Capítol 6

Congruències d'Eichler-Shimura

A. Travesa

6.1 Definicions i notacions

6.1.1 • Fixem una $\mathbb{Q}$-àlgebra de quaternions indefinida, B; un ordre maximal, $\mathcal{O} \subseteq B$; i una immersió de B en $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}(2, \mathbb{R})$, $\chi : B \longrightarrow \mathrm{M}(2, \mathbb{R})$.

• Sigui $D := \operatorname{disc}(B) = \operatorname{disc}(\mathcal{O})$ el discriminant de l'àlgebra de quaternions, que coincideix amb el dels ordres maximals, i considerem el subgrup d'unitats de norma 1 de $\mathcal{O}$, $\Gamma := \{\alpha \in \mathcal{O} : \mathrm{n}(\alpha) = 1\}$.

• Considerem, també, el semigrup dels elements de $\mathcal{O}$ de norma positiva, $\Delta := \{\alpha \in \mathcal{O} : \mathrm{n}(\alpha) > 0\}$.

• Denotarem per $\alpha \mapsto \alpha'$ la conjugació canònica de B; aquesta conjugació es pot veure com la restricció de la conjugació de $\mathrm{M}(2, \mathbb{R})$,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

• Per a tot ideal bilateral $\mathfrak{a} = \alpha\mathcal{O} = \mathcal{O}\alpha \subseteq \mathcal{O}$, escriurem $\Gamma_\alpha := \Gamma_{\mathfrak{a}} := \{\gamma \in \Gamma : \gamma \equiv 1 \pmod{\mathfrak{a}}\}$.

• Notem que, per a tot nombre enter $m \neq 0$, $m\mathcal{O} = \mathcal{O}m$ és un ideal bilateral, ja que m és un element regular i central. En particular, podem considerar el grup Γ_m.

• Se satisfan les inclusions $\Gamma \subseteq \Delta \subseteq \tilde{\Gamma}$, on $\tilde{\Gamma} = B^*$ és el commensurador de Γ en B^*. Per tant, podem parlar de l'anell de Hecke $R(\Gamma, \Delta)$ (cf. Arenas, capítol 5).

• Si, per a $\alpha \in \Delta$, posem

$$\deg(\Gamma\alpha\Gamma) := \#\{\Gamma\alpha_i : \Gamma\alpha_i \subseteq \Gamma\alpha\Gamma,\ \alpha_i \in B^*\},$$

obtenim que $\deg(\Gamma\alpha\Gamma) = [\Gamma : \Gamma \cap \alpha^{-1}\Gamma\alpha] = [\alpha\Gamma\alpha^{-1} : \alpha\Gamma\alpha^{-1} \cap \Gamma] < +\infty$, perquè $\alpha \in \tilde{\Gamma}$.

6.1.1 Divisors elementals

6.1.2 Volem associar, a cada $\alpha \in \Delta$, una família de "divisors elementals", un per a cada nombre natural primer.

• Si $p \nmid D$, és $B_p := B \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \mathrm{M}(2, \mathbb{Q}_p)$ i l'isomorfisme pot ésser triat de manera que $\mathcal{O}_p := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ s'identifiqui amb $\mathrm{M}(2, \mathbb{Z}_p)$. Llavors, vist α en $\mathrm{M}(2, \mathbb{Z}_p)$, existeixen $\varepsilon_1, \varepsilon_2 \in \mathrm{GL}(2, \mathbb{Z}_p)$ tals que $\varepsilon_1\alpha\varepsilon_2 = \begin{bmatrix} p^{e_1} & 0 \\ 0 & p^{e_2} \end{bmatrix}$, on $e_1, e_2 \in \mathbb{Z}$ i $0 \leq e_1 \leq e_2$. El p-èsim divisor elemental associat a α és, per definició, la parella (e_1, e_2).

• Si $p|D$, B_p és un cos no commutatiu i $\mathcal{O}_p$ és l'únic ordre maximal de B_p. Sigui $\pi_p \in \mathcal{O}_p$ un element qualsevol de norma p (l'existència n'és garantida, ja que en B hi ha elements de norma qualsevol nombre racional donat). Ara, l'ideal $\mathcal{O}_p\alpha$ generat per α en $\mathcal{O}_p$ és una certa potència de $\mathcal{O}_p\pi_p$, posem $\mathcal{O}_p\alpha = (\mathcal{O}_p\pi_p)^{e_p}$, on $e_p \in \mathbb{Z}$, $e_p \geq 0$, és un nombre enter independent de l'element π_p elegit de norma p. El p-èsim divisor elemental associat a α és, per definició, e_p.

6.1.3 Proposició. *Siguin $\alpha, \beta \in \Delta$. Les propietats següents són equivalents.*

(a) $\Gamma\alpha\Gamma = \Gamma\beta\Gamma$.

(b) *Per a tot nombre natural primer p, el p-èsim divisor elemental de α coincideix amb el p-èsim divisor elemental de β.*

(c) *Els $\mathcal{O}$-mòduls $\mathcal{O}/\mathcal{O}\alpha$ $\mathcal{O}/\mathcal{O}\beta$ són isomorfs.*

(d) *Existeix $\gamma \in \Gamma$ tal que $\mathcal{O}\alpha\gamma = \mathcal{O}\beta$.* $\square$

Notem que les condicions (a), (c) i (d) són globals, mentre que la condició (b) és intrínsecament local.

6.2 Sèries de Dirichlet formals

Donat un anell R, que suposarem que és commutatiu, l'anell de les sèries de Dirichlet de coeficients en R és l'anell que té per elements les funcions aritmètiques $S : \mathbb{N} - \{0\} \longrightarrow R$; és a dir, les successions $S := (S(1), S(2), \dots, S(n), \dots)$ d'elements $S(n) \in R$. La suma es defineix com la suma de successions, i el producte és la convolució de Dirichlet, definida de la manera següent. Si $S = (S(1), S(2), \dots, S(n), \dots)$ i $T = (T(1), T(2), \dots, T(n), \dots)$, $S(n), T(n) \in R$, llavors,

$$S * T := (U(1), U(2), \dots, U(n), \dots),$$

on, per a tot nombre natural $n \geq 1$, és

$$U(n) := \sum_{d|n} S(d)T(n/d).$$

És un exercici immediat comprovar que aquestes operacions determinen una estructura d'anell, que anomenarem l'anell de les sèries de Dirichlet de coeficients en R.

És usual escriure les sèries de Dirichlet en la forma

$$D(S; s) = \sum_{n \geq 1} S(n) n^{-s},$$

i el producte de Dirichlet s'ha definit de manera que se satisfaci formalment la propietat que

$$\begin{aligned} D(S; s)D(T; s) &= \sum_{n \geq 1} S(n) n^{-s} \sum_{n \geq 1} T(n) n^{-s} \\ &= \sum_{n \geq 1} (S * T)(n) n^{-s} = D(S * T; s), \end{aligned}$$

on els símbols n^{-s} (de moment, només són símbols) satisfan les propietats $(n \cdot m)^{-s} = n^{-s}m^{-s}$, per a tot $m, n \in \mathbb{Z}$, $m, n \geq 1$, per definició.

6.2.1 Observació. Notem que si, per exemple, s és una variable complexa, es pot definir una funció $\mathbb{N} - \{0\} \times \mathbb{C} \longrightarrow \mathbb{C}$ per $(n, s) \mapsto n^{-s}$, de manera que se satisfan les propietats anteriors dels símbols n^{-s}.

6.2.1 Productes d'Euler formals

Sigui $D(S; s)$ una sèrie de Dirichlet formal de coeficients en un anell commutatiu R i suposem que la funció aritmètica $S : \mathbb{N} - \{0\} \longrightarrow R$ és multiplicativa; és a dir, que se satisfà que $S(mn) = S(m)S(n)$, per a $m, n \geq 1$ tals que $\mathrm{mcd}(m, n) = 1$.

En aquest cas, se satisfà la propietat que

$$D(S; s) = \sum_{n \geq 1} S(n)n^{-s} = \prod_p \sum_{m \geq 0} S(p^m)p^{-ms} \text{ (producte d'Euler)},$$

el producte estès, com és habitual, al conjunt de tots els nombres naturals primers.

Això és dir que, d'una banda, considerem una infinitat de sèries de Dirichlet, una per a cada nombre primer p,

$$E_p(S; s) := \sum_{m \geq 0} S(p^m)p^{-ms},$$

els coeficients de la qual que corresponen als índexs n que no són potències de p són nuls; i, d'altra banda, que considerem el producte infinit d'aquestes sèries

$$\prod_p E_p(S; s).$$

Hem d'observar que cal definir aquest producte infinit; però això no comporta cap problema. En efecte; donat $n \in \mathbb{Z}$, $n \geq 1$, el conjunt de nombres primers p que divideixen n és finit; per tant, per a tot $n \geq 1$, i per al càlcul del coeficient de n^{-s} de la sèrie producte, només intervé una quantitat finita de sèries $E_p(S; s)$ en què el coeficient de les quals que cal multiplicar és diferent de 1. Així, podem definir el producte infinit, perquè cadascun dels coeficients de la sèrie producte és definit com un producte (finit) d'elements de R.

6.2.2 Observació. Suposem que la funció aritmètica S és completament multiplicativa; és a dir, que la propietat que $S(mn) = S(m)S(n)$ se satisfà per a tota parella de nombres naturals $m, n \geq 1$, sense restricció. Aleshores, per als factors d'Euler se satisfà que

$$E_p(S; s) = \sum_{m\geq 0} S(p^m)p^{-ms} = (1 - S(p)p^{-s})^{-1}.$$

En efecte; observem que $1 - S(p)p^{-s}$ és una sèrie de Dirichlet que només conté els dos sumands que corresponen a $n = 1$ i $n = p$, de manera que el càlcul dels coeficients de la sèrie de Dirichlet producte de $1 - S(p)p^{-s}$ per

$$\sum_{m\geq 0} S(p^m)p^{-ms}$$

és immediat i proporciona la sèrie de Dirichlet 1; és a dir, $1 - S(p)p^{-s}$ és l'element invers, en l'anell de les sèries de Dirichlet, de

$$\sum_{m\geq 0} S(p^m)p^{-ms}.$$

Notem que, de fet, per a un factor d'Euler donat, $E_p(S; s)$, només cal demanar que se satisfaci la propietat que $S(p^m) = S(p)^m$, per a tot $m \geq 0$. Si és així, obtenim que aquest factor d'Euler és

$$E_p(S; s) = \sum_{m\geq 0} S(p^m)p^{-ms} = (1 - S(p)p^{-s})^{-1},$$

independentment de si els altres satisfan o no la propietat anàloga.

6.3 Sèries de Dirichlet a l'anell de Hecke

6.3.1 Definició i propietats

Volem definir una sèrie de Dirichlet de coeficients en l'anell de Hecke $R(\Gamma, \Delta)$; cal, doncs, donar els coeficients.

En el capítol anterior, i per a tot nombre enter $n \geq 1$, s'han definit els elements de Hecke o coeficients de Hecke (més endavant, definirem els *operadors* de Hecke)

$$T(n) := \sum \{(\Gamma\alpha\Gamma) : \alpha \in \Delta, \, \mathrm{n}(\alpha) = n\} \in R(\Gamma, \Delta).$$

6.3.1 Definició. Posarem,

$$D(T; s) := \sum_{n \geq 1} T(n) n^{-s},$$

la sèrie de Dirichlet definida pels coeficients de Hecke $T(n) \in R(\Gamma, \Delta)$.

6.3.2 En el nostre cas, les propietats dels elements Hecke anàlogues a les de **5.1.5** i **5.1.6** es poden escriure en la forma:

• La funció aritmètica $n \mapsto T(n)$ és multiplicativa.

• Si $p|D$, per a tot nombre enter $m \geq 0$, és

$$T(p^m) = T(p)^m.$$

A més a més, si $\alpha \in \Delta$ és un element de norma $\mathrm{n}(\alpha) = p$ i $m \geq 0$, és

$$T(p^m) = (\Gamma\alpha^m\Gamma).$$

• Suposem ara que $p \nmid D$; per a nombres enters $e_1, e_2 \in \mathbb{Z}$ tals que $0 \leq e_1 \leq e_2$, posem

$$T(p^{e_1}, p^{e_2}) := (\Gamma\alpha\Gamma),$$

on $(\Gamma\alpha\Gamma)$ és l'única classe doble amb $\alpha \in \Delta$ caracteritzada pel fet que el p-èsim divisor elemental de α és la parella (e_1, e_2). Llavors:

(a) $T(p^{e_1+1}, p^{e_2+1}) = T(p,p)T(p^{e_1}, p^{e_2})$.

(b) Per a tot $e \geq 1$, $T(p)T(p^e) = T(1, p^{e+1}) + (p+1)T(p,p)T(p^{e-1})$.

(c) Per a tot $e > 1$, $T(1,p)T(1,p^e) = T(1,p^{e+1}) + pT(p,p^e)$.

(d) Per a tot $e \geq 1$, $\deg(T(1,p^m)) = p^{m-1}(p+1)$.

(e) Notem que $T(1) = 1$ i que $T(1,p) = T(p)$; en particular, el cas $e = 1$ de (b) és $T(1,p)^2 = T(1,p^2) + (p+1)T(p,p)$.

(f) Per a $m \geq 2$, se satisfà que

$$T(p^m) = T(1,p^m) + T(p,p)T(p^{m-2}).$$

6.3.2 Producte d'Euler

Les propietats anteriors ens permeten establir fàcilment el resultat següent.

6.3.3 Teorema. *Per a la sèrie de Dirichlet $D(T;s)$ se satisfà que*

$$D(T;s) = \prod_{p|D}(1 - T(p)p^{-s})^{-1} \prod_{p\nmid D}(1 - T(p)p^{-s} + T(p,p)p^{1-2s})^{-1}.$$

DEMOSTRACIÓ: Com que la funció aritmètica $n \mapsto T(n)$ és multiplicativa, obtenim de seguida el desenvolupament de $D(T;s)$ com a producte d'Euler de la forma

$$D(T;s) = \sum_{n\geq 1} T(n)n^{-s} = \prod_p E_p(T;s),$$

on

$$E_p(T;s) = \sum_{m\geq 0} T(p^m)p^{-ms};$$

doncs, cal estudiar aquests factors.

Suposem, en primer lloc, que p és un divisor de D. El fet que, per a tot $m \geq 0$ sigui $T(p^m) = T(p)^m$ fa que el factor d'Euler $E_p(T;s)$ sigui la sèrie

$$E_p(T;s) = \sum_{m\geq 0} T(p)^m p^{-ms} = (1 - T(p)p^{-s})^{-1},$$

com més amunt.

Suposem, finalment, que $p \nmid D$, i calculem els coeficients de la sèrie de Dirichlet producte de les dues sèries $1 - T(p)p^{-s} + pT(p,p)p^{-2s}$ i

$$E_p(T;s) = \sum_{m\geq 0} T(p^m)p^{-ms}.$$

Clarament, per als valors de n que no siguin potències de p, els coeficients n-èsims del producte són nuls. A més a més, per a $n = 1$, el coeficient del producte és $T(1) = 1$; per a $n = p$, el coeficient del producte és $T(p) - T(p)T(1) = 0$; i, per a $n = p^m$, amb $m \geq 2$, obtenim que el coeficient del producte és

$$\begin{aligned} & T(p^m) - T(p)T(p^{m-1}) + pT(p,p)T(p^{m-2}) \\ =& T(p^m) - (T(1,p^m) + (p+1)T(p,p)T(p^{m-2})) + pT(p,p)T(p^{m-2}) \\ =& T(p^m) - T(1,p^m) - T(p,p)T(p^{m-2}) = 0, \end{aligned}$$

ja que $T(p^m) = T(1,p^m) + T(p,p)T(p^{m-2})$. Això acaba la prova. □

6.3.4 Corol·lari. *Per a tot nombre enter $n \geq 1$, és té*

$$\deg(T(n)) = \sum_{\substack{d|n \\ \mathrm{mcd}(d,D)=1}} d. \quad \square$$

6.4 Operadors de Hecke

6.4.1 Caracterització de l'anell de Hecke

Interessa, a continuació, caracteritzar l'anell de Hecke a partir dels ideals bilaterals coprimers amb el discriminant D de l'àlgebra de quaternions. Per a això, comencem per observar que els subgrups $\Gamma_{\mathfrak{a}}$, per a $\mathfrak{a} = \mathcal{O}\alpha$ un ideal bilateral de $\mathcal{O}$, fan el paper dels subgrups $\Gamma(N) \subseteq \mathrm{SL}(2,\mathbb{Z})$ del cas clàssic. En efecte, se satisfan les propietats següents.

6.4.1 • Si $\mathfrak{a}$, $\mathfrak{b} \subseteq \mathcal{O}$ són ideals bilaterals primers entre si, llavors $\Gamma = \Gamma_{\mathfrak{a}}\Gamma_{\mathfrak{b}}$.

• Si $\mathfrak{a} \subseteq \mathcal{O}$ és un ideal bilateral de $\mathcal{O}$ i $\alpha, \beta \in \Delta$ són elements tals que $\mathrm{mcd}(\mathrm{n}(\alpha), \mathfrak{a}) = \mathrm{mcd}(\mathrm{n}(\beta), \mathfrak{a}) = 1$, llavors, condició necessària i suficient perquè sigui $\Gamma_{\mathfrak{a}}\alpha = \Gamma_{\mathfrak{a}}\beta$ és que sigui $\Gamma\alpha = \Gamma\beta$ i, alhora, $\alpha \equiv \beta \pmod{\mathfrak{a}}$.

• Si $\mathfrak{a} \subseteq \mathcal{O}$ és un ideal bilateral i $\alpha \in \Delta$ és un element tal que $\mathrm{mcd}(\mathrm{n}(\alpha), \mathfrak{a}) = 1$, llavors,

(a) $\Gamma\alpha\Gamma = \Gamma\alpha\Gamma_{\mathfrak{a}} = \Gamma_{\mathfrak{a}}\alpha\Gamma$.

(b) $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} = \{\beta \in \Gamma\alpha\Gamma : \beta \equiv \alpha \pmod{\mathfrak{a}}\}$.

(c) Si $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} = \biguplus_i \Gamma_{\mathfrak{a}}\alpha_i$, llavors, $\Gamma\alpha\Gamma = \biguplus_i \Gamma\alpha_i$.

6.4.2 Definició. Per a tot ideal bilateral $\mathfrak{a} \subseteq \mathcal{O}$, posarem $\Delta_{\mathfrak{a}} := \{\alpha \in \Delta : \operatorname{mcd}(\operatorname{n}(\alpha), \mathfrak{a}) = 1\}$.

6.4.3 Definició. Si $\mathfrak{a} \subseteq \mathcal{O}$ és un ideal bilateral tal que $\operatorname{mcd}(D, \mathfrak{a}) = 1$, llavors existeix un nombre enter $a \in \mathbb{Z}$, $a > 0$, tal que $\mathfrak{a} = a\mathcal{O}$ i $\mathcal{O}/\mathfrak{a} = \mathcal{O}/a\mathcal{O} \simeq \mathrm{M}(2, \mathbb{Z}/a\mathbb{Z})$. Posarem $\Delta_{\mathfrak{a}}^* := \{\alpha \in \Delta_{\mathfrak{a}} :$ existeix $c \in \mathbb{Z}/a\mathbb{Z}$ tal que $\alpha \equiv \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix} \pmod{a}\}$.

El conjunt $\Delta_{\mathfrak{a}}^*$ és un subsemigrup de B^* que conté $\Gamma_{\mathfrak{a}}$ i que, alhora, està inclòs en el commensurador de $\Gamma_{\mathfrak{a}}$. Per tant, podem parlar, també, de l'anell de Hecke $R(\Gamma_{\mathfrak{a}}, \Delta_{\mathfrak{a}}^*)$. Se satisfà el resultat següent, que permet caracteritzar l'anell de Hecke $R(\Gamma, \Delta)$.

6.4.4 Proposició. *Si* $\mathfrak{a} \subseteq \mathcal{O}$ *és un ideal bilateral tal que* $\operatorname{mcd}(D, \mathfrak{a}) = 1$*, l'assignació*

$$\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} \mapsto \Gamma\alpha\Gamma$$

defineix un isomorfisme $R(\Gamma_{\mathfrak{a}}, \Delta_{\mathfrak{a}}^*) \longrightarrow R(\Gamma, \Delta)$ *entre els anells de Hecke.* $\square$

Notem que, ara, el grup $\Gamma_{\mathfrak{a}}$ ja no és el grup de les unitats de norma 1 d'un ordre maximal de B, sinó que n'és un cert subgrup.

6.4.2 Formes modulars

Posarem $\mathcal{H} := \{z \in \mathbb{C} : \operatorname{Im}(z) > 0\}$, el semiplà superior de Poincaré, i considerarem l'acció usual de $\mathrm{GL}^+(2, \mathbb{R})$ en $\mathcal{H}$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z := \frac{az+b}{cz+d};$$

denotarem per $j\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, z\right)$ el nombre complex $cz + d$.

6.4.5 La representació (fidel) $\chi : B \longrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}(2, \mathbb{R})$ identifica Γ amb un subgrup discret de $\mathrm{GL}^{+}(2, \mathbb{R})$. En particular, per a tot ideal bilateral $\mathfrak{a} \subseteq \mathcal{O}$ i per a tot nombre enter $k \geq 0$ podem parlar de les formes parabòliques de pes k respecte de $\Gamma_{\mathfrak{a}}$; sigui $S_k(\Gamma_{\mathfrak{a}})$ l'espai vectorial complex d'aquestes formes parabòliques.

Recordem que f és una forma parabòlica de $S_k(\Gamma_{\mathfrak{a}})$ si:

(a) $f : \mathcal{H} \longrightarrow \mathbb{C}$ és una funció holomorfa;

(b) per a tot $\gamma \in \Gamma_{\mathfrak{a}}$ i tot $z \in \mathcal{H}$ és $f(\gamma(z)) j(\gamma, z)^{-k} = f(z)$; i

(c) f s'anul·la en les puntes de $\Gamma_{\mathfrak{a}}$.

6.4.6 Definició. Sigui $\mathfrak{a} \subseteq \mathcal{O}$ un ideal bilateral. Donada una classe doble $\Gamma_{\mathfrak{a}} \alpha \Gamma_{\mathfrak{a}}$, $\alpha \in \Delta_{\mathfrak{a}}^{*}$, considerem una descomposició

$$\Gamma_{\mathfrak{a}} \alpha \Gamma_{\mathfrak{a}} = \biguplus_{i} \Gamma_{\mathfrak{a}} \alpha_i$$

i, a cada $f \in S_k(\Gamma_{\mathfrak{a}})$, associem-li la funció $g(z)$ definida per

$$g(z) := \mathrm{n}(\alpha)^{k-1} \sum_{i} f(\alpha_i(z)) j(\alpha_i, z)^{-k}.$$

6.4.7 Se satisfan les propietats següents:

• La funció g no depèn ni de α ni de la família de representants $\{\alpha_i\}_i$; només depèn de la classe doble $\Gamma_{\mathfrak{a}} \alpha \Gamma_{\mathfrak{a}}$ (i, naturalment, de la funció f).

• $g \in S_k(\Gamma_{\mathfrak{a}})$; és a dir, $g(z)$ és una forma parabòlica de pes k per a $\Gamma_{\mathfrak{a}}$.

• L'aplicació

$$(\Gamma_{\mathfrak{a}} \alpha \Gamma_{\mathfrak{a}})_k : S_k(\Gamma_{\mathfrak{a}}) \longrightarrow S_k(\Gamma_{\mathfrak{a}}),$$

definida per l'assignació

$$f \mapsto f | (\Gamma_{\mathfrak{a}} \alpha \Gamma_{\mathfrak{a}})_k := g,$$

és $\mathbb{C}$-lineal.

6.4.8 Proposició. *L'aplicació* $R(\Gamma_{\mathfrak{a}}, \Delta_{\mathfrak{a}}^*) \longrightarrow \operatorname{End}_{\mathbb{C}}(S_k(\Gamma_{\mathfrak{a}}))$*, definida per l'assignació* $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}}) \mapsto (\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k$ *i estesa per linealitat, és una representació de l'anell de Hecke* $R(\Gamma, \Delta) \simeq R(\Gamma_{\mathfrak{a}}, \Delta_{\mathfrak{a}}^*)$ *en l'espai de les formes parabòliques* $S_k(\Gamma_{\mathfrak{a}})$*.* $\square$

6.4.9 Si prenem una $\mathbb{C}$-base $\{f_1, \ldots, f_m\}$ de $S_k(\Gamma_{\mathfrak{a}})$, obtenim un isomorfisme d'anells $\operatorname{End}_{\mathbb{C}}(S_k(\Gamma_{\mathfrak{a}})) \simeq \mathbf{M}(m, \mathbb{C})$ i, per composició, una representació $R(\Gamma_{\mathfrak{a}}, \Delta_{\mathfrak{a}}^*) \longrightarrow \mathbf{M}(m, \mathbb{C})$, on designem per $\mathcal{T}_k(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})$ la imatge de $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})$. Així, $\mathcal{T}_k(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}}) \in \mathbf{M}(m, \mathbb{C})$ és una matriu tal que, si posem $\mathbf{f} := \begin{bmatrix} f_1 \\ \vdots \\ f_m \end{bmatrix}$, és

$$\mathbf{f}|(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k = \mathcal{T}_k(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})\mathbf{f}.$$

Se satisfan les propietats següents.

- Si $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} = \biguplus_i \Gamma_{\mathfrak{a}}\alpha_i$, llavors $\Gamma_{\mathfrak{a}}\alpha'\Gamma_{\mathfrak{a}} = \biguplus_i \alpha_i'\Gamma_{\mathfrak{a}}$; i, per a tota funció $f \in S_k(\Gamma_{\mathfrak{a}})$, és

$$f|(\Gamma_{\mathfrak{a}}\alpha'\Gamma_{\mathfrak{a}})_k = \mathrm{n}(\alpha^{-1}) \sum_i f(\alpha_i'^{-1}(z)) j(\alpha_i'^{-1}, z)^{-k}.$$

- En particular, si $b \in \mathbb{Z}$, $b > 0$, obtenim que

$$f|(\Gamma_{\mathfrak{a}}b\Gamma_{\mathfrak{a}})_k = b^{k-2}f.$$

6.4.10 Proposició. *L'assignació* $\alpha \mapsto \mathcal{T}_k(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})$ *proporciona una representació del grup* Γ *tal que* $\Gamma_{\mathfrak{a}}$ *està inclòs en el nucli de la representació; per tant, una representació de* $\Gamma/\Gamma_{\mathfrak{a}}$*.* $\square$

6.4.3 Operadors de Hecke i sèries de Dirichlet

6.4.11 Definició. Sigui $\mathfrak{a} \subseteq \mathcal{O}$ un ideal bilateral tal que $\operatorname{mcd}(D, \mathfrak{a}) = 1$. Per a tot nombre enter $b \in \mathbb{Z}$ tal que $\operatorname{mcd}(b, \mathfrak{a}) = 1$, existeix un element $\gamma \in \Gamma$ tal que $\gamma \equiv \begin{bmatrix} b^{-1} & 0 \\ 0 & b \end{bmatrix} \pmod{\mathfrak{a}}$, i la matriu $\mathcal{T}_k(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})$ és determinada unívocament per b; escriurem $R_k(b; \mathfrak{a}) := \mathcal{T}_k(\Gamma_{\mathfrak{a}}\gamma\Gamma_{\mathfrak{a}})$.

6.4.12 Definició. Anàlogament, per a tot nombre natural n i tot nombre primer p tal que $p \nmid D$, escriurem $T(n;\mathfrak{a})$, $T(p,p;\mathfrak{a})$ les imatges en $R(\Gamma_{\mathfrak{a}}, \Delta^*_{\mathfrak{a}})$ dels elements $T(n)$, $T(p,p)$, i $\mathcal{T}_k(n;\mathfrak{a})$, $\mathcal{T}_k(p,p;\mathfrak{a})$ les imatges en $\mathbf{M}(m,\mathbb{C})$, respectivament.

6.4.13 Si $\gamma \in \Gamma$ és un element tal que $\gamma \equiv \begin{bmatrix} p^{-1} & 0 \\ 0 & p \end{bmatrix} \pmod{\mathfrak{a}}$, llavors $p\gamma \equiv \begin{bmatrix} 1 & 0 \\ 0 & p^2 \end{bmatrix} \pmod{\mathfrak{a}}$, i $\mathcal{T}_k(p,p;\mathfrak{a}) = p^{k-2} R_k(p;\mathfrak{a})$.

Aquestes propietats formals dels operadors de Hecke —observem que, efectivament, ara són operadors lineals, mentre que abans eren elements d'un anell abstracte—, permeten escriure el resultat següent.

6.4.14 Teorema. *Sigui* $\mathfrak{a} \subseteq \mathcal{O}$ *un ideal bilateral tal que* $\mathrm{mcd}(D,\mathfrak{a}) = 1$. *Siguin* $k \geq 0$ *un nombre enter i* m *la dimensió de l'espai* $S_k(\Gamma_{\mathfrak{a}})$, *de les formes parabòliques, i fixem una* $\mathbb{C}$*-base,* $\mathbf{f}$*, d'aquest espai, respecte de la qual considerarem la representació matricial de l'anell de Hecke* $R(\Gamma_{\mathfrak{a}}, \Delta^*_{\mathfrak{a}})$*. Aleshores, com a sèries de Dirichlet de matrius de* $\mathbf{M}(m,\mathbb{C})$*, se satisfà la igualtat*

$$\sum_{\substack{(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}}) \\ \alpha \in \Delta^*_{\mathfrak{a}}}} \mathcal{T}_k(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})\, \mathrm{n}(\alpha)^{-s} = \sum_{\mathrm{mcd}(n,\mathfrak{a})=1} \mathcal{T}_k(n;\mathfrak{a}) n^{-s}.$$

D'altra banda, també es té la descomposició en producte de factors d'Euler

$$\sum_{\mathrm{mcd}(n,\mathfrak{a})=1} \mathcal{T}_k(n;\mathfrak{a}) n^{-s} =$$
$$= \prod_{p|D} (1 - \mathcal{T}_k(p;\mathfrak{a}) p^{-s})^{-1} \prod_{p \nmid D\mathfrak{a}} (1 - \mathcal{T}_k(p;\mathfrak{a}) p^{-s} + R_k(p;\mathfrak{a}) p^{k-1-2s})^{-1}.$$

A més a més, per a la topologia usual de $\mathbf{M}(m,\mathbb{C})$*, la sèrie és convergent per a tot nombre complex* $s \in \mathbb{C}$ *tal que* $\mathrm{Re}(s) > k+1$.

Demostració: Les igualtats formals es dedueixen immediatament del resultat anàleg formal; només cal preocupar-se de les qüestions de convergència.

Per a cada forma parabòlica $f \in S_k(\Gamma_{\mathfrak{a}})$, definim $f^* : \mathrm{SL}(2,\mathbb{R}) \longrightarrow \mathbb{C}$ per l'assignació $\beta \mapsto f^*(\beta) := f(\beta(i))j(\beta,i)^{-k}$, on $i^2 = -1$. Ara, si $\mathfrak{a} \subseteq \mathcal{O}$ és un ideal bilateral, $\alpha \in \Delta^*_{\mathfrak{a}}$, $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} = \biguplus_i \Gamma_{\mathfrak{a}}\alpha_i$, i $f \in S_K(\Gamma_{\mathfrak{a}})$ és una forma parabòlica qualsevol, podem considerar la funció g^* definida a partir de la forma parabòlica $g := f|(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k$; obtenim immediatament que, per a tot $\beta \in \mathrm{SL}(2,\mathbb{R})$, se satisfà la igualtat

$$g^*(\beta) = \mathrm{n}(\alpha)^{k-1} \sum_i f^*(\alpha_i\beta).$$

Com que per a tot $\gamma \in \Gamma_{\mathfrak{a}}$ i tot $\beta \in \mathrm{SL}(2,\mathbb{R})$ és $f^*(\gamma\beta) = f^*(\beta)$, podem considerar la funció g^* com una funció definida en el conjunt quocient $\Gamma_{\mathfrak{a}}\backslash \mathrm{SL}(2,\mathbb{R})$, que és compacte (recordem que l'àlgebra de quaternions és indefinida), de manera que g^* assoleix el màxim en algun punt de $\mathrm{SL}(2,\mathbb{R})$. Com a conseqüència, s'obté que les arrels característiques de l'operador $\mathcal{T}_k(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})$ són fitades, en valor absolut, per $\mathrm{n}(\alpha)^{k-1}\deg(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})$.

Si ara tenim en compte que, per a una certa base de $S_k(\Gamma_{\mathfrak{a}})$, tots els operadors $\mathcal{T}_k(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})$ són diagonals (cf. més avall), el corol·lari 3.5 ens serveix per a concloure que la sèrie de Dirichlet és absolutament convergent per a $\mathrm{Re}(s) > k+1$, com volíem demostrar. □

Resta provar que, per a una certa base de $S_k(\Gamma_{\mathfrak{a}})$, tots els operadors $\mathcal{T}_k(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})$ són diagonals. Per a això, comencem per observar que si $\varepsilon \in \mathcal{O}$ és un element de norma $\mathrm{n}(\varepsilon) = -1$, i si considerem l'operador $T(\varepsilon)_k \in \mathrm{End}_{\mathbb{Z}}(S_k(\Gamma_{\mathfrak{a}}))$ definit per

$$f|T(\varepsilon)_k(z) := f(\varepsilon(\overline{z}))j(\varepsilon,z)^{-k},$$

on la barra indica la conjugació complexa, llavors, per a tot nombre complex $a \in \mathbb{C}$, és $(af)|T(\varepsilon)_k = \overline{a}(f|T(\varepsilon)_k)$; és a dir, $T(\varepsilon)_k$ és un operador hermitià en $S_k(\Gamma_{\mathfrak{a}})$.

D'altra banda, en el cas en què $\mathfrak{a}$ sigui un ideal bilateral tal que $\mathrm{mcd}(D,\mathfrak{a}) = 1$, podem prendre $\varepsilon \equiv \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{\mathfrak{a}}$, i obtenim que $\varepsilon^2 \in \Gamma_{\mathfrak{a}}$ i que, per a tot $\alpha \in \Delta^*_{\mathfrak{a}}$, és $\varepsilon^{-1}\alpha\varepsilon \equiv \alpha \pmod{\mathfrak{a}}$. Això implica que és $T(\varepsilon)_k^2 = 1$ i que $T(\varepsilon)_k$ commuta amb tots els operadors $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k$.

Com a conseqüència d'aquestes propietats, els operadors $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k$ són tots hermitians respecte de la mètrica de Petersson i formen un anell commutatiu d'operadors normals; en conseqüència, obtenim el resultat següent.

6.4.15 Proposició. *Per a tot ideal bilateral $\mathfrak{a} \subseteq \mathcal{O}$ existeix una base de $S_k(\Gamma_{\mathfrak{a}})$ tal que tots els operadors $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k$, $\alpha \in \Delta_{\mathfrak{a}}^*$, són representats per matrius diagonals.* $\square$

6.4.16 Corol·lari. *Per a tot nombre natural parell k i tot element $\alpha \in \Delta$, les arrels característiques dels operadors $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k$ són nombres enters algebraics. A més a més, si $\mathfrak{a} = \mathcal{O}$, aquestes arrels característiques són nombres totalment reals.* $\square$

Finalment, en el cas que $\mathfrak{a} = \mathcal{O}$, observem que podem elegir una base de $S_k(\Gamma_{\mathfrak{a}})$ formada per elements invariants per a l'operador $T(\varepsilon)_k$; per a aquesta base, els operadors $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k$, $\alpha \in \Delta_{\mathfrak{a}}^*$, són representats per matrius de coeficients reals.

Suposem, ara, que B és un cos no commutatiu; és a dir, que l'àlgebra de quaternions B no és isomorfa a l'àlgebra de matrius $\mathrm{M}(2, \mathbb{Q})$.

Un procés d'adelització, que inclou considerar les adeles i les ideles de B, però no només aquestes, més l'elecció de mesures de Haar adequades i anàlisi harmònica en els grups de les adeles i de les ideles, més la fórmula de Selberg, més la fórmula de sumació de Poisson, més l'ús de transformades de Fourier, etcètera, permeten obtenir el teorema següent, en el qual només fem la descripció de l'equació funcional en el cas en què $\mathfrak{a} = \mathcal{O}$.

6.4.17 Teorema. *Siguin $\mathfrak{a} \subseteq \mathcal{O}$ un ideal bilateral tal que $\mathrm{mcd}(D, \mathfrak{a}) = 1$, i $k \geq 0$ un nombre enter. Posem*

$$H_k(s; \mathfrak{a}) := D^{s/2}(2\pi)^{-s}\Gamma(s) \sum_{\mathrm{mcd}(n,\mathfrak{a})=1} \mathcal{T}_k(n; \mathfrak{a})n^{-s}.$$

Llavors, $H_k(s; \mathfrak{a})$ és una funció holomorfa en tot $\mathbb{C}$, per a la qual se satisfà una certa equació funcional. Per al cas en què $\mathfrak{a} = \mathcal{O}$, una equació funcional es pot escriure en la forma

$$H_k(s; \mathcal{O}) = \Lambda H_k(k - s; \mathcal{O}),$$

on

$$\Lambda := (-1)^{k/2} \prod_{p|D} p^{k/2-1} \mathcal{T}_k(p; \mathcal{O})$$

és un nombre tal que $\Lambda^2 = 1$. $\square$

Aquest teorema és el punt de partida per a l'obtenció del següent; l'altre ingredient bàsic és la fórmula de congruència de què parlarem en les dues subseccions següents.

6.4.18 Teorema. *Siguin* B *una* $\mathbb{Q}$*-àlgebra de quaternions indefinida i* $\mathcal{O} \subseteq B$ *un ordre maximal. Siguin* $D := \mathrm{disc}(B) = \mathrm{disc}(\mathcal{O})$ *el discriminant de l'àlgebra i de l'ordre, i* $N \in \mathbb{Z}$, $N > 0$, *un nombre enter tal que* $\mathrm{mcd}(D, N) = 1$. *Considerem el grup de congruència*

$$\Gamma_N := \{\gamma \in \mathcal{O}^* : \mathrm{n}(\gamma) > 0, \gamma \equiv 1 \pmod{N\mathcal{O}}\}.$$

Llavors, existeix una corba algebraica llisa $X(D, \Gamma_N)$, *definida sobre* $\mathbb{Q}$, *anomenada corba de Shimura, tal que*

(a) *el cos de les funcions de* $X(D, \Gamma_N)$ *és isomorf al cos de les funcions automorfes respecte de* Γ_N.

(b) *la funció zeta de* $X(D, \Gamma_N)$ *sobre* $\mathbb{Q}$ *s'escriu en la forma*

$$\zeta(s; X(D, \Gamma_N)) = f(s)\zeta(s)\zeta(s-1)D(s)^{-1},$$

on $f(s)$ *és un producte de funcions racionals de* p^{-s}, *per a un conjunt finit de nombres primers* p, $\zeta(s)$ *és la funció zeta de Riemann, i*

$$D(s) = \det \left(\sum_{\mathrm{mcd}(n,N)=1} \mathcal{T}_2(n; N\mathcal{O}) n^{-s} \right). \square$$

Per tant, la funció zeta $\zeta(s; X(D, \Gamma_N))$ admet prolongació meromorfa a tot $\mathbb{C}$ i satisfà una certa equació funcional, deduïda de l'equació funcional per a $D(s)$.

6.4.4 Correspondències modulars

Recordem que, si C és una corba llisa, una correspondència pròpia de C és un divisor de $C \times C$ sense components de cap de les formes $x \times C$ ni $C \times x$, per a $x \in C$; i que les correspondències pròpies de C formen un anell, en el qual la permutació dels dos factors del producte cartesià $C \times C$ indueix un antiautomorfisme, $x \mapsto {}^t x$, anomenat involució de Rosati.

En interessa especialment el cas en què $C = X(D, \Gamma_N)$ és la corba de Shimura definida més amunt; notem que el cas $N = 1$ correspon a la corba $X(D, \Gamma)$. Per a qualsevol element $\alpha \in \Delta$, posem $\Gamma(\alpha) := \Gamma \cap \alpha^{-1}\Gamma\alpha$ i sigui $f_1 : \Gamma(\alpha)\backslash\mathcal{H} \longrightarrow X(D, \Gamma)$ la projecció canònica. D'altra banda, per a tot $z \in \mathcal{H}$ i tot $\alpha \in \Delta$, és $\alpha\Gamma(\alpha)z \subseteq \Gamma\alpha z$; per tant, obtenim immediatament una altra aplicació $f_2 : \Gamma(\alpha)\backslash\mathcal{H} \longrightarrow X(D, \Gamma)$.

6.4.19 Proposició. *Per a tot element $\alpha \in \Delta$, la imatge de $\Gamma(\alpha)\backslash\mathcal{H}$ en $X(D, \Gamma) \times X(D, \Gamma)$ per l'aplicació (f_1, f_2) és una correspondència pròpia, que només depèn de la classe doble $\Gamma\alpha\Gamma$.* $\square$

6.4.20 Definició. Aquesta correspondència s'anomena la correspondència modular, i l'escriurem en la forma $\mathrm{md}(\Gamma\alpha\Gamma)$.

6.4.21 • L'aplicació $\Gamma\alpha\Gamma \mapsto \mathrm{md}(\Gamma\alpha\Gamma)$ indueix un morfisme d'anells de l'anell de Hecke $R(\Gamma, \Delta)$ en l'anell de les correspondències modulars pròpies, definides sobre $\mathbb{Q}$, de la corba de Shimura.

• Per a tot nombre primer p, es té que la correspondència modular associada a l'element $T(p, p)$ és la identitat.

• Si $\Gamma\alpha\Gamma = \biguplus_i \Gamma\alpha_i$, i si pr indica la projecció canònica de $\mathcal{H}$ en $X(D, \Gamma_N)$, es té que

$$\mathrm{md}(\mathrm{pr}(z)) = \sum_i \mathrm{pr}(\alpha_i(z)).$$

6.4.5 Fórmula de congruència

6.4.22 Proposició. *Siguin red_p la reducció mòdul un nombre primer p que no divideixi el discriminant D de l'àlgebra de quaternions i que* *sigui un primer de bona reducció;* $\mathrm{red}_p(T(p))$ *la reducció mòdul* p *de l'operador* $T(p)$ *vist com a correspondència sobre* $\mathrm{red}_p(X(D,\Gamma))$*; i* π_p *la correspondència de Frobenius de* $\mathrm{red}_p(X(D,\Gamma))$*; és a dir, el graf de l'aplicació que eleva a la potència* p *les coordenades homogènies dels punts. Se satisfà la fórmula de congruència:*

$$\mathrm{red}_p(T(p)) = \pi_p + {}^t\pi_p. \; \Box$$

Per al cas més general de la corba $X(D,\Gamma_N)$, la fórmula de congruència no és tan senzilla; de fet, la demostració presenta algunes complicacions tècniques i cal introduir un automorfisme convenient Y_N de la corba $X(D,\Gamma_N)$ que deixa invariants les fibres de $X(D,\Gamma_N) \longrightarrow X(D,\Gamma)$.

En aquest cas, la fórmula de congruència s'escriu de la forma

$$\begin{aligned} \mathrm{red}_p(T(p)) &= \pi_p + {}^t\pi_p \circ \mathrm{red}_p(Y_p), \\ {}^t\pi_p \circ \mathrm{red}_p(Y_p) &= {}^t\mathrm{red}_p(Z) \circ {}^t\pi_p \circ \mathrm{red}_p(Z), \end{aligned}$$

on Z és un automorfisme convenient de $X(D,\Gamma_N)$ definit sobre $\mathbb{Q}$.

6.5 Reducció de les corbes de Shimura

Per als primers de bona reducció de les corbes de Shimura que apareixen a la fórmula de congruència, cal tenir en compte el teorema de Morita dels primers de bona reducció.

6.5.1 • Mantinguem la hipòtesi que la $\mathbb{Q}$-àlgebra de quaternions indefinida B sigui un cos no commutatiu; és a dir, que no sigui isomorfa a l'àlgebra de matrius $\mathrm{M}(2,\mathbb{Q})$. Siguin $\mathcal{O}$ un ordre maximal i D el seu discriminant.

• Siguin G el grup algebraic, definit sobre $\mathbb{Q}$, tal que $G_{\mathbb{Q}} = B^*$; i G_A, l'adelització de G.

• Notem que $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}(2,\mathbb{R})$, de manera que la projecció en ∞ de G_A és $\mathrm{M}(2,\mathbb{R})$; per tant, podem considerar $G_{A,+} := \{x \in G_A : \det x_\infty > 0\}$.

• Siguin $G_{\infty,+} := \mathrm{GL}^+(2,\mathbb{R})$ la part arquimediana, i G_0 la part finita de $G_{A,+}$; i $G_{\mathbb{Q},+} := G_{A,+} \cap G_{\mathbb{Q}} = G_{A,+} \cap B^*$.

• Sigui $\mathcal{S}$ la família dels subgrups $S \subseteq G_{A,+}$ tals que S és de la forma $S = G_{\infty,+} \cdot S_0$, on S_0 és qualsevol subgrup compacte i obert de G_0.

• Per a tot $S \in \mathcal{S}$, sigui $\Gamma_S := S \cap G_{\mathbb{Q},+} \subseteq \mathrm{GL}(2, \mathbb{R})$. Així, Γ_S actua en el semiplà $\mathcal{H}$ i l'espai quocient $\Gamma_S \backslash \mathcal{H}$ defineix una corba completa i no singular.

• Per teoria de cossos de classes, i si $\mathrm{n} : B^* \longrightarrow \mathbb{Q}^*$ és la norma reduïda, al subgrup $\mathrm{n}(S)\mathbb{Q}^* \subseteq \mathbb{Q}_A^*$ de les ideles de $\mathbb{Q}$ li correspon una extensió abeliana de $\mathbb{Q}$, que denotarem per $k_S|\mathbb{Q}$.

• En aquesta situació (i, més generalment, en una situació anàloga on $\mathbb{Q}$ es pot canviar per un cos de nombres totalment real, F, i B per una F-àlgebra de quaternions que sigui un cos i tal que $B \otimes_{\mathbb{Q}} \mathbb{R}$ sigui el producte d'una sola còpia de $\mathrm{M}(2, \mathbb{R})$ i, la resta, còpies dels quaternions de Hamilton), podem parlar de la corba de Shimura X_S; és una corba algebraica llisa, definida sobre k_S, i isomorfa, a nivell de punts complexos, a $\Gamma_S \backslash \mathcal{H}$.

6.5.2 Teorema. *Amb les notacions i les hipòtesis anteriors, i per a tot $S \in \mathcal{S}$, sigui P_S el conjunt dels ideals primers $\mathfrak{q}$ de k_S tals que $\mathfrak{q} \nmid D$ i existeix $x_p \in G_{\mathbb{Q},+}$ per al qual $S \subseteq x_p^{-1}\mathcal{O}_p^* x_p$, on $p\mathbb{Z} := \mathfrak{q} \cap \mathbb{Q}$, i $\mathcal{O}_p$ és la compleció p-àdica de $\mathcal{O}$. Llavors,*

(a) *P_S és un conjunt d'ideals primers de $\mathcal{O}_{k_S}$, tots llevat d'una quantitat finita.*

(b) *La corba de Shimura X_S admet un model enter sobre $\mathcal{O}_{k_S}$ que té bona reducció per a tot $\mathfrak{q} \in P_S$.* $\square$

6.6 El teorema de comparació

Acabarem l'exposició amb l'enunciat d'un teorema de comparació aplicable a les funcions zeta associades a corbes de Shimura que corresponen a àlgebres de quaternions de discriminants diferents i a ordres de nivells diferents en aquestes àlgebres.

Fixem notacions.

• Siguin D, D', p nombres enters, p primer, tals que $DD'p$ sigui lliure de quadrats.

• Siguin B una $\mathbb{Q}$-àlgebra de quaternions de discriminant D, i $\mathcal{O} \subseteq B$ un ordre d'Eichler de nivell D' cf. Rio, capítol 1.

• Siguin B' una $\mathbb{Q}$-àlgebra de quaternions de discriminant D, i $\mathcal{O}' \subseteq B'$ un ordre d'Eichler de nivell $D'p$.

• Siguin B'' una $\mathbb{Q}$-àlgebra de quaternions de discriminant Dp, i $\mathcal{O}'' \subseteq B''$ un ordre d'Eichler de nivell D'.

• Notem que B i B' són àlgebres del mateix discriminant i que el discriminant de B'' té exactament un divisor primer més. Per tant, si B, B' són indefinides, llavors B'' és definida; i, recíprocament, si B, B' són definides, llavors B'' és indefinida.

• Si considerem el grup de les ideles de B, $\mathcal{I}$, i el grup de les $\mathcal{O}$-unitats de $\mathcal{I}$, $\mathcal{U}$, per adelització de les nocions establertes en les seccions anteriors, podem parlar, per a tot nombre enter $k > 0$, d'un espai de funcions automorfes de pes k i d'una representació $\mathcal{T}_k$ de l'anell de Hecke $R(\mathcal{U}, \mathcal{I})$ en aquest espai.

• En conseqüència, podem parlar de la sèrie de Dirichlet

$$\mathcal{D}(s) := \sum_{n \geq 1} \mathcal{T}_k(T(n)) n^{-s};$$

aquesta sèrie és convergent per a $\Re(s) \gg 0$, i admet un producte d'Euler de la forma

$$\mathcal{D}(s) = \prod_{\ell} \mathcal{E}_\ell(s).$$

• Com que les sèries i els factors depenen de l'àlgebra i de l'ordre, escriurem $\mathcal{D}(B, \mathcal{O}; s)$ per a designar aquesta dependència.

• Escriurem $\mathcal{D}'(B, \mathcal{O}; s) := \prod_{\ell \neq p} \mathcal{E}_\ell(B, \mathcal{O}; s)$ el producte de tots els factors d'Euler, llevat el que correspon al primer p, fixat a l'inici.

• Un cop fixada una base de l'espai de representació, és a dir, de l'espai de funcions automorfes, la funció $\mathcal{D}(B, \mathcal{O}; s)$ pren valors en un espai de matrius. Per a $a, b \in \mathbb{Z}$, $a, b \geq 0$, i per a matrius X, Y, escriurem $aX \oplus bY$ per a designar la suma directa de a còpies de la matriu X i b còpies de la matriu Y.

6.6.1 Teorema. (Eichler, Shimizu) *Amb aquestes notacions i hipòtesis, se satisfà que*

(a) $\mathcal{D}'(B', \mathcal{O}'; s) = \mathcal{D}'(B'', \mathcal{O}''; s) \oplus 2\mathcal{D}'(B, \mathcal{O}; s)$.

(b) $\mathcal{D}(B, \mathcal{O}; s)$ *només depèn de* D *i de* D'*, però no de l'àlgebra de quaternions de discriminant* D *ni de l'ordre de nivell* D' *que considerem.* $\square$

Bibliografia

[Bor65] A. Borel, *Opérateurs de Hecke et fonctions zêta*, Séminaire Bourbaki, Vol. 9, exp.307, Soc. Math. France, 1965, pp. 441–463.

[Mor81] Y. Morita, *Reduction mod $\mathfrak{p}$ of Shimura curves*, Hokkaido Math. J. **10** (1981), num. 2, 209–238.

[Shi61] G. Shimura, *On the zeta-functions of the algebraic curves uniformized by certain automorphic functions*, J. Math. Soc. Japan **13** (1961), num. 3, 275–331.

[Shi65] H. Shimizu, *On zeta functions of quaternion algebras*, Ann. of Math. **81** (1965), 166–193.

[Shi67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. **85** (1967), 58–159.