{nuevo} \oplus \Omega^1({}_KS(D))^{viejo}. \tag{2.38}$$

Definimos $\mathbb{T}(K)_\mathbb{Q} \subset \mathbb{T}(K)$ como la $\mathbb{Q}$-subálgebra de $\mathbb{T}(K)$ generada sobre $\mathbb{Q}$ por los operadores T^{class} con $T \in \mathcal{H}(K_v)_\mathbb{Z}$.

Proposición 2.39. *La descomposición* (2.38) *está definida sobre $\mathbb{Q}$. Más precisamente,*

1. *Los caracteres de* $\mathbb{T}(K)$ *son todos definidos sobre la clausura algebraica* $\overline{\mathbb{Q}}$ *de* $\mathbb{Q}$*, y si* $\lambda : \mathbb{T}(K)_{\mathbb{Q}} \to \overline{\mathbb{Q}}$ *es un carácter no trivial. entonces, para* $\tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$*,* $\tau \circ \lambda$ *es también un carácter de* $\mathbb{T}(K)_{\mathbb{Q}}$*:*

$$M_\rho(D^\times, K)[\lambda] \neq 0 \Rightarrow M_\rho(D^\times, K)[\tau \circ \lambda] \neq 0, \ \forall \tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q}).$$

2. *Si* $\dim M_\rho(D^\times, K)^{nuevo}[\lambda] = 1$ *entonces,*

$$\forall \tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q}), M_\rho(D^\times, K)^{viejo}[\tau \circ \lambda] = 0.$$

Demostración. La primera parte de la proposición es un caso particular de un teorema de Shimura sobre la racionalidad de formas modulares. Ahora, si λ' es un carácter de $\mathbb{T}(K)$ tal que $M_\rho(D^\times, K)^{viejo}[\lambda'] \neq 0$, entonces hay un ideal $\mathfrak{n}' \supsetneq \mathfrak{n}$ con $M_\rho(D^\times, K_1(\mathfrak{n}', D))[\lambda'] \neq 0$. La segunda parte se obtiene aplicando la primera parte a los subespacios $M_\rho(D^\times, K_1(\mathfrak{n}', D))$ de $M_\rho(D^\times, K_1(\mathfrak{n}, D))$ con $\mathfrak{n}' \supsetneq \mathfrak{n}$. □

Ejercicio 2.5. Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_F$. Suponemos que

$$D_{\mathfrak{p}}^\times \xrightarrow{\sim} GL(2, F_{\mathfrak{p}}).$$

Sea $a \geq 1$ un entero y sea $\mathfrak{n} = \mathfrak{p}^a$. Sea $\varpi \in \mathcal{O}_{\mathfrak{p}}$ un uniformizador en $F_{\mathfrak{p}}$ y sea $\gamma_b = \begin{pmatrix} \varpi^b & 0 \\ 0 & 1 \end{pmatrix}$, $b = 1, \ldots, a$. Sea $\mathfrak{m}$ un ideal de $\mathcal{O}_F$ relativamente primo a $\mathfrak{p}$. Demostrar que la traslación por $\gamma_b^{-1} \in D_{\mathfrak{p}}^\times \xrightarrow{\sim} GL(2, F_{\mathfrak{p}})$:

$$U_b(f)(g) = f(g\gamma_b^{-1})$$

define un mapeo inyectivo

$$U_b : M_\rho(D^\times, K_0(\mathfrak{m} \cdot \mathfrak{p}^{a-b}, D)) \to M_\rho(D^\times, K_0(\mathfrak{m} \cdot \mathfrak{p}^a, D)).$$

El espacio de formas viejas es la suma de las imágenes de los U_b.

Ejercicio 2.6. Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_F$. Suponemos que

$$D_{\mathfrak{p}}^\times \xrightarrow{\sim} GL(2, F_{\mathfrak{p}}).$$

Sea $w_{\mathfrak{p}} = \begin{pmatrix} 0 & 1 \\ \varpi & 1 \end{pmatrix}$. Sea $\mathfrak{m}$ como en el Ejercicio 2.5. Demostrar que la traslación por $w_{\mathfrak{p}}$ (definida como en el Ejercicio 2.5) define una involución de $M_\rho(D^\times, K_0(\mathfrak{m} \cdot \mathfrak{p}, D))$.

3. Formas modulares cuaterniónicas y curvas elípticas

3.1. Curvas elípticas sobre un cuerpo totalmente real. Una *curva elíptica* E sobre un cuerpo F es una curva no singular proyectiva de género 1 definida por ecuaciones con coefficientes en F, con un punto racional ∞ sobre F. Toda curva elíptica E es isomorfa a una

curva plana definida por una ecuacion cúbica en tres variables, o en forma inhomogénea de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in F, i = 1, 2, 3, 4, 6.$$

Decir que una curva elíptica esta definida sobre F es equivalente de decir que su invariante j pertenece a F.

Como E es de género 1, su jacobiano $J(E)$ es de dimensión 1, y la aplicación

$$E \to J(E), x \mapsto (x - \infty)$$

es un isomorfismo. En particular, los puntos de E sobre cualquier cuerpo forman un grupo conmutativo, y designamos por 0 su elemento neutro. El teorema siguiente[2] es fundamental:

Teorema 3.1. *Sea $\bar{F}$ una clausura algebraica de F. Si $n \in \mathbb{N}$ es coprimo con la característica de F, el grupo $E[N] = \{x \in X(\bar{F}), nx = 0\}$ es isomorfo a $(\mathbb{Z}/N\mathbb{Z})^2$.*

El grupo de Galois $Gal(\bar{F}/F)$ actúa sobre $E[N]$ y si fijamos una base obtenemos una representación

$$Gal(\bar{F}/F) \to GL(2, \mathbb{Z}/N\mathbb{Z}).$$

Sea p un número primo invertible en F, y definimos el *módulo de Tate*

$$T_p(E) = \varprojlim_n E[p^n]$$

donde el mapeo $E[p^n] \to E[p^{n-1}]$ es multiplicación por p. Entonces $T_p(E) \xrightarrow{\sim} \mathbb{Z}_p^2$, y la acción de $Gal(\bar{F}/F)$ sobre $T_p(E)$ es una representación continua

$$\rho_{E,p} : Gal(\bar{F}/F) \to GL(2, \mathbb{Z}_p).$$

Ahora suponemos que F es un cuerpo de números totalmente real. Entonces es un teorema de Serre (en el caso $F = \mathbb{Q}$) y otros que la representación $\rho_{E,p}$ es absolutamente irreducible. Sea v un primo de F no arquimediano de característica residual distinta de p. Existe un conjunto finito $S = S(E)$ de primos de F tal que la curva E tiene buena reducción en el cuerpo residual $k(v)$ de v para $v \notin S$. Sea $v \notin S$, $q_v = |k(v)|$. Entonces $E \pmod v$ es una curva elíptica sobre el cuerpo finito $k(v)$, y el grupo $E(k(v))$ es un grupo finito. Sea $N_v(E) = |E(k(v))|$, y escribimos

$$N_v(E) = 1 + q_v - a_v(E).$$

Entonces el número $a_v(E) \in \mathbb{Z}$ determina la restricción ρ_v de la representación $\rho_{E,p}$ a un grupo de descomposición $\Gamma_v \subset Gal(\bar{F}/F)$. De

[2]Ver, por ejemplo, J. Silverman, *The Arithmetic of Elliptic Curves*, Corollary 6.4.

hecho, esa restricción es no ramificado, porque E tiene buena reducción, y ρ_v es determinado por la traza del Frobenius $\rho_{E,p}(Frob_v)$; y

$$Tr(\rho_{E,p}(Frob_v)) = a_v(E).$$

Como el teorema de densidad de Chebotarev implica que la unión de las clases de conjugación de los $\rho_{E,p}(Frob_v)$, con $v \notin S$, es densa en la imagen de $\rho_{E,p}$, y como $\rho_{E,p}$ es absolutamente irreducible, su clase de isomorfismo esta completamente determinada por los números $N_v(E)$ con $v \notin S$.

Si E y E' son dos curvas elípticas isógenas sobre F, entonces $S(E) = S(E')$ y $N_v(E) = N_v(E')$ para todo $v \notin S$. En consecuencia, tenemos la primera parte del teorema siguiente:

Teorema 3.2. *(a) Si E y E' son dos curvas elípticas isógenas sobre F, entonces $\rho_{E,p}$ y $\rho_{E',p}$ son equivalentes para todo p.*

(b) [Faltings] Si E y E' son dos curvas elípticas sobre F, y si $\rho_{E,p}$ y $\rho_{E',p}$ son equivalentes como representaciones de $Gal(\bar{F}/F)$ para un número primo p, entonces E y E' son isógenas.

Comentario 3.3. En particular, el teorema de Faltings implica que, si $\rho_{E,p}$ y $\rho_{E',p}$ son equivalentes como representaciones de $Gal(\bar{F}/F)$ para un número primo p, entonces $\rho_{E,q}$ y $\rho_{E',q}$ son equivalentes para todo primo q. Pero este es un resultado mucho más elemental que el teorema de Faltings. Lo mencionamos aquí porque es importante en la demostración de la automorfía de curvas elípticas sobre cuerpos reales cuadráticos.

3.1.1. La función L de una curva elíptica.

3.2. El jacobiano de una curva de Shimura. Si $X = \coprod X_i$ es una curva proyectiva lisa con componentes conexas X_i, definimos $Jac(X) = \prod_i Jac(X_i)$. Sea $K = K_f \subset D^\times(\mathbf{A}_f)$ y X la curva de Shimura ${}_KS(D)$, considerada como superficie de Riemann. El jacobiano se construye del siguiente modo. La cohomologia $H^1({}_KS(D), \mathbb{C})$ admite una descomposicion de Hodge

$$H^1({}_KS(D), \mathbb{C}) = \Omega^1({}_KS(D)) \oplus \bar{\Omega}^1({}_KS(D)) \tag{3.4}$$

en suma directa de espacios de diferenciales holomorfas y anti-holomorfas. Por otro lado, como hay el isomorfismo de Proposition 1.10, podemos identificar

$$H^1({}_KS(D), \mathbb{C}) \xrightarrow{\sim} M_{(2,2,\dots,2)}(D^\times, K) \oplus \bar{M}_2(D^\times, K) \tag{3.5}$$

Por dualidad, la descomposición (3.4) corresponde a una descomposición de la homologia:

$$H_1({}_KS(D), \mathbb{C}) = \Omega^1({}_KS(D))^\perp \oplus \bar{\Omega}^1({}_KS(D))^\perp \tag{3.6}$$

El teorema siguiente es válido para toda curva lisa proyectiva compleja:

Teorema 3.7. *Hay isomorfismos naturales (funtoriales) de grupos*

$$H_1({}_KS(D),\mathbb{Z})\backslash Hom_{\mathbb{C}}(\Omega^1({}_KS(D),\mathbb{C})) \xrightarrow{\sim}$$
$$H_1({}_KS(D),\mathbb{Z})\backslash H_1({}_KS(D),\mathbb{C})/\Omega^1({}_KS(D))^{\perp} \xrightarrow{\sim} Jac({}_KS(D)).$$

Comentario 3.8. Si X es una curva proyectiva y lisa compleja, la inclusión $H_1(X,\mathbb{R}) \hookrightarrow H_1(X,\mathbb{C})$ define un isomorfismo

$$H_1(X,\mathbb{R}) \xrightarrow{\sim} H_1(X,\mathbb{C})/\Omega^1(X)^{\perp}$$

de espacios vectoriales reales. Así podemos escribir

$$Jac(X) \xrightarrow{\sim} H_1(X,\mathbb{Z})\backslash H_1(X,\mathbb{C})/\Omega^1(X)^{\perp} \xrightarrow{\sim} H_1(X,\mathbb{R})/H_1(X,\mathbb{Z})).$$

3.3. El álgebra de Hecke como álgebra de endomorfismos del jacobiano. Sean X y Y dos curvas proyectivas lisas conexas sobre el cuerpo k. Una *correspondencia* entre X y Y es una subvariedad cerrada $C \subset X \times Y$ (no necesariamente conexa) tal que las dos proyecciones $p_1 : C \to X$ y $p_2 : C \to Y$ son morfismos finitos. Sean n_1 y n_2 los grados de los morfisms finitos p_1 y p_2. Una correspondencia define un homomorfismo

$$[C] : Jac(X) \to Jac(Y)$$

del siguiente modo. Si $x \in X$, la fibra $C_x = p_1^{-1}(x) = \sum a_i c_i(x)$ es un divisor efectivo en C de grado $n_1 = \sum a_i$; aqui $a_i \in \mathbb{N}$ y $c_i(x) \in C_x$. Entonces $[C](x) = \sum a_i p_2(c_i(x)) \in Jac(Y)$. Si C es una curva lisa (eso será el caso en nuestros ejemplos), la definición es mas sencilla. Por funtorialidad del jacobiano tenemos morfismos $p_{1,*} : Jac(C) \to Jac(X)$ y $p_{2,*} : Jac(C) \to Jac(Y)$. Por dualidad (autodualidad del jacobiano), tenemos también un morfismo

$$p_1^* : Jac(X) = \widehat{Jac(X)} \to \widehat{Jac(C)} = Jac(C)$$

, y $[C] = p_{2,*} \circ p_1^*$.

Si $K \subset \mathbb{C}$ es un subcuerpo de $\mathbb{C}$, y si C es una curva lisa, tenemos también morfismos de homología

$$p_1^* : H_1(X,\mathbb{Z}) \to H_1(C,\mathbb{Z}); p_{2,*} : H_1(C,\mathbb{Z}) \to H_1(Y,\mathbb{Z})$$

y los morfismos análogos para homología con coefficientes reales. El primero homomorfismo es definido por dualidad de Poincaré. El homomorfismo $[C]$ se define explicitamente por

$$p_{2,*} \circ p_1^* : Jac(X) = H_1(X,\mathbb{R})/H_1(X,\mathbb{Z}) \to$$
$$H_1(C,\mathbb{R})/H_1(C,\mathbb{Z}) \to H_1(Y,\mathbb{R})/H_1(Y,\mathbb{Z}) = Jac(Y).$$

La definición de una correspondencia queda válida con modificaciones naturales cuando X y Y son curvas lisas y proyectivas pero no necesariamente conexas. Ahora sea $K = \prod_v K_v \subset D^\times(\mathbf{A}_f)$ y consideremos el caso cuando $X = Y$ es la curva de Shimura ${}_KS(D)$ (no necesariamente conexa) de nivel K. Esta curva es proyectiva y lisa si K es un subgrupo bastante pequeño, lo que vamos a suponer. Sea v un primo no ramificado para D y con $K_v = GL(2, \mathcal{O}_v)$ (decimos que v es *relativamente primo al nivel de* K). Sea

$$I_v = \{k = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K_v \mid c \in \varpi_v \mathcal{O}_v\}$$

con ϖ_v un uniformizador de F_v. Sea $K_0(v) = \prod_{w \neq v} K_w \times I_v$ (hemos reemplazado K_v por I_v). La inclusión $\iota_v : K_0(v) \hookrightarrow K_v$ define un morfismo natural $p_1 : {}_{K_0(v)}S(D) \to {}_KS(D)$. Pero hay una segunda inclusión $\iota'_v : K_0(v) \hookrightarrow K_v$, definida por

$$\iota'_v(k) = n_v k n_v^{-1}, \text{ con } n_v = \begin{pmatrix} 0 & \varpi^{-1} \\ 1 & 0 \end{pmatrix} \in D_v^\times$$

La inclusión ι'_v define un segundo morfismo $p_2 : {}_{K_0(v)}S(D) \to {}_KS(D)$. La imagen del morfismo

$$(p_1, p_2) : {}_{K_0(v)}S(D) \to {}_KS(D) \times {}_KS(D)$$

es una correspondencia $T(v)$.

Escribimos $Jac_K(D) = Jac({}_KS(D))$. El homomorfismo $[T(v)] = p_{2,*} \circ p_1^* : Jac_K(D) \to Jac_K(D)$ es una *correspondencia de Hecke*. Por otro lado, hemos visto que $Jac_K(D)$ es isomorfo al grupo

$$H_1({}_KS(D), \mathbb{Z}) \backslash Hom_{\mathbb{C}}(\Omega^1({}_KS(D), \mathbb{C})$$

que es cociente de $Hom_{\mathbb{C}}(M_{(2,2,\ldots,2)}(D^\times, K), \mathbb{C})$. La proposición siguiente se demostra por un cálculo explícito elemental.

Proposición 3.9. *Sea v un primo no arquimediano que es relativamente primo al nivel de K. La correspondencia de Hecke $[T(v)] \in End(Jac_K(D))$ es inducida por el operador de Hecke T_v actuando en $M_{(2,2,\ldots,2)}(D^\times, K)$ vía la suryección*

$$Hom_{\mathbb{C}}(M_{(2,2,\ldots,2)}(D^\times, K), \mathbb{C}) \to Jac_K(D).$$

Además, hay una correspondencia $R(v) \subset {}_KS(D) \times {}_KS(D)$ tal que $[R(v)] \in End(Jac_K(D))$ es inducida por la acción del operador de Hecke R_v sobre $M_{(2,2,\ldots,2)}(D^\times, K)$.

Corolario 3.10. *La subalgebra $\mathbb{T}_K \subset End(Jac_K(D)) \otimes \mathbb{Q}$ generada por las correspondencias $[T(v)]$ y $[R(v)]$, para todos los primos v que son primos al nivel de K, es conmutativa.*

3.3.1. El módulo de Tate y la cohomología étale de ${}_KS(D)$. Recordamos un teorema fundamental de Shimura:

Teorema 3.11 (Shimura)**.** *Sea $\sigma : F \hookrightarrow \mathbb{R}$ el único primo (real) en Σ_D. El conjunto de curvas de Shimura ${}_KS(D)$, con $K \subset D^\times(\mathbf{A}_f)$ abierto compacto, tiene un modelo canónico ${}_KS(D)_\sigma$ sobre el cuerpo $\sigma(F)$. Más precisamente, para todo K hay un isomorfismo canónico*

$$ {}_KS(D) \xrightarrow{\sim} {}_KS(D)_\sigma \times_{F,\sigma} \mathbb{C}$$

y una acción del grupo $D^\times(\mathbf{A}_f)$ sobre el conjunto de ${}_KS(D)_\sigma$ que conserva estos isomorfismos.

En consecuencia, el sistema de jacobianos $Jac_K(D)$ tiene también un modelo canónico sobre σ_F (que identificamos con F), y podemos definir el módulo de Tate p-adico $T_p(Jac_K(D)) = \varprojlim_n Jac_K(D)[p^n]$ como representación del grupo de Galois $Gal(\bar{F}/F)$. Por otra lado, hay isomorfismos canónicos entre cohomologia p-adica étale y espacios duales de módulos de Tate:

$$H^1({}_KS(D), \mathbb{Q}_p) \xrightarrow{\sim} Hom(T_p(Jac_K(D)), \mathbb{Q}_p) \tag{3.12}$$

como representaciones de $Gal(\bar{F}/F)$. Además, los isomorfismos (3.12) son isomorfismos de módulos sobre el álgebra de Hecke $\mathbb{T}_K$.

Para simplificar la notación, fijamos $\Sigma_D = \{\sigma\}$ y escribimos

$$X(D) = {}_{K(D)}S(D)_\sigma;\ X_0(\mathfrak{n}, D) = {}_{K_0(\mathfrak{n},D)}S(D)_\sigma; X_1(\mathfrak{n}, D) = {}_{K_1(\mathfrak{n},D)}S(D)_\sigma;$$

y definimos los jacobianos $Jac(D) = Jac(X(D))$, $Jac_0(\mathfrak{n}, D)$, y $Jac_1(\mathfrak{n}, D)$ y las álgebras de Hecke $\mathbb{T}(D)$, $\mathbb{T}_0(\mathfrak{n}, D)$, y $\mathbb{T}_1(\mathfrak{n}, D)$ del modo evidente.

Comentario 3.13. En general, si una de las curvas $X(D)$, $X_0(\mathfrak{n}, D)$, y $X_1(\mathfrak{n}, D)$ es singular, la reemplazamos por su modelo liso para definir su jacobiano. Eso no cambia nada de esencial.

Ya hemos visto en la sección 2.7.1 que la teoría de *formas nuevas* es válida para curvas de Shimura $X_1(\mathfrak{n}, D)$ y $X_0(\mathfrak{n}, D)$. Como por un lado tenemos

$$H^1(X_i(\mathfrak{n}, D), \mathbb{Q}_p) \xrightarrow{\sim} H^1(X_i(\mathfrak{n}, D), \mathbb{Q}) \otimes \mathbb{Q}_p, i = 0, 1;$$

$$H^1(X_i(\mathfrak{n}, D), \mathbb{C}) \xrightarrow{\sim} H^1(X_i(\mathfrak{n}, D), \mathbb{Q}) \otimes \mathbb{C}, i = 0, 1$$

y como por otro lado tenemos la descomposición de cada uno de los dos factores del miembro derecho de (3.4) en formas nuevas y formas viejos, siguiendo (2.38), eso implica que el miembro izquierdo de (3.12) admite una descomposición análoga al (2.38):

(3.14)

$$H^1(X_i(\mathfrak{n}, D), \mathbb{Q}_p) = H^1(X_i(\mathfrak{n}, D), \mathbb{Q}_p)^{nuevo} \oplus H^1(X_i(\mathfrak{n}, D), \mathbb{Q}_p)^{viejo}\ i = 0, 1.$$

Por dualidad, (3.14) y (3.12) implican una descomposición del módulo de Tate de $Jac_i(\mathfrak{n}, D)$:

(3.15)
$$\begin{aligned} &T_p(Jac_i(\mathfrak{n}, D)) \otimes \mathbb{Q}_p \\ =&[T_p(Jac_i(\mathfrak{n}, D)) \otimes \mathbb{Q}_p]^{nuevo} \oplus [T_p(Jac_i(\mathfrak{n}, D)) \otimes \mathbb{Q}_p]^{viejo},\ i = 0, 1. \end{aligned}$$

Es una consecuencia de la Proposición 2.39 que la descomposición (3.15) proviene de una descomposición de la homología

(3.16)
$$\begin{aligned} &H_1(Jac_i(\mathfrak{n}, D), \mathbb{Q}) = H_1(X_i(\mathfrak{n}, D), \mathbb{Q}) \\ =&H_1(Jac_i(\mathfrak{n}, D), \mathbb{Q})^{nuevo} \oplus H_1(Jac_i(\mathfrak{n}, D), \mathbb{Q})^{viejo}. \end{aligned}$$

Definimos el *cociente nuevo* $Jac_i(\mathfrak{n}, D)^{nuevo}$ de $Jac_i(\mathfrak{n}, D)$, $i = 0, 1$, como la variedad abeliana cociente maximal $p : Jac_i(\mathfrak{n}, D) \to A$, con la propiedad que el núcleo del mapeo $p_* : H_1(Jac_i(\mathfrak{n}, D), \mathbb{Q}) \to H_1(A, \mathbb{Q})$ sea igual a $H_1(Jac_i(\mathfrak{n}, D), \mathbb{Q})^{viejo}$.

Proposición 3.17. *1. La inclusión* $\mathbb{T}_i(\mathfrak{n}, D) \hookrightarrow End(Jac_i(\mathfrak{n}, D)) \otimes \mathbb{Q}$ *induce un homomorfismo*

$$\mathbb{T}_i(\mathfrak{n}, D) \to End(Jac_i(\mathfrak{n}, D)^{nuevo}) \otimes \mathbb{Q},\ i = 0, 1.$$

2. La homología $H_1(Jac_i(\mathfrak{n}, D)^{nuevo}, \mathbb{Q})$ *es un* $\mathbb{T}_i(\mathfrak{n}, D)$*-módulo semisimple.*

3. Sean A *y* B *dos variedades abelianas de dimension* ≥ 1*, y sean*

$$p : Jac_i(\mathfrak{n}, D)^{nuevo} \to A; q : Jac_i(\mathfrak{n}, D)^{nuevo} \to B$$

homomorfismos de variedades abelianas. Suponemos que los núcleos de p *y* q *son conexos. Si* A *y* B *son isomorfas, entonces* $\ker p = \ker q$*.*

Demostración. Es una consecuencia inmediata de la Proposición 2.39. □

3.4. Curvas elípticas como cocientes de una curva de Shimura. Sea E una curva elíptica sobre el cuerpo totalmente real F. Es un celebrado teorema de Breuil, Conrad, Diamond, y Taylor [1], basado sobre los métodos introducidos por Andrew Wiles, que si $F = \mathbb{Q}$, E es isomorfa a un cociente del jacobiano de la curva modular clásica $X_0(N)$ donde N es igual al conductor de E. (El caso de curvas elípticas semi-estables había sido demostrado un poco antes por Wiles y Taylor-Wiles, y había permitido a Wiles de demostrar el Última Teorema de Fermat.)

Un teorema análogo, válido para cualquier cuerpo real cuadático F – $[F : \mathbb{Q}] = 2$ – ha sido demostrado muy recientemente por Freitas,

Le Hung, y Siksek [4]. Pero el enunciado del teorema es un poco diferente en el caso general. En el siguiente teorema consideramos F como subcuerpo del cuerpo $\mathbb{R} \subset \mathbb{C}$ por uno de las inyecciones $\sigma : F \hookrightarrow \mathbb{R}$.

Teorema 3.18 (Freitas, Le Hung, y Siksek)**.** *Sea E una curva elíptica sobre el cuerpo real cuadático F. Entonces E es modular: existe una forma modular de Hilbert f de peso $(2, 2)$, que es vector propio para los operadores de Hecke de nivel relativamente primo al nivel K, tal que hay una identidad de funciones L:*

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

Si además existe un primo no arquimediano v donde E tiene una reducción multiplicativa o supercuspidal [ver más abajo], entonces E es isomorfa a un cociente del jacobiano de una curva de Shimura de la forma $X_0(\mathfrak{n}, D)$, donde D es un álgebra de cuaterniones sobre F con $|\Sigma_D| = 1$.

En particular, la condición "E es modular"no implica necesariamente que E es isomorfa a un cociente del jacobiano de una curva de Shimura si $d = [F : \mathbb{Q}]$ es par. Existen ejemplos de curvas elípticas sobre cuerpos reales cuadráticos con buena reducción en todos los primos no arquimedianos; una tal curva no puede ser cociente del jacobiano de una curva de Shimura.

Tenemos que explicar el significado de "reducción multiplicativa o supercuspidal." Esas nociones tienen significados puramente geométricos, pero para nosotros es más fácil explicarlas en terminos del sistema de representaciones $\{\rho_{E,p}\}$ de $Gal(\overline{\mathbb{Q}}/F)$. Sea v un primo no arquimediano de F, y sea $\Gamma_v \subset Gal(\overline{\mathbb{Q}}/F)$ un grupo de descomposición del primo v – es el estabilizador de una extensión $\bar{v}$ de la valuación sobre F asociada al primo v a la extensión $\overline{\mathbb{Q}}$. Fijamos un primo racional p y sea $\rho_{p,E,v}$ la restricción de $\rho_{E,p}$ al subgrupo Γ_v de $Gal(\overline{\mathbb{Q}}/F)$. La clase de isomorfismo de $\rho_{p,E,v}$ no depende de la elección de la extensión $\bar{v}$ de v. Para un v fijo podemos siempre suponer que v no divide p. Si $\rho_{p,E,v}$ es una representación irreducible, entonces el Teorema 2.18 implica la existencia de una representación supercuspidal $\pi_v(E) = \pi(\rho_{p,E,v})$, irreducible y lisa, de $GL(2, F_v)$. En este caso decimos que E *tiene una reducción supercuspidal*.

Más generalmente, el Teorema 2.18 es la parte dificil de la *correspondencia local de Langlands para $GL(2)$* (sobre un cuerpo no arquimediano). Sea L un cuerpo p-adico, con v relativamente primo a p, y sea $\rho : \Gamma_v \to GL(2, L)$ una representación continua. La correspondencia local de Langlands da una representación $\pi(\rho)$, irreducible y lisa, de $GL(2, F_v)$. Si ρ es irreducible, es la representación del Teorema 2.18.

Si ρ es reducible, tenemos que distinguir entre dos casos. Sea $I_v \subset \Gamma_v$ el subgrupo de inercia.

1. Si ρ es reducible y la imagen de la restricción de ρ al subgrupo I_v es infinita, entonces $\pi(\rho)$ es una representación de Steinberg.
2. Si ρ es reducible y la imagen de la restricción de ρ al subgrupo I_v es finita, entonces reemplazamos ρ por su semisimplificado ρ^{ss}. Es una suma de dos caracteres de Γ_v: $\rho^{ss} = \sigma_1 \oplus \sigma_2$,
$$\sigma_i : \Gamma_v \to L^\times, \ i = 1, 2.$$
con valores en L. Sea $\chi_i : F_v^\times \to L^\times$ el carácter de $F_v^\times$ asociado a σ_i por la teoría de cuerpo de clases para F_v. Entonces $\pi(\rho) = I(\chi_1, \chi_2)$ cuando esta representación inducida esta irreducible (lo que el único caso que nos interese).
3. En particular, $\pi(\rho)$ es una representación esférica si y solamente si ρ es una representación no ramificada.

Comentario 3.19. La definición de $\pi(\rho)$ parace depender de la idenficación de los caracteres $\chi_i : F_v^\times \to L^\times$ con caracteres con valores *complejos*. Cuando $\rho = \rho_{p,E,v}$, o más generalmente cuando ρ proviene de una representación sobre la cohomologia p-adica de una curva de Shimura, es un teorema que los caracteres χ_i tienen valores algebraicos, y existe un método para reemplazar los χ_i p-adicos con χ_i complejos.

Decimos que *E tiene reducción multiplicativa* si $\pi(\rho_{p,E,v})$ es una representación de Steinberg.

Hemos definido para todo primo v no arquimediano una representación lisa e irreducible $\pi_v(E) = \pi(\rho_{p,E,v})$ asociada a la curva elíptica E, o más bien a su módulo de Tate. El siguiente teorema implica que $\pi_v(E)$ es no ramificada para todos los primos salvo un número finito:

Teorema 3.20. *La curva elíptica E tiene buena reducción en el primo v si y solamente si, para todo primo racional p relativamente primo a v, $\rho_{p,E,v}$ es una representación no ramificada (es decir, si y solamente si $\pi(\rho)$ es una representación esférica).*

Siguiendo el Comentario 2.26, para un primo σ arquimediano definimos $\pi_v(E) = \pi_1$, la representación de $GL(2, \mathbb{R})/\mathbb{R}^\times$ que corresponde a las formas modulares de peso 2. Así podemos definir la representación irreducible $\pi(E) = \otimes'_v \pi_v(E)$ de $GL(2, F_{\mathbf{A}})$, teniendo en cuenta el hecho (Teorema 3.20) que casi todas las $\pi_v(E)$ son no ramificadas. El Teorema 3.18 admite la siguiente reformulación:

Teorema 3.21 (Freitas, Le Hung, y Siksek)**.** *Sea E una curva elíptica sobre el cuerpo real cuadático F. Entonces la representación $\pi(E)$ de $GL(2, F_{\mathbf{A}})$ es isomorfa a una representación automorfa cuspidal.*

Si además existe un primo no arquimediano v donde E tiene una reducción multiplicativa o supercuspidal , entonces $\pi(E)$ es de la forma $\pi(E) = JL(\pi^D(E))$, donde $\pi^D(E)$ es una representación automorfa de $D^\times(\mathbf{A})$ con D un álgebra cuaterniónica de división sobre F, ramificada en todos los primos arquimedianos de F salvo uno.

Más generalmente, tenemos la siguiente conjetura.

Conjetura 3.22. *Sea E una curva elíptica sobre el cuerpo totalmente real F. Entonces la representación $\pi(E)$ de $GL(2, F_{\mathbf{A}})$ es isomorfa a una representación automorfa cuspidal.*

Si además el grado $d = [F : \mathbb{Q}]$ es impar, o si existe un primo no arquimediano v donde E tiene una reducción multiplicativa o supercuspidal, entonces $\pi(E)$ es de la forma $\pi(E) = JL(\pi^D(E))$, donde $\pi^D(E)$ es una representación automorfa de $D^\times(\mathbf{A})$ con D un álgebra cuaterniónica de división sobre F, ramificada en todos los primos arquimedianos de F salvo uno.

3.5. Algunas ideas de la demostración de Freitas et al.

3.5.1. La parte automorfa. Como $d = 1$ es un número impar, Conjetura 3.22 se aplica al caso $d = 1$, es decir, al caso $F = \mathbb{Q}$. Cuando $F = \mathbb{Q}$, Conjetura 3.22 es el teorema de [1]. La demostración en el caso de un cuerpo real cuadrático tiene la misma estructura que la demostración de [1], que generaliza la demostración del caso ya tratado por Wiles en [9]. Wiles trabajaba no con curvas de Shimura construidas a partir de álgebras de división sino con las curvas modulares $X_0(N)$ asociadas al grupo $GL(2) = M(2)^\times$ sobre $\mathbb{Q}$:

$$X_0(N) = [GL(2, \mathbb{Q})\backslash \mathfrak{H}^{\pm} \times GL(2, \mathbf{A}_{\mathbb{Q}})/K_0(N) \cdot \mathbf{A}_{\mathbb{Q}}^{\times}]^*$$

donde el sobreíndice * designa la compactificación. Aquí hemos reemplazado el ideal $\mathfrak{n}$ por el entero $N > 1$. Como $D = M(2, \mathbb{Q})$, escribimos $\mathbb{T}_N$ en vez de $\mathbb{T}_0(N, D)$ para el álgebra de Hecke correspondente.

Sea E una curva elíptica sobre $\mathbb{Q}$. Para demostrar que E es isomorfa a un cociente de $J_0(N) = Jac(X_0(N))$, es suficiente (Teorema 3.2) demostrar que la representación $\rho_{E,p}$ de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ sobre el módulo de Tate de E es isomorfa a una subrepresentación del módulo de Tate de $Jac(X_0(N))$. Una consecuencia de [1] es el siguiente teorema más preciso:

Teorema 3.23. *De hecho, $\rho_{E,p}$ es isomorfa a la representación de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ sobre un $\mathbb{T}_N$-submódulo de*

$$T_p(Jac(X_0(N))^{nuevo} = \varprojlim_n Jac(X_0(N))^{nuevo}[p^n]$$

de $\mathbb{Z}_p$-rango 2.

Como $T_p(Jac(X_0(N))^{nuevo}) \xrightarrow{\sim} H_1(Jac(X_0(N))^{nuevo}, \mathbb{Z}) \otimes \mathbb{Z}_p$, un $\mathbb{T}_N$-submódulo $M \subset H_1(Jac(X_0(N))^{nuevo}, \mathbb{Z})$ define un $\mathbb{T}_N$-submódulo de $T_p(Jac(X_0(N))^{nuevo})$. Por otra parte, el isomorfismo de Hodge (3.4) identifica $M \otimes \mathbb{C}$ con un $\mathbb{T}_N$ submódulo de

$$Hom(\Omega^1(X_0(N)), \mathbb{C}) \oplus Hom(\bar{\Omega}^1(X_0(N)), \mathbb{C}).$$

Como el álgebra de Hecke $\mathbb{T}_N$ es autoadjunto para el producto escalar de Petersson, se puedo demostrar que

Proposición 3.24. *(a) Los $\mathbb{T}_N$-módulos $\Omega^1(X_0(N)), \mathbb{C})$ y $\bar{\Omega}^1(X_0(N)), \mathbb{C})$ son isomorfos.*

(b) Sea $h \subset H^1(Jac(X_0(N))^{nuevo}, \mathbb{C})$ un vector propio de $\mathbb{T}_N$:

$$T(h) = \lambda(T)h \ \forall T \in \mathbb{T}_N.$$

Entonces hay una forma modular nueva

$$\omega \in \Omega^1(X_0(N)), \mathbb{C}) \xrightarrow{\sim} M_2(\Gamma_0(N))$$

que es vector propio de $\mathbb{T}_N$ con carácter λ.

(c) Sea $M \subset H_1(Jac(X_0(N))^{nuevo}, \mathbb{Z})$ un $\mathbb{T}_N$-submódulo de $\mathbb{Z}$-rango 2. Entonces la acción de $\mathbb{T}_N$ sobre M se factoriza por un carácter $\mathbb{T}_N \to \mathbb{Z}$.

Sea $M \subset H_1(Jac(X_0(N))^{nuevo}, \mathbb{Z})$ un $\mathbb{T}_N$-submódulo de $\mathbb{Z}$-rango 2. La Proposición 3.24 implica que existe una forma modular nueva $\omega \in M_2(\Gamma_0(N))$ con las mismas valores propias que M para el álgebra de Hecke $\mathbb{T}_N$. Ya hemos visto que ω corresponde a una representación automorfa Π de $GL(2, \mathbf{A}_{\mathbb{Q}})$. (Y es fácil demostrar que Π es una representación *cuspidal*.)

Por otra parte, si Π es una representación automorfa cuspidal de $GL(2, \mathbf{A}_{\mathbb{Q}})$ tal que $\dim \Pi^{K_0(N)} = 1$, y si el carácter de $\mathbb{T}_N$ sobre $\Pi^{K_0(N)}$ tiene valores en $\mathbb{Z}$, entonces existe un cociente E de $Jac(X_0(N))^{nuevo}$ de dimensión 1, invariante por las correspondencias de Hecke, y la acción de $\mathbb{T}_N$ sobre $T_p(E) \subset T_p(Jac(X_0(N))^{nuevo})$ (o sobre el cociente $T_p(Jac(X_0(N))^{nuevo}) \to T_p(E)$) es idéntica a la acción sobre $\Pi^{K_0(N)}$.

La misma construcción es válida si reemplazamos $\mathbb{Q}$ por un cuerpo totalmente real F y $X_0(N)$ por la curva de Shimura $X_0(\mathfrak{n}, D)$. El siguiente teorema de Carayol es una generalización de un resultado celebrado de Eichler y Shimura.

Teorema 3.25 (Carayol)**.** *Sea E una curva elíptica sobre el cuerpo totalmente real F. Suponemos que E es isomorfa al cociente de*

$Jac(X_0(\mathfrak{n}, D))^{nuevo}$ asociado a la la representación automorfa Π^D de $D^\times(\mathbf{A})$. Entonces $\pi(E) \xrightarrow{\sim} JL(\Pi^D)$. En particular, tenemos

$$L(s, E) \xrightarrow{\sim} L(s, \Pi^D).$$

La demostración del teorema de Carayol (y del teorema de Eichler-Shimura) esta basada sobre una comparación de las correspondencias $T(q)$ (para un número primo q) con la correspondencia de Frobenius, actuando sobre un modelo de la curva de Shimura en característica q. Esta comparación se llama la *Formula de congruencia de Eichler-Shimura*.

3.5.2. La parte aritmética. Hasta ahora hemos explicado (muy rapidamente!) como obtenir una curva elíptica sobre F a partir de una representación automorfa con ciertas propiedades. Pero el teorema de Freitas et al va en la dirección opuesta. ¿Como obtener una representación automorfa π cuando tenemos solamente la curva elíptica E, o más bien su representación p-adica $\rho_{E,p}$?

Designamos por $\rho_E[p]$ la representación de $Gal(\overline{\mathbb{Q}}/F)$ sobre $E[p]$, que es un espacio vectorial de dimension 2 sobre $\mathbb{F}_p$. El idea de Wiles es de comenzar por suponer que $p = 3$. ¿Por qué 3? Porque un teorema de Langlands y un teorema de Tunnell implican el siguiente teorema.

Teorema 3.26. *Sea F un cuerpo totalmente real. Sea*

$$\rho : Gal(\overline{\mathbb{Q}}/F) \to GL(2, \mathbb{F}_3)$$

una representación continua. Entonces hay un ideal $\mathfrak{n} \subset \mathcal{O}_F$ y una forma modular nueva de Hilbert f de peso $(2, 2, \ldots, 2)$ para $K_0(\mathfrak{n})$ tal que $\rho_{f,3} \equiv \rho$ (mód 3).

No hemos definido las representaciones $\rho_{f,p} : Gal(\overline{\mathbb{Q}}/F) \to GL(2, \bar{\mathbb{Q}}_p)$ asociadas a las formas nuevas de Hilbert. Si f es de peso $(2, 2, \ldots, 2)$ y de nivel $K_0(\mathfrak{n})$, y si $d = [F : \mathbb{Q}]$ es un número impar, entonces $\rho_{f,p}$ es la representación sobre un submódulo del módulo de Tate del jacobiano de una curva de Shimura, y la reducción módulo p de $\rho_{f,p}$ es la acción sobre un subgrupo del grupo de elementos de p-torsión del jacobiano. Más generalmente la primera construcción de estas representaciones fue encontrada por Taylor en su tésis.

Como consecuencia del Teorema 3.26, sabemos que $\rho_E[3]$ es isomorfa a una representación de la forma $\rho_{f,3}$ (mód 3) por una forma modular nueva de Hilbert f de peso $(2, 2, \ldots, 2)$. El siguiente teorema del artículo [4] es basado sobre el método de Wiles y Taylor-Wiles, y más directamente es una consecuencia de un resultado de Breuil y Diamond (y de resultados anteriores de Kisin, Gee, y Barnet-Lamb-Gee-Geraghty):

Teorema 3.27. *Sea E una curva elíptica sobre un cuerpo totalmente real F. Sea p un número primo impar. Suponemos que*

1. *$\rho_E[p]$ es isomorfa a una representación de la forma $\rho_{f,p}$ (mód p) donde f es una forma modular nueva de Hilbert para F de peso $(2, 2, \ldots, 2)$;*
2. *La restricción de $\rho_E[p]$ al grupo de Galois $Gal(\overline{\mathbb{Q}}/F(\zeta_p))$ es absolutamente irreducible.*

Entonces E es modular.

Ya sabemos que $\rho_E[3]$ satisface la primera condición. Pero qué hacer si la restricción de $\rho_E[3]$ a $Gal(\overline{\mathbb{Q}}/F(\zeta_3))$ es reducible? Cuando $F = \mathbb{Q}$, Wiles utilice una propiedad geométrica de la curva $X_0(15)$ – es una curva de género uno, con un número finito de puntos racionales sobre $\mathbb{Q}$ – para mostrar que, si la imagen de $\rho_E[3]$ es demasiado pequeña, entonces (i) se puede mostrar que $\rho_E[5]$ es isomorfa a una representación de la forma $\rho_{f,5}$ (mód 5) y (ii) las imágenes de $\rho_E[3]$ y $\rho_E[5]$ no pueden estar simultaneamente pequeñas. Así el Teorema 3.27 implica que E es modular. (Ver el artículo [3] de K. Buzzard para una explicación mas detallada de la demostración de Wiles.)

Cuando F es un cuerpo real cuadrático, la curva $X_0(15)$ puede tener un número infinito de puntos racionales sobre F, y el argumento de Wiles no funciona. Los autores de [4] son obligados a generalizar este argumento. En vez de la curva $X_0(15)$ y las solas representaciones $\rho_E[3]$ y $\rho_E[5]$ utilicen una familia de 27 curvas modulares y las tres representaciones $\rho_E[3]$, $\rho_E[5]$ y $\rho_E[7]$. El análisis de puntos racionales de estas 27 curvas, sobre cuerpos reales, es muy sutil, y es poco probable que permitira demostrar la Conjetura 3.22 en toda su generalidad.

Referencias

[1] Breuil, Christophe, Brian Conrad, Fred Diamond and Richard Taylor, On the modularity of elliptic curves over **Q**: wild 3-adic exercises, *J. Amer. Math. Soc.*, **14** (2001) 843–939.

[2] Breuil, Christophe, and Fred Diamond, Formes modulaires de Hilbert módulo p et valeurs dextensions galoisiennes, *Ann. Sci. ENS*, **47** (2014) 905–974.

[3] Buzzard, Kevin, Potential modularity – a survey, in J. Coates et al., ed, *Non-abelian fundamental groups and Iwasawa theory*, Cambridge: Cambridge University Press, *London Mathematical Society Lecture Note Series*, **393** (2011) 188–211.

[4] Freitas, Nuno, B. V. Le Hung, and S. Siksek, Elliptic Curves over Real Quadratic Fields are Modular, *Inventiones Math.*, **201** (2015) 159–206.

[5] Godement, Roger and Hervé Jacquet, *Zeta functions of simple algebras*, *Lecture Notes in Mathematics* **260** (1972).

[6] Harris, Michael, An introduction to the stable trace formula. *On the stabilization of the trace formula*, *Stab. Trace Formula Shimura Var. Arith. Appl. 1*, Int. Press, Somerville, MA, (2011) 3–47.
[7] Ribet, Kenneth and William Stein, *Lectures on Modular Forms and Hecke Operators*, https://code.google.com/p/ribet-stein-modforms/.
[8] Taylor, Richard and Andrew Wiles, Ring-theoretic properties of certain Hecke algebras, *Annals of Mathematics* **141** 553–572 (1995).
[9] Wiles, Andrew, Modular elliptic curves and Fermat's Last Theorem *Annals of Mathematics* **141** 443551 (1995).