

# Endomorphisms of Jacobians of Modular Curves

## 1. Introduction

**Let**  $\Gamma$  be a congruence group with  $\Gamma_1(N) \leq \Gamma \leq \Gamma_0(N)$ ,

$X_\Gamma = \Gamma \backslash \mathfrak{H}^*$  be the associated modular curve,

$X = X_{\Gamma, \mathbb{Q}}$  its canonical model over  $\mathbb{Q}$ ,

$J = J_X$ , its Jacobian variety of dimension  $g_X$ ,

$\mathbb{E} = \text{End}_{\mathbb{Q}}^0(J) = \text{End}_{\mathbb{Q}}(J) \otimes \mathbb{Q}$ , its endomorphism algebra.

**Problem 1:** Determine  $\mathbb{E}$ , i.e. find explicit generators for  $\mathbb{E}$ .

**Recall:** The Hecke operators (correspondences)  $T_n$  on  $X$  give rise to a commutative subalgebra called the Hecke algebra,

$$\mathbb{T} = \langle T_n : n \geq 1 \rangle \subset \mathbb{E}.$$

It contains the (semi-simple) subalgebra

$$\mathbb{T}' = \langle T_n : n \geq 1, (n, N) = 1 \rangle \subset \mathbb{T} \subset \mathbb{E}.$$

Then we have

$$\begin{aligned} \dim_{\mathbb{Q}} \mathbb{T} &= \dim J, && \text{(Shimura)} \\ \dim_{\mathbb{Q}} \mathbb{T}' &= \#\mathcal{N}(\Gamma), && \text{(Atkin-Lehner)} \end{aligned}$$

where  $\mathcal{N}(\Gamma) \subset S_2(\Gamma)$  denotes the set of normalized newforms of weight 2 of all levels, i.e. if  $f \in \mathcal{N}(\Gamma)$ , then  $f$  is a normalized newform of level  $N_f | N$ .

**Note:** If  $N = p$  is prime, then by Ribet we have that  $\mathbb{T}' = \mathbb{T} = \mathbb{E}$ , but in general these three algebras are different.

**Reason:** For each pair  $(M, d)$  with  $Md|N$ , there is a **degeneracy morphism (Mazur)**

$$B_{M,d} : X \rightarrow X_M,$$

where  $X_M$  is the corresponding curve of level  $M$ , and these give rise to new endomorphisms

$$D_{M,d} := B_{M,1}^* \circ (B_{M,d})_*, \quad {}^t D_{M,d} := B_{M,d}^* \circ (B_{M,1})_* \in \text{End}(J_X).$$

**Theorem 1:**  $\mathbb{E} = \langle \mathbb{T}', \{D_{M,d}, {}^t D_{M,d} : Md|N\} \rangle$ .

**Corollary:**  $Z(\mathbb{E}) = \mathbb{T}'$ .

**Thus:**  $\mathbb{T}'$  has an **intrinsic** interpretation.

**Remark:** The above results also apply to **other** modular curves such as the **principal modular curve**

$$X(N) = X_{\Gamma(N), \mathbb{Q}},$$

where  $\Gamma(N) = \text{Ker}(\text{SL}_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/N\mathbb{Z}))$ . Indeed, since  $\Gamma(N)$  is conjugate to the group

$$\Gamma[N] := \beta_N \Gamma(N) \beta_N^{-1} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a \equiv d \equiv 1 \pmod{N}, c \equiv 0 \pmod{N^2} \right\},$$

(where  $\beta_N = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$ ), we have  $\mathbb{Q}$ -isomorphisms

$$X(N) \simeq X_{\Gamma[N], \mathbb{Q}} \quad \text{and} \quad J(N) \simeq J_{X_{\Gamma[N], \mathbb{Q}}}$$

which are compatible with the action of the **Hecke algebras**. Note, however, that  $\Gamma[N]$  has level  $N^2$ , i.e.

$$\Gamma_1(N^2) \leq \Gamma[N] \leq \Gamma_0(N).$$

**Problem 2:** For each  $\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times$ , determine  $\dim_{\mathbb{Q}} \mathbb{T}_\varepsilon$ , where

$$\mathbb{T}_\varepsilon = \sum_{a^2 n \equiv \varepsilon (N)} \mathbb{Q}T_{a,n}.$$

Here  $T_{a,n} = T(a, a)T_n$ , where  $T(a, a) = \langle a \rangle$  denotes the **diamond operator**. Note that by definition we have

$$\sum_{\varepsilon} \mathbb{T}_\varepsilon = \mathbb{T}'.$$

**Theorem 2:** If  $X = X(N)$ , then

$$\mathbb{T}' = \bigoplus_{\varepsilon} \mathbb{T}_\varepsilon.$$

**Remarks:** 1) Thus, we might expect that

$$\dim \mathbb{T}_\varepsilon \stackrel{?}{=} \frac{1}{\phi(N)} \dim \mathbb{T}' = \frac{1}{\phi(N)} \#\mathcal{N}(\Gamma_N).$$

This is almost true, but the presence of **CM elliptic curves** in  $J(N)$  makes the actual result a bit more complicated. (See **Theorem 5** below.)

2) As we shall see,  $\mathbb{T}_\varepsilon$  also has an **intrinsic** interpretation in terms of the algebra  $\mathbb{M}$  of all **modular correspondences**.

3) The group  $\mathbb{T}_\varepsilon$  is closely related to the **Neron-Severi group**  $NS(Z_{N,\varepsilon})$  of the **modular diagonal quotient surface** (MDQS)

$$Z_{N,\varepsilon} = (X(N) \times X(N))/\Delta_\varepsilon,$$

where  $\Delta_\varepsilon \leq G_N \times G_N$  is a certain (twisted) **diagonal subgroup** of the group  $G_N = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$ .

## 2. The Degeneracy Algebra $\mathbb{D}$

**Recall:** The algebra  $\mathbb{E}$  acts **faithfully** on the  $\mathbb{Q}$ -vector spaces

$$H^0(J, \Omega_J^1) \simeq H^0(X, \Omega_X^1) \simeq S_2(\Gamma, \mathbb{Q}),$$

where  $S_2(\Gamma, \mathbb{Q}) =$  space of all weight 2 **cuspidal forms** on  $\Gamma$  with  $\mathbb{Q}$ -rational Fourier expansions. Thus:

$$\mathbb{E}_{\mathbb{C}} = \mathbb{E} \otimes \mathbb{C} \quad \text{acts faithfully on } S := S_2(\Gamma).$$

**Aim:** Study the action of suitable subalgebras of  $\mathbb{E}_{\mathbb{C}}$  on  $S$ .

**Basic Fact (Atkin-Lehner Theory):** The **isotypic** decomposition of  $S$  as a  $\mathbb{T}'_{\mathbb{C}}$ -module is given by

$$(1) \quad S = \bigoplus_{f \in \mathcal{N}(\Gamma)} S_f, \quad \text{where } S_f = \sum_{d|(N/N_f)} \mathbb{C}f|\beta_d.$$

Note that  $f|\beta_d(z) = f(dz)$  and that hence

$$n_f := \dim S_f = \sigma_0(N/N_f).$$

**Definition:** The **degeneracy algebra** is

$$\mathbb{D} = \langle \mathbb{T}', \{D_{M,d}, {}^t D_{M,d} : Md|N\} \rangle \subset \mathbb{E}.$$

**Remark:** Recall from the introduction that  $D_{M,d} = B_{M,1}^* \circ (B_{M,d})_*$  and  ${}^t D_{M,d} = B_{M,d}^* \circ (B_{M,1})_*$ . Since

$$\begin{aligned} f'|B_{M,d}^* &= f'|\beta_d, & \text{if } f' \in S_2(\Gamma_M) \subset S, \\ f|(B_{M,d})_* &= tr_M(f|\beta_d), & \text{if } f \in S = S_2(\Gamma), \end{aligned}$$

we see that

$$f|D_{M,d} = tr_M(f|\beta_d) \quad \text{and} \quad f|{}^t D_{M,d} = tr_M(f)|\beta_d, \quad \text{if } f \in S.$$

**Theorem 3:** Each  $S_f$  is an **irreducible**  $\mathbb{D}_{\mathbb{C}}$ -module, and every irreducible  $\mathbb{D}_{\mathbb{C}}$ -module is isomorphic to a **unique**  $S_f$ . Thus  $Z(\mathbb{D}_{\mathbb{C}}) = \mathbb{T}'_{\mathbb{C}}$  and  $\mathbb{D}_{\mathbb{C}} = C_S(\mathbb{T}'_{\mathbb{C}})$ , the **centralizer** of  $\mathbb{T}'$  in  $\text{End}_{\mathbb{C}}(S)$ .

**Remark:** There is an analogous statement for the space  $S_k(\Gamma)$  of cusp forms of **arbitrary** weight  $k$ .

**Proof (Sketch).** It is easy to verify that each  $S_f$  is a  $\mathbb{D}_{\mathbb{C}}$ -module, and hence the Atkin-Lehner decomposition (1) is a decomposition of  $\mathbb{D}_{\mathbb{C}}$ -modules.

Suppose  $S_f$  were reducible. Then  $S_f = V_1 \oplus V_2$  because  $\mathbb{D}_{\mathbb{C}}$  is **semi-simple** (being  $*$ -closed). Now

$$tr := tr_{N_f} : S_f \rightarrow S_2(\Gamma_{N_f}) \cap S_f = \mathbb{C}f \quad (\text{by A-L theory})$$

is surjective, so  $tr(V_i) \neq 0$  for some  $i = 1, 2$  and  $\exists g \in V_i$  such that  $tr(g) = f$ . Thus  $g|D_{N_f, d} = f|\beta_d$ , for all  $d|N/N_f$ , and hence  $V_i = S_f$ . This means that  $S_f$  is an irreducible  $\mathbb{D}_{\mathbb{C}}$ -module.

Thus, by Wedderburn and the Atkin-Lehner decomposition (1) we have

$$\mathbb{D}_{\mathbb{C}} \simeq \prod_{f \in \mathcal{N}(\Gamma)} M_{n_f}(\mathbb{C}),$$

and so  $\dim Z(\mathbb{D}_{\mathbb{C}}) = \#\mathcal{N}(\Gamma) = \dim \mathbb{T}'_{\mathbb{C}}$ . Since  $\mathbb{T}'_{\mathbb{C}} \subset Z(\mathbb{D}_{\mathbb{C}})$ , we see that  $\mathbb{T}'_{\mathbb{C}} = Z(\mathbb{D}_{\mathbb{C}})$ . The rest of the assertions follow easily.

**Note:**  $S$  has **multiplicity 1** as a  $\mathbb{D}_{\mathbb{C}}$ -module!

### 3. The Structure of $\mathbb{E} = \text{End}_{\mathbb{Q}}^0(J)$

**Fact (Shimura construction):** Each  $f \in \mathcal{N}(\Gamma)$  defines an abelian subvariety (or quotient)  $A_f/\mathbb{Q}$  of  $J$  of dimension

$$\dim A_f = [K_f : \mathbb{Q}], \quad \text{where } K_f = \mathbb{Q}(\{a_n(f)\}).$$

Here the  $a_n(f)$ 's are the Fourier coefficients of  $f = \sum a_n(f)q^n$ .

**Theorem 4 (Ribet)** a)  $\text{End}_{\mathbb{Q}}^0(A_f) \simeq K_f$ , for all  $f \in \mathcal{N}(\Gamma)$ .

b) If  $f, g \in \mathcal{N}(\Gamma)$ , then  $A_f \sim A_g \Leftrightarrow f = g^\sigma, \sigma \in G_{\mathbb{Q}}$ , where  $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  denotes the absolute Galois group.

**Remark:** Theorem 4a) was proved in Ribet's 1980 paper, and part b) can be proved with similar methods (see a recent preprint of M. Baker et al.)

**Corollary:** We have the isogeny relation

$$(2) \quad J_X \sim \prod_{f \in \mathcal{N}(\Gamma)/G_{\mathbb{Q}}} A_f^{n_f},$$

and hence

$$\mathbb{E} \simeq \prod_{f \in \mathcal{N}(\Gamma)/G_{\mathbb{Q}}} M_{n_f}(K_f).$$

**Proof of Theorem 1:** Since  $\mathbb{D} \subset \mathbb{E}$ , we have  $Z(\mathbb{E}) \subset C_S(\mathbb{E}) \subset C_S(\mathbb{D}) = \mathbb{T}'$  (Theorem 3). But by the above Corollary we have  $\dim Z(\mathbb{E}) = \#\mathcal{N}(\Gamma) = \dim \mathbb{T}'$ , and so  $Z(\mathbb{E}) = C_S(\mathbb{E}) = \mathbb{T}'$ . Thus  $\mathbb{D} = \mathbb{E}$  by the double centralizer theorem.

## 4. Examples

**Example 1:**  $X = X_0(p^2)$ ,  $p$  a prime.

Let  $\eta = B_{p,1} : X_0(p^2) \rightarrow X_0(p)$  be the **usual** covering map and  $\eta' = B_{p,p} : X_0(p^2) \rightarrow X_0(p)$  the **twisted** covering, and put  $\tau = \eta^* \circ \eta_*$ ,  $\tau' = (\eta')^* \circ \eta'_*$ . Then **Theorem 1** (+ a refinement) gives

$$\mathbb{E} = \langle \mathbb{T}', \tau, T_p, {}^tT_p \rangle = \langle \mathbb{T}', \tau, \tau' \rangle.$$

Indeed,  $\tau = D_{p,1}$ ,  $T_p = {}^tD_{p,p}$ , and  ${}^tT_p = D_{p,p}$ . Moreover,

$$\begin{aligned} \dim \mathbb{T}' &= g_0(p^2) - g_0(p) \\ \dim \mathbb{T} &= g_0(p^2) \\ \dim \mathbb{E} &= g_0(p^2) + 2g_0(p) \end{aligned}$$

where  $g_0(g^k) = g_{X_0(p^k)}$  denotes the genus of the curve  $X_0(g^k)$ .

**Example 2:**  $X = X(p)$ ,  $p$  a prime.

Let  $\eta : X(p) \rightarrow X^1(p)$  and  $\eta' : X(p) \rightarrow X_1(p)$  be the usual covering maps, and put  $\tau = \eta^* \circ \eta_*$ ,  $\tau' = (\eta')^* \circ \eta'_*$ . Then **Theorem 1** (+ a refinement) gives

$$\mathbb{E} = \langle \mathbb{T}', \tau, T_p, {}^tT_p \rangle = \langle \mathbb{T}', \tau, \tau' \rangle.$$

because we have  $\tau = D_{p,1}$ ,  $T_p = {}^tD_{p,p}$ , and  ${}^tT_p = D_{p,p}$  via the isomorphism  $X(p) \simeq X[p]$ . Moreover,

$$\begin{aligned} \dim \mathbb{T}' &= g(p) - g_1(p) \\ \dim \mathbb{T} &= g(p) \\ \dim \mathbb{E} &= g(p) + 2g_1(p) \end{aligned}$$

where  $g(p) = g_{X(p)}$  and  $g_1(p) = g_{X_1(p)}$ .

## 5. CM-forms and the Dimension of $\mathbb{T}_\varepsilon$

**Notation:** Let  $f, g \in \mathcal{N}(\Gamma)$ . If  $\chi$  is a Dirichlet character with conductor  $\text{cond}(\chi) | N$ , then we write

$$f_\chi \sim g \Leftrightarrow \chi(n)a_n(f) = a_n(g), \forall n \geq 1, (n, N) = 1.$$

**Definition:**  $f \in \mathcal{N}(\Gamma)$  is called a CM-form if  $f_\theta \sim f$ , for some Dirichlet character  $\theta \neq 1$ .

Let  $\mathcal{N}(\Gamma)^{CM} \subset \mathcal{N}(\Gamma)$  denote set of all CM-forms on  $\Gamma$ .

**Remarks:** 1) If  $f_\theta \sim f$ ,  $\theta \neq 1$ , then  $\theta^2 = 1$  and  $\theta = \theta_f$  is uniquely determined by  $f$ .

2)  $\#\mathcal{N}(\Gamma)^{CM}$  can be calculated explicitly in terms of class numbers of imaginary quadratic fields. (Shimura)

3)  $f \in \mathcal{N}(\Gamma)^{CM} \Leftrightarrow A_f \otimes \mathbb{C} \sim E^m$ , where  $E$  is a CM elliptic curve. (Shimura, Ribet)

**Notation:** If  $f \in \mathcal{N}(\Gamma)$ , let  $\lambda_f : \mathbb{T}' \rightarrow \mathbb{C}$  denote its associated character, i.e.  $\lambda_f$  is given by

$$f|T = \lambda_f(T)f, \quad \text{for all } T \in \mathbb{T}'.$$

Note that we have

$$(3) \quad \lambda_f(T_{a,n}) = \chi_f(a)a_n(f),$$

where  $\chi_f : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  denotes the Nebentypus character of  $f$ .

**Observation 1:** If  $f_\chi \sim g$ , where  $\text{cond}(\chi)|N$ , then by (3) we have

$$(4) \quad \lambda_g(T) = \chi(\varepsilon)\lambda_f(T), \quad \text{for all } T \in \mathbb{T}_\varepsilon.$$

In particular, if  $f \in \mathcal{N}(\Gamma)^{CM}$  and  $\theta_f(\varepsilon) \neq 1$ , then

$$(5) \quad \lambda_f(T) = 0, \quad \text{for all } T \in \mathbb{T}_\varepsilon.$$

**Notation:** If  $f, g \in \mathcal{N}(\Gamma)$ , then we write

$$f \approx g \quad \Leftrightarrow \quad f_\chi \sim g, \text{ for some } \chi \text{ with } \text{cond}(\chi)|N.$$

Moreover, for  $\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times$  put

$$\mathcal{N}_\varepsilon(\Gamma) = \{f \in \mathcal{N}(\Gamma) : f \notin \mathcal{N}(\Gamma)^{CM} \text{ or } f \in \mathcal{N}(\Gamma)^{CM} \text{ and } \theta_f(\varepsilon) = 1\}.$$

**Observation 2:** We have

$$(6) \quad \dim \mathbb{T}_\varepsilon \leq \#\mathcal{N}_\varepsilon(\Gamma)/\approx .$$

[Indeed, let  $\underline{f} = \{f_1, \dots, f_r\}$  be a system of representatives of  $\mathcal{N}_\varepsilon(\Gamma)/\approx$ , and consider the map

$$\lambda_{\underline{f}} : \mathbb{T}_\varepsilon \rightarrow \mathbb{C}^r$$

defined by  $\lambda_{\underline{f}}(T) = (\lambda_{f_1}(T), \dots, \lambda_{f_r}(T))$ . Now  $\lambda_{\underline{f}}$  is injective, for if  $\lambda_{\underline{f}}(T) = 0$ , then by (4), (5) we have  $\lambda_f(T) = 0$ , for all  $f \in \mathcal{N}(\Gamma)$ , and so  $T = 0$ . This proves (6).]

**Theorem 5:** We have

$$\dim \mathbb{T}_\varepsilon = \#\mathcal{N}_\varepsilon(\Gamma)/\approx .$$

**Remark:** By **Observation 2** and a **reduction step**, it is enough to verify Theorem 5 for  $\Gamma = \Gamma(N)$ .

**Observation 3:** Let  $\Gamma = \Gamma(N)$ , and let  $\chi \in \widehat{Z}_N$ , where  $Z_N = (\mathbb{Z}/N\mathbb{Z})^\times$ . Then for every  $f \in \mathcal{N}(\Gamma)$  there is a **unique**  $f^\chi \in \mathcal{N}(\Gamma)$  such that  $f^\chi \sim f$ .

Thus, the group  $\widehat{Z}_N$  acts on the sets  $\mathcal{N}(\Gamma)$  and  $\mathcal{N}_\varepsilon(\Gamma)$ , and the equivalence classes  $\mathcal{N}(\Gamma)/\approx$  are the  $\widehat{Z}_N$ -orbits under this action. Therefore

$$\#\mathcal{N}(\Gamma)/\approx = \frac{1}{\phi(N)} (\#\mathcal{N}(\Gamma) + \#\mathcal{N}(\Gamma)^{CM}),$$

and hence (exercise!)

$$(7) \quad \sum_{\varepsilon} \#\mathcal{N}_\varepsilon(\Gamma)/\approx = \#\mathcal{N}(\Gamma).$$

**Proof of Theorems 5 and 2:** We have

$$\#\mathcal{N}(\Gamma) = \dim \mathbb{T}' \leq \sum_{\varepsilon} \dim \mathbb{T}_\varepsilon \stackrel{(6)}{\leq} \sum_{\varepsilon} \#\mathcal{N}_\varepsilon(\Gamma)/\approx \stackrel{(7)}{=} \#\mathcal{N}(\Gamma),$$

and so we must have equality throughout. Thus (6) is an equality (**Theorem 5**) and the sum  $\mathbb{T}' = \sum \mathbb{T}_\varepsilon$  is a direct sum (**Theorem 2**).

## 6. The Algebra $\mathbb{M}$ of Modular Correspondences

**Fact (Klein, Gierster, Hurwitz, ... )** Each  $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$  defines a modular correspondence

$$T_\Gamma(\alpha) \subset X_\Gamma \times X_\Gamma$$

and hence induces an endomorphism  $f_\alpha \in \mathrm{End}_{\mathbb{C}}(X_\Gamma)$ . We call the  $\mathbb{Q}$ -algebra  $\mathbb{M} \subset \mathrm{End}_{\mathbb{C}}^0(X_\Gamma)$  generated by the  $f_\alpha$ 's the algebra of modular correspondences.

**Remarks:** 1) As Shimura explains in his book, the additive group generated by the  $f_\alpha$ 's forms a ring  $\mathbb{M}_{\mathbb{Z}} \subset \mathrm{End}_{\mathbb{C}}(X_\Gamma)$ , and hence  $\mathbb{M} = \mathbb{M}_{\mathbb{Z}} \otimes \mathbb{Q}$ .

2) The Hecke correspondence  $T_p$  ( $p$  any prime) is given by  $T_p = f_{\alpha_p}$ , where  $\alpha_p = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ .

3) It turns out (see the example below) that

$$\mathbb{M} \subset \mathbb{E}' := \mathrm{End}_{K_N}^0(X_\Gamma), \quad \text{where } K_N = \mathbb{Q}(\zeta_N).$$

Thus, the group  $Z_N \simeq \mathrm{Gal}(K_N/\mathbb{Q})$  induces a natural Galois action on  $\mathbb{E}'$  and on  $\mathbb{M}$  via

$$\tau_a(f) = \tilde{\tau}_a \circ f \circ \tilde{\tau}_a^{-1}, \quad a \in Z_N,$$

where  $\tilde{\tau}_a$  is the lift of  $\tau_a \in \mathrm{Gal}(K_N/\mathbb{Q})$  to  $J \otimes K_N$ .

**Example:** Let  $\Gamma = \Gamma(N)$ . Then

$$\mathbb{M} = \langle \mathbb{T}, G_N \rangle, \quad \text{where } G_N = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\},$$

viewed as acting as a group of automorphisms on  $X(N)$  and hence on  $J(N)$ .

The **Galois action** of  $Z_N$  on  $\mathbb{M}$  is given by

$$\begin{aligned}\tau_a(T) &= T, & \text{if } T \in \mathbb{T}, \\ \tau_a(g) &= \bar{\beta}_a g \bar{\beta}_a^{-1}, & \text{if } g \in G_N,\end{aligned}$$

where  $\bar{\beta}_a = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ .

**Observation:** In the above situation we have

$$(8) \quad Tg = \tau_\varepsilon(g)T, \quad \text{for all } T \in \mathbb{T}_\varepsilon, g \in G_N.$$

**Notation:** Let  $\rho : \mathbb{M}_{\mathbb{C}} := \mathbb{M} \otimes \mathbb{C} \rightarrow \text{End}_{\mathbb{C}}(S)$  be the **representation** afforded by  $S = S_2(\Gamma)$  (viewed as an  $\mathbb{M}_{\mathbb{C}}$ -module), and put

$$\text{End}_{\mathbb{M},\varepsilon}(S) = \{f \in \text{End}(S) : f\rho(x) = \rho(\tau_\varepsilon(x))f, \text{ for all } x \in \mathbb{M}\}.$$

Thus  $\text{End}_{\mathbb{M},\varepsilon}(S) = \text{Hom}_{\mathbb{M}_{\mathbb{C}}}(S, S^{(\tau_\varepsilon)})$ , where  $S^{(\tau_\varepsilon)}$  denotes the  $\mathbb{M}_{\mathbb{C}}$ -module  $S$  with action **twisted** by the automorphism  $\tau_\varepsilon$ .

**Theorem 6:**  $\rho(\mathbb{T}_\varepsilon \otimes \mathbb{C}) = \text{End}_{\mathbb{M},\varepsilon}(S)$ .

**Proof:** The relation (8) shows that  $\rho(\mathbb{T}_\varepsilon \otimes \mathbb{C}) \subset \text{End}_{\mathbb{M},\varepsilon}(S)$ , and so by **Theorem 5** it is enough to show that  $\text{End}_{\mathbb{M},\varepsilon}(S)$  has the right dimension. This follows from:

**Theorem 7:** For each  $f \in \mathcal{N}(\Gamma)$ , the space  $V(f) := \sum_{g \approx f} S_g$  is an **irreducible**  $\mathbb{M}_{\mathbb{C}}$ -module, and so

$$S = \bigoplus_{f \in \mathcal{N}(\Gamma)/\approx} V(f)$$

is the  **$\mathbb{M}_{\mathbb{C}}$ -module decomposition** of  $S$ . Moreover,

$$S_f^{(\tau_\varepsilon)} \not\cong S_f \quad \Leftrightarrow \quad f \in \mathcal{N}(\Gamma)^{CM} \text{ with } \theta_f(\varepsilon) \neq 1.$$

## 7. Application to $NS(Z_{N,\varepsilon})$

**Definition:** The modular diagonal quotient surface of type  $(N, \varepsilon)$  is the quotient surface

$$Z_{N,\varepsilon/\mathbb{C}} = (X(N)_{/\mathbb{C}} \times X(N)_{/\mathbb{C}}) / \Delta_{N,\varepsilon}$$

where  $\Delta_{N,\varepsilon} = \{(g, \tau_\varepsilon(g)) : g \in \Gamma_N\} \leq G_N \times G_N$ .

**Note:**  $Z_{N,\varepsilon/\mathbb{C}}$  has a canonical model  $Z_{N,\varepsilon}$  over  $\mathbb{Q}$ , even though the automorphism group is only defined over  $K_N = \mathbb{Q}(\zeta_N)$ . In addition, the quotient map

$$\Psi : X(N) \times X(N) \rightarrow Z_{N,\varepsilon}$$

is defined over  $\mathbb{Q}$ .

**Remark:** The MDQS's have the following modular interpretation. Let

$$Z'_{N,\varepsilon} = Z_{N,\varepsilon} \setminus \cup \{\text{cuspidal divisors}\}.$$

Then:  $Z'_{N,\varepsilon}$  is the (coarse) moduli space for the functor classifying isomorphisms of mod  $N$  Galois representations of elliptic curves, i.e.

$$Z'_{N,\varepsilon}(K) \text{ “=” } \{(E, E', \psi) : E/K, E'/K \text{ are elliptic curves, } \psi : E[N] \xrightarrow{\sim} E'[N] \text{ is a } G_K\text{-isomorphism of determinant } \varepsilon \text{ (via the Weil pairings)}\} / (\text{twists}).$$

Special Case:  $\varepsilon = -1 \rightsquigarrow$  Hurwitz spaces

$Z'_{N,-1} \supset H_N$  : classifies normalized genus 2 covers  $f : C \rightarrow E$  of degree  $N$  of some elliptic curve  $E$ .

**Key Open Question:** If  $N = p > 19$ , is every curve  $C \subset Z_{N,\varepsilon}$  of genus  $\leq 1$  a **modular curve**, i.e. of the form  $C = T_{a,n}$ ?  
 - via **Lang's Conjecture**, this would have interesting **Diophantine** consequences.

**Simpler Question:** Up to (algebraic) equivalence, are all the **curves/divisors** on  $Z_{N,\varepsilon}$  **modular**?

**Notation:** Let  $NS^0(Z_{N,\varepsilon}) = NS(Z_{N,\varepsilon}) \otimes \mathbb{Q}$ , where  $NS(Z_{N,\varepsilon})$  denotes the **Neron-Severi group** of  $Z_{N,\varepsilon}$ , i.e.

$$NS(Z_{N,\varepsilon}) = \text{Div}(Z_{N,\varepsilon}) / (\text{algebraic equivalence}).$$

In addition, we write

$$\overline{NS}^0(Z_{N,\varepsilon}) = NS^0(Z_{N,\varepsilon}) / \langle cl(\Psi(P \times X)), cl(\Psi(X \times P)) \rangle,$$

where  $X = X(N)$  and  $P \in X(\mathbb{Q})$ , and, as above,  $\Psi$  denotes the quotient map

$$\Psi : X \times X \rightarrow Z_{N,\varepsilon}.$$

**Recall:** For any curve  $X/K$ , there is a close connection between the **Neron-Severi group**  $NS(X \times X)$  of the **product surface** and the endomorphism ring  $\text{End}_K(J_X)$  of its Jacobian  $J_X$ . Indeed, by the **theory of correspondences** we have an exact sequence

$$0 \rightarrow \kappa \rightarrow NS(X \times X) \rightarrow \text{End}_K(J_X) \rightarrow 0.$$

where  $\kappa = \langle cl(P \times X), cl(X \times P) \rangle$  (if  $X(K) \neq \emptyset$ ).

**Proposition:** We have a canonical identification

$$\overline{NS}^0(Z_{N,\varepsilon}) \simeq \text{End}_{G_{N,\varepsilon}}^0(J(N)),$$

where

$$\text{End}_{G_{N,\varepsilon}}(J(N)) = \{f \in \text{End}_{\mathbb{Q}}^0(J(N)) : gf = f\tau_{\varepsilon}(g), \forall g \in G_N\}.$$

**Corollary:** For any  $(N, \varepsilon)$  we have a natural embedding

$$\mathbb{T}_{\varepsilon^{-1}} \subset \overline{NS}^0(Z_{N,\varepsilon})$$

**Theorem 7:** If  $N = p$  is prime, then

$$\overline{NS}^0(Z_{p,\varepsilon}) \simeq \mathbb{T}_{\varepsilon^{-1}}.$$

**Proof (Sketch)** Use [Example 2](#) and [Theorem 6](#).

**Conclusion:** Thus, up to algebraic equivalence, all divisors in  $Z_{p,\varepsilon}$  are **modular**, i.e. they are  $\mathbb{Q}$ -linear combinations of the divisors  $\Psi(T_{a,n})$  with  $a^2n \equiv \varepsilon(N)$ , together with the two curves  $\Psi(P \times X)$  and  $\Psi(X \times P)$ .

**Corollary:** We have

$$\text{rk } NS(Z_{p,\varepsilon}) = 2 + \frac{1}{24}(p-1)(p-5) + \frac{1}{2} \left( \frac{\varepsilon}{p} \right) h(p),$$

where

$$h(p) = \begin{cases} h(\mathbb{Q}(\sqrt{-p})) & \text{if } p \equiv 3(4) \\ 0 & \text{if } p \equiv 1(4) \end{cases}$$

**Proof of Theorem 7 (Details).** Recall from **Example 2** that

$$\mathbb{E} = \langle \mathbb{T}', \tau, \tau' \rangle.$$

Since  $\tau, \tau' \in \mathbb{Q}[G]$ , we see that

$$\mathbb{M} = \langle \mathbb{E}, G \rangle = \langle \mathbb{T}', G \rangle.$$

But since  $\mathbb{T}' = Z(\mathbb{E})$ , we have

$$fT = Tf = \tau_\varepsilon(T)f, \quad \forall f \in \mathbb{E}, T \in \mathbb{T}',$$

and so

$$\begin{aligned} \text{End}_{\mathbb{M}, \varepsilon}(\mathbb{E}) &:= \{f \in E : fx = \tau_\varepsilon(x)f, \forall x \in \mathbb{M}\} \\ &= \text{End}_{G, \varepsilon}(J(p)) \end{aligned}$$

Now it follows from **Theorem 6** that

$$\text{End}_{\mathbb{M}, \varepsilon}(\mathbb{E}) = \mathbb{T}_{\varepsilon^{-1}},$$

which proves **Theorem 7** (via the **Proposition**).