Modular Forms and Modular Curves

Emmanuel Ullmo

August 26, 2006

Contents

Chapter 0

Introduction

0.1 Modular Curves

Let $\mathbb{H} = \{z \in \mathbb{C}\,; z = x + \mathrm{i}y, y = \mathrm{Im}(z) > 0\}$ be the Poincaré upper half plane, and let $\mathrm{SL}_2(\mathbb{R}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{R})\,, ad - bc = 1 \right\}$, then $\mathrm{SL}_2(\mathbb{R})$ acts transitively on the upper plane $\mathbb{H}$ by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z = \frac{az+b}{cz+d}$.

Definition 0.1. Let $N \in \mathbb{N}$, $\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})\,, ad - bc = 1 \right\}$. Define the subgroups

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

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})\,; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\};$$

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

Then $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ are some fundamental examples of *congruence subgroups* of $\mathrm{SL}_2(\mathbb{Z})$. By definition, a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is said to be a ***congruence subgroup*** if there exist $N \in \mathbb{N}$, such that $\Gamma(N) \subset \Gamma \subset \mathrm{SL}_2(\mathbb{Z})$.

A congruence subgroup Γ is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$.Such a subgroup acts ***properly discontinuously*** on $\mathbb{H}$: for any $K_1\,, K_2$ compact subsets of $\mathbb{H}$, the set $\{\gamma \in \Gamma, \gamma \cdot K_1 \cap K_2 \neq \emptyset\}$ is a finite set.

We will show that $Y(\Gamma) = \Gamma \backslash \mathbb{H}$ is endowed with the structure of Riemann surface. It is possible to add a finite set of points $\{c_1, \ldots, c_n\}$ called *cusps* of Γ such that $X(\Gamma) = Y(\Gamma) \cup \{c_1\,, \ldots, c_n\}$ has a structure of a compact Riemann surface.

The upper half plane $\mathbb{H}$ is endowed with a $\mathrm{SL}_2(\mathbb{R})$-invariant measure $d\mu_0 = \frac{dx \cdot dy}{y^2}$: for all $\alpha \in \mathrm{SL}_2(\mathbb{Z}), \alpha^* \cdot d\mu_0 = d\mu_0$. For any congruence subgroup Γ, we'll show $\mathrm{Vol}_{d\mu_0}(\Gamma\backslash\mathbb{H}) = \int_{\Gamma\backslash\mathbb{H}} d\mu_0$ is finite.

We say that Γ is a lattice in $\mathbb{H}$.

0.2 Elliptic Curves

Over $\mathbb{C}$, there are three equivalent ways of defining elliptic curves.

1. A couple (E, O), consisting of a compact Riemann surface E of genus 1, and a point O of $E(\mathbb{C})$. (The point O is the origin of $E(\mathbb{C})$.)

2. Let Γ be a lattice of $\mathbb{C}$, then $E = \mathbb{C}/\Gamma$, is endowed with the structure of a Riemann Surface of genus 1 with origin ΓO.

3. An algebraic curve with an equation of the form

$$y^2 = x^3 + Ax + B$$

in $\mathbb{C}^2$ s.t. $\Delta = -(4A^3 + 27B^2) \neq 0$.

There is an abelian group structure on $E(\mathbb{C})$ (clear from the 2nd definition). "Modular curves"="Hyperbolic analogue of elliptic curves". The 3rd definition extends to more general fields, such as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}_p$, $\mathbb{F}_p$.

Fundamental links between Modular Forms and Elliptic curves:

Proposition 0.2.1. $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ *is a "moduli space" for elliptic curves over* $\mathbb{C}$. *For any* $\tau \in \mathbb{H}$, *we define the lattice* $\Gamma_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau \subset \mathbb{C}$, *and the associated elliptic curve* $E_\tau = \mathbb{C}/\Gamma_\tau$.

(a) *Any elliptic curve over* $\mathbb{C}$ *is isomorphic to* E_τ *for some* $\tau \in \mathbb{H}$

(b) *The two elliptic curves* E_τ *and* $E_{\tau'}$ *are isomorphic if and only if there exists* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ *s.t.* $\tau' = \gamma \cdot \tau$

More generally, if Γ is a congruence lattice (ex. $\Gamma = \Gamma(N), \Gamma_1(N), \Gamma_0(N)$), then $Y(\Gamma) = \Gamma\backslash\mathbb{H}$ is a moduli space for "elliptic curves endowed with some extra structures".

Example 0.1. We saw that $E(\mathbb{C})$ has the structure of an abelian group. A point $P \in E(\mathbb{C})$ is said to be a torsion point of $E(\mathbb{C})$, if there is N s.t. $[N] \cdot P = O$ ($\iff P \in \frac{1}{N}\Gamma/\Gamma$ if $E = \mathbb{C}/\Gamma$.)

We'll show that $Y_1(N) = \Gamma_1(N)\backslash\mathbb{H}$ is a moduli space for couples (E, P) where E is elliptic curve over $\mathbb{C}$ and $P \in E(\mathbb{C})$ is a torsion point of order N.

The purpose of the course is to give a more arithmetic link between modular curves and elliptic curves.

0.3 Zeta Function and L-function

The fundamental example is the ***Riemann Zeta function***

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}} \, .$$

The Dirichlet Series $\sum_{n=1}^{\infty} \frac{1}{n^s}$ is convergent for $\mathrm{Re}(s) > 1$. We have an analytic continuation of $\zeta(s)$ to $\mathbb{C}$ (with a simple pole at $s = 1$). There is a functional equation: let

$$\Lambda(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s) \, ,$$

then

$$\Lambda(1-s) = \Lambda(s) \, .$$

If E is an elliptic curve over $\mathbb{Q}$, we will define an associated L-function

$$L(E, s) = \sum_{n=1}^{\infty} a_n n^{-s} = \prod_p L_p(E\,, s) \, .$$

We will also define the L-function of a modular form f on $\Gamma\backslash\mathbb{H}$ for a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$. A modular form f will be interpreted as an holomorphic differential form on $\Gamma\backslash\mathbb{H}$.

The goal of the course is to give a precise meaning to the following statement :

Conjecture 0.1 (**Taniyama-Weil conjecture, Wiles' theorem**). *For any elliptic curve E over $\mathbb{Q}$, there exist an integer $N = N_E$(called the* conductor *of E) and a modular form f for $\Gamma_0(N)$ such that $L(E\,, s) = L(f\,, s)$.*

0.4 The L-function of an Elliptic Curve over $\mathbb{Q}$

We start with an elliptic curve over $\mathbb{Q}$ defined by an equation

$$y^2 = x^3 + ax + b \, ; a, b \in \mathbb{Q}, \Delta = -(4a^3 + 27b^2) \neq 0 \, .$$

For almost all prime numbers p, $a\,, b \in \mathbb{Z}_p$, and the curve in $\mathbb{F}_p^2$ with equation

$$y^2 = x^3 + \bar{a}x + \bar{b}\,. \tag{0.1}$$

where $\bar{a}, \bar{b} \in \mathbb{F}_p$ are mod p reduction of a and b, is an elliptic curve over $\mathbb{F}_p$. ($\bar{\Delta} = -(4\bar{a}^3 + 27\bar{b}^2) \neq 0$)

Let $\#(E(\mathbb{F}_p))$ be the number of solutions of the equation (0.1) in $\mathbb{F}_p \times \mathbb{F}_p$. We will show the following proposition:

Proposition 0.4.1. *If we write $a_p = p - \#(E(\mathbb{F}_p))$, then $|\, a_p \,| < 2\sqrt{p}$.*

We then define

$$L_p(E, s) = \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

for all "good primes". We will also give a definition of $L_p(E, s)$ for the remaining "bad primes".

By definition,

$$L(E, s) := \prod_{p \text{ prime}} L_p(E, s)\,.$$

0.5 The L-function $L(f, s)$ of Modular Form f

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ (ex. $\Gamma = \Gamma(N), \Gamma_1(N)\,, \Gamma_0(N)$). A ***modular form of weight*** $2k$ for Γ is a holomorphic function f on $\mathbb{H}$ such that

1. $\forall \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, $\forall z \in \mathbb{H}$, $f(\gamma \cdot z) = f(\frac{az+b}{cz+d}) = (cz + d)^{2k} f(z)$.
2. A holomorphic condition at the cusps $\{c_1, \ldots, c_n\}$ of Γ.

We remark that there exists $r \in \mathbb{N}$, s.t. $\gamma_0 = \left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$. If f is a weight $2k$ modular form, then $f(\gamma_0 \cdot z) = f(z + r) = f(z)$, so f is r-periodic. Assume $r = 1$ for simplicity, then the theory of Fourier series tells us that

$$f(z) = \sum_{n \in \mathbb{Z}} a_n e^{2\mathrm{i}\pi n z} := \sum_{n \in \mathbb{Z}} a_n q^n$$

where $q = e^{2\mathrm{i}\pi z}$.

The holomorphic condition in 2. implies in fact that

$$f(z) = \sum_{n \geq 0} a_n q^n := \sum_{n \geq 0} a_n(f) q^n$$

i.e, $a_n = 0\,$, for $n < 0$. We then define

$$L(f\,, s) = \sum_{n \geq 1} a_n(f) n^{-s}.$$

0.6 Central Results of the Course

- The space $\mathcal{M}_{2k}(\Gamma)$ of weight $2k$-modular forms for Γ is finite dimensional. The dimension of $\mathcal{M}_{2k}(\Gamma)$ will be computed using the *Riemann-Roch theorem* on the compact Riemann surface $X(\Gamma) = \Gamma\backslash\mathbb{H}\cup\{c_1,.....,c_n\}$.

- There is a basis $\mathscr{B} = \{f_1, f_2, \ldots, f_r\}$ of (almost all) $\mathcal{M}_{2k}(\Gamma)$ s.t. for any $i \in \{1, ..., r\}$,

$$L(f_i, s) = \prod_{p \text{ good primes}} \frac{1}{1 - a_p(f_i)p^{-s} + p^{2k-1}p^{-2s}} \prod_{p \text{ bad primes}} L_p(f_i, s) \, .$$

  (There are only finitely many bad primes.) And it is not too difficult to prove that $L(f_i, s)$ admits an analytic continuation relating $L(f_i, s)$ and $L(f_i, 2k - s)$.

- The existence of such an Euler product is given by the existence of *Hecke operators* acting on $\mathcal{M}_{2k}(\Gamma)$. The $f_i \in \mathscr{B}$ are *eigenfunctions* of Hecke operators. The existence of the Hecke operators comes from the fact that Γ is an *arithmetic lattice* ($\Leftrightarrow [\mathrm{Comm}_{\mathrm{GL}_2(\mathbb{R})}(\Gamma) : \Gamma] = \infty$, where $\mathrm{Comm}_{\mathrm{GL}_2(\mathbb{R})}(\Gamma) := \{\alpha \in \mathrm{GL}_2(\mathbb{R}) \, ; \Gamma \text{ and } \alpha\Gamma\alpha^{-1} \text{ are commensurable}\}$. Two subgroups Γ and Γ' are said to be ***commensurable*** if and only if $\Gamma \cap \Gamma'$ is of finite index in Γ and Γ').

  Conjecture 0.2. *For any elliptic curve E over $\mathbb{Q}$, there is an $N = N_E$, and a weight 2 modular form f for $\Gamma_0(N)$ such that for all prime p,*

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

  By the definitions of $L_p(E\,, s)$ and $L_p(f\,, s)$, this means that $a_p(E) = a_p(f)$.

  Moreover, we'll see that there is a natural model $X_0(N)_{\mathbb{Q}}$ of $X_0(N)_{\mathbb{C}}$ over $\mathbb{Q}$, i.e, a curve C over $\mathbb{Q}$ such that

$$C \otimes_{\mathbb{Q}} \mathbb{C} \cong \Gamma_0(N)\backslash\mathbb{H} \cup \{ \text{ cusps of } \Gamma_0(N) \}.$$

  Then the Taniyama-Weil conjecture is equivalent to the following statement.

  Conjecture 0.3. *There exists a non-constant morphism of algebraic curves over $\mathbb{Q}$*

$$\varphi \; : \; X_0(N)_{\mathbb{Q}} \longrightarrow E_{\mathbb{Q}} \, .$$

If α is a holomorphic differential form on $E/\mathbb{Q}$, then $\varphi^*\alpha = c \cdot f$ where $c \in \sqrt{-1}\pi\mathbb{Q}$ and f is a modular form on $X_0(N)$ such that $L(f\,,s) = L(E\,,s)$.

Remark 0.1. (a) Using the relation $a_p(E) = a_p(f)$, we get $|a_p(f)| < 2\sqrt{p}$ (a deep result conjectured by Ramanujan and proved by Deligne) as $|a_p(E)| < 2\sqrt{p}$ is an easy result.

(b) It's easy to prove that $L(f\,,s)$ has an analytic continuation to $\mathbb{C}$ and a functional equation relating $L(f\,,s)$ and $L(f\,,2-s)$. Using the Taniyama-Weil conjecture we get an analytic continuation and a functional equation for $L(E\,,s)$.

Note that (b) is very important in the formulation of the Birch and Swinnerton-Dyer conjecture.

Conjecture 0.4. *Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$. By the Mordell-Weil theorem $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}^r$ for some integer $r = \text{rank}(E/\mathbb{Q})$(the rank of $E/\mathbb{Q}$). Then $r = \text{ord}_{s=1}L(E\,,s)$.*

Chapter 1

Modular Functions and Modular Forms

1.1 The Modular Group

Let $G = \mathrm{SL}_2(\mathbb{R})$ and $\mathbb{H} = \{ z \in \mathbb{C} \mid \mathrm{Im}(z) > 0 \}$. We have an action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z = \frac{az+b}{cz+d}$.

Exercise 1.1. Verify that this is indeed an action.

Lemma 1.1.1. *The action of* $\mathrm{SL}_2(\mathbb{R})$ *is not free as* $-\mathrm{Id}$ *acts trivially but* $\overline{G} := G/\{ \pm \mathrm{Id} \}$ *acts freely.*

Proof. For $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$,

$$g \cdot z = \frac{az+b}{cz+d} = z \,, \forall z \in \mathbb{H} \iff cz^2 + (d-a)z + b = 0 \,, \forall z \in \mathbb{H}$$
$$\iff b = c = 0 \,, d = a$$

This is also equivalent to $g = \pm \mathrm{Id}$ since $1 = ad - bc = a^2$. □

Lemma 1.1.2. $\mathrm{SL}_2(\mathbb{R})$ *acts transitively on* $\mathbb{H}$.

Proof. Any $z \in \mathbb{H}$ is in the orbit of $\mathrm{i} = \sqrt{-1}$ because we have

$$\begin{pmatrix} y^{1/2} & xy^{-1/2} \\ 0 & y^{-1/2} \end{pmatrix} \mathrm{i} = x + \mathrm{i}y \,.$$

□

Lemma 1.1.3. *The stabilizer of* $\mathrm{i} = \sqrt{-1}$ *is*

$$\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{R})}(\mathrm{i}) = \mathrm{SO}(2) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} ; a^2 + b^2 = 1. \right\}$$

Proof. For $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$,

$$\begin{aligned} g \cdot \mathrm{i} = \frac{a\mathrm{i} + b}{c\mathrm{i} + d} = \mathrm{i} &\iff -c - b + \mathrm{i}(d - a) = 0\,, \\ &\iff c = -b\,, d = a\,, 1 = ad - bc = a^2 + b^2. \end{aligned}$$

□

Corollary 1.1.4. *We have a homeomorphism:*

$$\begin{aligned} \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2) &\xrightarrow{\sim} \mathbb{H} \\ g\mathrm{SO}(2) &\mapsto g \cdot \mathrm{i} \end{aligned}$$

whose inverse is given by $z = x + \mathrm{i}y \mapsto \left(\begin{smallmatrix} y^{1/2} & xy^{-1/2} \\ 0 & y^{-1/2} \end{smallmatrix}\right)$.

Remark 1.1. One can show that $\mathrm{SO}(2)$ is a compact subgroup of $\mathrm{SL}_2(\mathbb{R})$, maximal among compact subgroups of $\mathrm{SL}_2(\mathbb{R})$. Then Corollary 1.1.4 is the description of $\mathbb{H}$ as a *symmetric space*.

Corollary 1.1.5. *We have* $\mathrm{SL}_2(\mathbb{R}) = B \cdot \mathrm{SO}(2)$ *where*

$$B = \{ \left(\begin{smallmatrix} a & b \\ 0 & a^{-1} \end{smallmatrix}\right) \mid a \in \mathbb{R}^*\,, b \in \mathbb{R} \}.$$

Proof. Let $g \in \mathrm{SL}_2(\mathbb{R})$. By Corollary 1.1.4, there exists $b \in B$ such that $g \cdot \mathrm{i} = b \cdot \mathrm{i}$ which is equivalent to

$$b^{-1}g \in \mathrm{SO}(2) \iff g = b \cdot k, \quad \text{with } b \in B\,, k \in \mathrm{SO}(2).$$

□

Definition 1.1. The group $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ is called the ***modular group***.

Definition 1.2. A subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Q})$ is said to be ***arithmetic*** if Γ and $\mathrm{SL}_2(\mathbb{Z})$ are commensurable, i.e, if $\Gamma \cap \mathrm{SL}_2(\mathbb{Z})$ is of finite index in Γ and $\mathrm{SL}_2(\mathbb{Z})$.

Definition 1.3. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is said to be a ***congruence group*** if $\exists N \in \mathbb{N}$ such that $\Gamma(N) \subset \Gamma$.

Example 1.1. $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$.

Proposition 1.1.6. *The action of* $\mathrm{SL}_2(\mathbb{Z})$ *on* $\mathbb{H}$ *is properly discontinuous, i.e, for any* K_1, K_2 *compact subsets of* $\mathbb{H}$, $\{\gamma \in \Gamma ; \gamma K_1 \cap K_2 \neq \emptyset\}$ *is a finite set.*

Lemma 1.1.7. *Let* $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ *and* $z = x + \mathrm{i}y \in \mathbb{H}$. *Then*

$$\mathrm{Im}(gz) = \frac{\mathrm{Im}(z)}{|cz+d|^2} > 0.$$

Proof. Just check it by computation. □

Proof of Prop.1.1.6. Let K_1, K_2 be two compact subsets of $\mathbb{H}$. Let $\varepsilon > 0$ such that $\forall \omega \in K_1 \cup K_2$, $\mathrm{Im}(w) \geq \varepsilon$.

Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, $z = x + \mathrm{i}y \in K_1$ such that $\gamma \cdot z \in K_2$. Then

$$\varepsilon \leq \mathrm{Im}(\gamma \cdot z) = \frac{\mathrm{Im}(z)}{(cx+d)^2 + c^2y^2} \leq \frac{\max_{\omega \in K_1} \mathrm{Im}(\omega)}{(cx+d)^2 + c^2\varepsilon^2} =: \frac{M}{(cx+d)^2 + c^2\varepsilon^2}. \tag{1.1}$$

Thus, $c^2 \leq \frac{M}{\varepsilon^3}$. There are therefore finitely many choices for c. As c is bounded and x is bounded, (1.1) implies there are only finitely many choices for d.

We need to show that given a pair (c, d) (with $\gcd(c, d) = 1$), there exist at most finitely many (a, b)'s such that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) K_1 \cap K_2 \neq \emptyset$.

Lemma 1.1.8. *Let* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $\gamma' = \left(\begin{smallmatrix} a' & b' \\ c & d \end{smallmatrix}\right)$. *Then* $\gamma'\gamma^{-1} = \pm\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ *for some* $n \in \mathbb{Z}$.

Proof of Lemma.1.1.8. Check it! □

Then for all $z \in \mathbb{H}$,

$$\mathrm{Re}(\gamma' z) = \mathrm{Re}\left(\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)\gamma z\right) = \mathrm{Re}(\gamma z) + n.$$

Fix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma K_1 \cap K_2 \neq \emptyset$. Let $\gamma' = \left(\begin{smallmatrix} a' & b' \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma' K_1 \cap K_2 \neq \emptyset$. Fix $\omega \in K_1$ with $\gamma'\omega \in K_2$, we have

$$\min_{K_2} \mathrm{Re}(z) \leq \mathrm{Re}(\gamma'\omega) = \mathrm{Re}(\gamma\omega) + n \leq \max_{K_2} \mathrm{Re}(z)$$

which yields

$$\min_{K_2} \mathrm{Re}(z) - \max_{K_1} \mathrm{Re}(\gamma z) \leq n \leq \max_{K_2} \mathrm{Re}(z) - \min_{K_1} \mathrm{Re}(\gamma z).$$

One then obtains the result from the boundedness of n. □

Corollary 1.1.9. $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ *is separated for the quotient topology.*

Exercise 1.2. Prove Corollary.1.1.9.

Definition 1.4 (***Fundamental domain***)**.** Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be a subgroup acting properly discontinuously on $\mathbb{H}$. A ***fundamental domain*** $\mathscr{F}$ for Γ is an open set such that:

(i) $\forall z \in \mathbb{H}$, $\exists \gamma \in \Gamma$ such that $\gamma z \in \overline{\mathscr{F}}$;

(ii) Let $z_1\,, z_2 \in \mathscr{F}$ and $\gamma \in \Gamma$. If $\gamma z_1 = z_2$, then $z_1 = z_2$ and $\gamma = \pm\,\mathrm{Id}$.

Example 1.2. $\mathscr{F} = \{\, z = x + \mathrm{i}y \,; -\frac{1}{2} < x < \frac{1}{2}\,, y > 0\,, |z| > 1 \,\}$ is a fundamental domain for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Lemma 1.1.10. *Let* Γ *be a discrete subgroup of* $\mathrm{SL}_2(\mathbb{R})$ *and* D *a fundamental domain for* Γ*. Let* $\Gamma' \subset \Gamma$ *be a subgroup of finite index. Write* $\Gamma = \bigsqcup_{i=1}^{r} \Gamma'\alpha_i$ *as a disjoint union of cosets, for some* $\alpha_i \in \Gamma$*. Then* $D' = \cup_{i=1}^{r} \alpha_i D$ *is a fundamental domain for* Γ'*.*

Proof. (a) Let $z \in \mathbb{H}$. There exists $\gamma \in \Gamma$ such that $z = \gamma \cdot z'$ with $z' \in \overline{D}$ and there exists $i \in \{\,1\,, 2\,, \ldots, r\,\}$ such that $\gamma = \gamma'\alpha_i$ with $\gamma' \in \Gamma'$. Therefore, $z = \gamma'(\alpha_i z') \in \gamma'\overline{D'}$.

(b) If $D' \cap \gamma D' \neq \emptyset$, for some $\gamma \in \Gamma'$, there exists $(i,,j) \in \{\,1\,, 2\,, \ldots, r\,\}^2$ such that $\gamma\alpha_i D \cap \alpha_j D \neq \emptyset$. This implies $\alpha_j^{-1}\gamma\alpha_i D \cap D \neq \emptyset$, and hence $\alpha_j = (\pm\gamma)\alpha_i$. Then we must have $i = j$ and $\gamma = \pm\,\mathrm{Id}$. □

Exercise 1.3. Prove that it's possible to choose the α_i in such a way $\overline{D'}$ is connected.

Exercise 1.4. Let p be a prime number. Prove

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{j=0}^{p-1} \Gamma_0(p) \begin{pmatrix} 1 & 0 \\ j & 1 \end{pmatrix} \bigsqcup \Gamma_0(p) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Proposition 1.1.11. *Let* $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$*,* $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$*. Then* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by* $T\,, S$*.*

Proof. Let Γ' be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by T and S. Then $S^2 = -\,\mathrm{Id} \in \Gamma'$. Let $\mathscr{F}$ be a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$.

(a) $\forall \gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma \cdot \mathscr{F}$ is also a fundamental domain.

(b) The fundamental domains $\gamma\mathscr{F}$ such that $\dim_{\mathbb{R}}(\overline{\mathscr{F}} \cap \overline{\gamma\mathscr{F}}) = 1$ are $T\mathscr{F}\,, T^{-1}\mathscr{F}$ and $S\mathscr{F}$.

(c) Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and let $\mathscr{F}_\gamma = \gamma\mathscr{F}$. Then there exist $\gamma_1 = \mathrm{Id}\,, \gamma_2\,, \ldots, \gamma_n = \gamma$ such that $\dim_{\mathbb{R}}(\overline{\gamma_k\mathscr{F}} \cap \overline{\gamma_{k+1}\mathscr{F}}) = 1$, for all $k = 1\,, \ldots, n-1$. Since

$$\dim_{\mathbb{R}}(\gamma_k^{-1}\gamma_{k+1}\overline{\mathscr{F}} \cap \overline{\mathscr{F}}) = 1 \Longleftrightarrow \gamma_k^{-1}\gamma_{k+1} = \pm S\,, \pm T\,, \text{ or } \pm T^{-1}\,,$$

γ is a product of $S\,, T\,, T^{-1}$ and $-\mathrm{Id} = S^2 \in \Gamma'$. Hence $\gamma \in \Gamma'$. □

Definition 1.5. An element $\alpha \in \mathrm{SL}_2(\mathbb{R})$ is said to be
(a) ***parabolic***, if $\mathrm{Tr}(\alpha) = \pm 2$ (ex. $\alpha = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$);
(b) ***elliptic***, if $|\,\mathrm{Tr}(\alpha)| < 2$;
(c) ***hyperbolic***, if $|\,\mathrm{Tr}(\alpha)| > 2$.

The characteristic polynomial of α is $\chi_\alpha(X) = X^2 - \mathrm{Tr}(\alpha)X + 1$ and $\Delta = \mathrm{Tr}(\alpha)^2 - 4$.

We remark that $\mathrm{SL}_2(\mathbb{R})$ acts also on $\mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$ via the same formula:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha = \begin{cases} \frac{a\alpha+b}{c\alpha+d}\,, & \text{if } c\alpha + d \neq 0 \\ \infty\,, & \text{if } c\alpha + d = 0 \end{cases}, \quad \forall \alpha \in \mathbb{R}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \begin{cases} \frac{a}{c}\,, & \text{if } c \neq 0 \\ \infty\,, & \text{if } c = 0 \end{cases}$$

Therefore, $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{H} \cup \mathbb{P}^1(\mathbb{R})$.

Lemma 1.1.12. *Let $\alpha \in \mathrm{SL}_2(\mathbb{R})$ acting on $\mathbb{H} \cup \mathbb{P}^1(\mathbb{R})$.*
(a) *if α is parabolic, then α has a unique fixed point z and $z \in \mathbb{P}^1(\mathbb{R})$;*
(b) *if α is elliptic, then α has a unique fixed point z and $z \in \mathbb{H}$;*
(c) *if α is hyperbolic, then α has two fixed points $z_1\,, z_2$ and $z_1\,, z_2$ are in $\mathbb{P}^1(\mathbb{R})$.*

Proof. Exercise, using $\chi_\alpha(X)$. □

Definition 1.6. Let Γ be a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$. A point $z \in \mathbb{H}$ is said to be ***elliptic*** if $\exists \gamma \in \Gamma$, $\gamma \neq \pm\,\mathrm{Id}$ such that $\gamma \cdot z = z$. A point $P \in \mathbb{P}^1(\mathbb{R})$ is said to be a ***cusp*** for Γ if there exists $\gamma \in \Gamma$, $\gamma \neq \pm\,\mathrm{Id}$ and γ parabolic such that $\gamma \cdot P = P$.

Lemma 1.1.13. *If $z \in \mathbb{H}$ is elliptic for Γ(or is a cusp), then $\forall \gamma \in \Gamma$, γz is elliptic (or a cusp).*

Proof. If $\alpha \in \Gamma$, then $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\gamma\alpha\gamma^{-1})$. Therefore α is elliptic or parabolic if and only if $\gamma\alpha\gamma^{-1}$ is elliptic or parabolic. Then the result follows from the fact that $\alpha z = z \Longleftrightarrow \gamma\alpha\gamma^{-1}(\gamma z) = \gamma z$. □

Lemma 1.1.14. *Let $z \in \mathbb{H}$ be an elliptic point, then its fixactor* $\mathrm{Fix}_\Gamma(z) = \{\, \gamma \in \Gamma \,|\, \gamma z = z \,\}$ *is a finite cyclic subgroup of* Γ.

Proof. Fix $\alpha \in \mathrm{SL}_2(\mathbb{R})$ such that $\alpha \mathrm{i} = z$ and let $\varphi_\alpha : \mathrm{SL}_2(\mathbb{R}) \longrightarrow \mathrm{SL}_2(\mathbb{R})$ be the map $\gamma \mapsto \alpha^{-1}\gamma\alpha$. Then

$$\mathrm{Fix}_\Gamma(z) \cong \alpha^{-1}\Gamma\alpha \cap \mathrm{Fix}_{\mathrm{SL}_2(\mathbb{R})}(\mathrm{i}) = \alpha^{-1}\Gamma\alpha \cap \mathrm{SO}_2(\mathbb{R}).$$

Then $\mathrm{Fix}_\Gamma(z)$ is a discrete subgroup of the compact group $\mathrm{SO}_2(\mathbb{R})$ and hence is finite.

Exercise 1.5. Using $U^1 := \{\, z \in \mathbb{C} \,|\, |z| = 1 \,\} \cong \mathrm{SO}_2(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ given by

$$e^{2\pi \mathrm{i}\theta} \longleftrightarrow \begin{pmatrix} \cos 2\pi\theta & \sin 2\pi\theta \\ -\sin 2\pi\theta & \cos 2\pi\theta \end{pmatrix} \longleftrightarrow \bar{\theta}\,,$$

prove that any finite subgroup of $\mathrm{SO}_2(\mathbb{R})$ is cyclic.

□

Lemma 1.1.15. *Let $\theta \in \mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\, \infty \,\}$ be a cusp of Γ. Then* $\{\, \pm \mathrm{Id} \,\} \backslash \mathrm{Fix}_\Gamma(\theta) \cong \mathbb{Z}$.

Proof. Let $\alpha \in \mathrm{SL}_2(\mathbb{R})$ such that $\alpha\infty = \theta$.

$$\mathrm{Fix}_\Gamma(\theta) \cong \alpha^{-1}\Gamma\alpha \cap \mathrm{Fix}_{\mathrm{SL}_2(\mathbb{R})}(\infty)\,,$$

and

$$\mathrm{Fix}_{\mathrm{SL}_2(\mathbb{R})}(\infty) = \left\{ \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \,|\, x \in \mathbb{R}^*, y \in \mathbb{R} \right\} := B.$$

Let $U := \{\, \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \,|\, x \in \mathbb{R} \,\} \subset B$. Then $U \cong (\mathbb{R}, +)$ and $U \cap \alpha^{-1}\Gamma\alpha$ is discrete and nontrivial in $(\mathbb{R}, +)$.

Exercise 1.6. The discrete subgroups of $(\mathbb{R}, +)$ are of the form $\mathbb{Z}a$ with $a \in \mathbb{R}$.

Let $\left(\begin{smallmatrix} y & x \\ 0 & y^{-1} \end{smallmatrix}\right) \in B \cap \alpha^{-1}\Gamma\alpha$ with $|y| < 1$, then

$$\begin{pmatrix} y & x \\ 0 & y^{-1} \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y^{-1} & -x \\ 0 & y \end{pmatrix} = \begin{pmatrix} 1 & ay^2 \\ 0 & 1 \end{pmatrix} \in U \cap \alpha^{-1}\Gamma\alpha.$$

But $|y^2| < 1$ leads to a contradiction. Therefore, we get $B \cap \alpha^{-1}\Gamma\alpha = U \cap \alpha^{-1}\Gamma\alpha$. □

Proposition 1.1.16. *Let $\mathscr{F}$ be the usual fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$. Then the elliptic points for $\mathrm{SL}_2(\mathbb{Z})$ in $\overline{\mathscr{F}}$ are $\mathrm{i} = \sqrt{-1}$, $\rho = \frac{1+\mathrm{i}\sqrt{3}}{2}$ and $\rho^2 = \frac{-1+\mathrm{i}\sqrt{3}}{2}$. Moreover,*

(a) $\mathrm{Stab}_\Gamma(\mathrm{i}) = \pm\langle S\rangle$ is of order 2 in $\mathrm{SL}_2(\mathbb{Z})/\{\pm\mathrm{Id}\}$;

(b) $\mathrm{Stab}_\Gamma(\rho) = \pm\langle TS\rangle$ is of order 3 in $\mathrm{SL}_2(\mathbb{Z})/\{\pm\mathrm{Id}\}$;

(c) $\mathrm{Stab}_\Gamma(\rho^2) = \pm\langle ST\rangle$ is of order 3 in $\mathrm{SL}_2(\mathbb{Z})/\{\pm\mathrm{Id}\}$.

Remark 1.2. Note that $\rho = T\rho^2$. Therefore, the elliptic points for $\mathrm{SL}_2(\mathbb{Z})$ are $\mathrm{SL}_2(\mathbb{Z})\mathrm{i} \cup \mathrm{SL}_2(\mathbb{Z})\rho$.

Proposition 1.1.17. *The set of cusps of $\mathrm{SL}_2(\mathbb{Z})$ is $\mathrm{SL}_2(\mathbb{Z})\infty$ and it is equal to $\mathbb{Q}\cup\{\infty\} = \mathbb{P}^1(\mathbb{Q})$.*

Proof. ∞ is fixed by $T = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and T is parabolic. Therefore ∞ is a cusp of $\mathrm{SL}_2(\mathbb{Z})$.

Let $\frac{m}{n} \in \mathbb{Q}$ with $\gcd(m, n) = 1$. There exist $r, s \in \mathbb{Z}$ such that $rm - ns = 1$. This gives $\gamma = \left(\begin{smallmatrix}m & s\\ n & r\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\left(\begin{smallmatrix}m & s\\ n & r\end{smallmatrix}\right)\infty = \frac{m}{n} \in \mathbb{Q}$. Therefore, $\mathbb{P}^1(\mathbb{Q}) \subset \mathrm{SL}_2(\mathbb{Z})\infty$. As $\mathrm{SL}_2(\mathbb{Z})\infty \subset \mathbb{P}^1(\mathbb{Q})$, we find that $\mathbb{P}^1(\mathbb{Q}) = \mathrm{SL}_2(\mathbb{Z})\infty$.

Let $t \in \mathbb{R}$ such that t is fixed by $\alpha = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $\mathrm{Tr}(\alpha) = 2$. Then we have

$$ct^2 + (d-a)t - b = 0.$$

Since $\Delta = (d-a)^2 - 4bc = (d+a)^2 - 4(ad-bc) = \mathrm{Tr}(\alpha) - 4 = 0$, we have $t = -\frac{d-a}{2c} \in \mathbb{Q}$. This finishes the proof. □

1.2 Complex Structure on $\Gamma\backslash\mathbb{H}^*$

Definition 1.7. Let X be a topological space, then a "*complex structure*" (of dimension 1) is a covering $X = \bigcup_{\alpha\in I} U_\alpha$ by open subsets and some homomorphism $t_\alpha : U_\alpha \to W_\alpha$ where W_α is a connected open subsets of $\mathbb{C}$ such that if $U_\alpha \cap U_\beta \neq \emptyset$, then $t_\beta \circ t_\alpha^{-1} : t_\alpha(U_\alpha \cap U_\beta) \to t_\beta(U_\alpha \cap U_\beta)$ is a biholomorphic isomorphism. Then (U_α, t_α) is called a "*local chart*".

Definition 1.8. Two complex structures are said to be *equivalent* if their union is also a "complex structure". An equivalence class of "complex structures" is a ***complex structure***.

Definition 1.9. A ***Riemann surface*** X is a topology space X endowed with a complex structure of dimension 1.

Example 1.3. $\mathbb{P}(\mathbb{C}) = \mathbb{C}^2 - \{(0,0)\}/\sim$ is a Riemann surface with the complex structure:

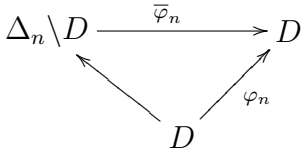
$$U_1 = \{[x,y], y \neq 0\} \xrightarrow{p_1} \mathbb{C}\,; \quad p_1 : [x,y] \mapsto \frac{x}{y}$$
$$U_2 = \{[x,y], x \neq 0\} \xrightarrow{p_2} \mathbb{C}\,; \quad p_2 : [x,y] \mapsto \frac{y}{x}$$

It is easy to see that p_1, p_2 are biholomorphisms as $p_1^{-1}(z) = [z,1]$, $p_2^{-1}(z) = [1,z]$, and

$$p_2 \circ p_1^{-1} \;:\; p_1(U_1 \cap U_2) = \mathbb{C}^* \longrightarrow p_2(U_1 \cap U_2) = \mathbb{C}^*\,; \quad z \mapsto \frac{1}{z}$$

is biholomorphic.

Example 1.4. Let $D = \{z \in \mathbb{C}\,;\, |z| < 1\}$, $\zeta_n = e^{\frac{2\pi i}{n}}$ and let Δ_n be the subgroup of the holomorphic automorphisms of D generated by $z = \zeta_n \cdot z$ (Therefore, $\Delta_n \cong \mathbb{Z}/n\mathbb{Z}$.) The function $\varphi_n : D \to D\,; z \mapsto z^n$ is invariant by Δ_n, so we get a map $\overline{\varphi}_n$ from the diagram:



Then $\overline{\varphi}_n$ is an homoeomorphism from $\Delta_n \backslash D$ to D, defining a complex structure of dimension 1 on $\Delta_n \backslash D$.

Example 1.5. $X_c = \{z \in \mathbb{C}\,;\, \mathrm{Im}(z) > c\}$. Let $h \in \mathbb{N}$ and $\Delta = \langle \delta_h \rangle \subset \mathrm{Aut}_{\mathrm{holo}}(X_c)$ generated by $z \mapsto z+h$. ($\Delta \cong \mathbb{Z}$ via the map $(\delta_n : z \mapsto z+nh) \mapsto n$.) Let $\overline{X}_c = X_c \cup \{\infty\}$ endowed with the topology such that a fundamental system of neighborhoods of ∞ is $X_n = \{z \in \mathbb{C}\,,\, \mathrm{Im}(z) > n\} \cup \{\infty\}$ for $n >> 0$. Then the action of Δ on X_c can be extended continuously to $\overline{X}_c$ by writing $\overline{\delta}_n \infty = \infty\,, \forall n \in \mathbb{N}$. The function

$$q(z) = \begin{cases} e^{\frac{2\pi i z}{h}}, & \text{if } z \neq \infty \\ 0, & \text{if } z = \infty \end{cases}$$

is a homeomorphism from $\Delta \backslash \overline{X}_c$ onto $B(0\,, e^{-\frac{2\pi c}{h}}) := \{z \in \mathbb{C}\,;\, |z| < e^{-\frac{2\pi c}{h}}\}$ Therefore, q defines a "complex structure" of dimension 1 on $\Delta \backslash \overline{X}_c$.

1.2.1 The Case of $\Gamma = \mathrm{SL}_2(\mathbb{Z})$

Let $\pi : \mathbb{H} \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$, $Q \mapsto P = \pi(Q)$. As the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ is properly discontinuous, there exists a neighborhood V of Q such that $\forall\gamma \in \Gamma, \gamma V \cap V \neq \emptyset \iff \gamma Q = Q$. If Q is not an elliptic point, then $V \to \pi(V)$ is a homeomorphism and $(\pi(V), \pi^{-1})$ is a local chart at P. If Q is an elliptic point, then $P = \Gamma\cdot\rho$ or $P = \Gamma\cdot\mathrm{i}$. If $P = \mathrm{SL}_2(\mathbb{Z})\cdot\mathrm{i}$, we may assume that $Q = \mathrm{i}$. There exists a neighborhood V of Q such that if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $\gamma V \cap V \neq \emptyset$ then $\gamma = \pm S$ or $\pm\,\mathrm{Id}$. By replacing V by $V \cap S\cdot V$, we may assume V is invariant by S. Thus we have a homeomorphism induced by $\pi : \langle S\rangle\backslash V \to \pi(V)$. Let φ be the holomorphic map $\mathbb{H} \to B(0,1)\ ;\ z \mapsto \frac{z-\mathrm{i}}{z+\mathrm{i}}$.

Lemma 1.2.1. *We have a commutative diagram*

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & \varphi(V) \\ {\scriptstyle S}\downarrow & & \downarrow{\scriptstyle z\mapsto -z} \\ V & \xrightarrow{\varphi} & \varphi(V) \end{array}$$

Proof. By direct computation, $\frac{-\frac{1}{z}-\mathrm{i}}{-\frac{1}{z}+\mathrm{i}} = \frac{-1-z\mathrm{i}}{-1+z\mathrm{i}} = -\frac{z-\mathrm{i}}{z+\mathrm{i}}$.

Exercise 1.7. Prove Lemma.1.2.1 by using the *Schwarz Lemma*.

□

The function $(\frac{z-\mathrm{i}}{z+\mathrm{i}})^2$ is an holomorphic function in the neighborhood of i invariant by S, therefore defines a function ψ_V near $P = \pi(\mathrm{i})$ which gives a local chart.

Local Chart at $\Gamma\mathrm{i}$

$$\begin{array}{ccc} \langle S\rangle\backslash V & \xrightarrow{\sim} & \{\pm\,\mathrm{Id}\}\backslash\varphi(V) \\ \downarrow & & \downarrow{\scriptstyle z\mapsto z^2} \\ \pi(V) & \xrightarrow[\psi_V]{} & B(0,1) \end{array}$$

Local Chart at $\Gamma\rho^2$

$$\begin{array}{ccc} \langle ST\rangle\backslash U & \xrightarrow{\sim} & \Delta_3\backslash\psi(U) \\ \downarrow & & \downarrow{\scriptstyle z\mapsto z^3} \\ \pi(U) & \xrightarrow[\psi_U]{} & B(0,1) \end{array}$$

In the same way, if $Q = \rho^2\,, P = \Gamma\cdot\rho^2$, let ψ be the map $z \mapsto \frac{z-\rho^2}{z-\bar{\rho}^2}$ and Δ_3 be the subgroup of holomorphic automorphisms generated by $z \mapsto e^{\frac{2\pi i}{3}}z$. Since ρ^2 is fixed by ST, we can choose a neighborhood U of ρ^2 invariant by ST (just replacing U by $U \cap ST\cdot U \cap (ST)^2\cdot U$ if necessary). The function $(\frac{z-\rho^2}{z-\bar{\rho}^2})^3$ is ST-invariant and therefore defines a local chart at $P = \pi(\rho^2)$.

Now we consider the complex structure at ∞.

We write $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ with the following topology: a basis of neighborhoods of ∞ is given by $U_N = \{z \in \mathbb{H}\,;\, \mathrm{Im}(z) > N\} \cup \{\infty\}$. More generally if $c = \sigma \cdot \infty \in \mathbb{P}^1(\mathbb{Q})$, then $\sigma \cdot U_N$ is a fundamental system of neighborhoods of c.

Note that

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^* = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathrm{SL}_2(\mathbb{Q})\backslash\mathbb{H} \cup \{\infty\}.$$

There exists a neighborhood U of ∞ in $\mathbb{H}^*$, (ex. $U_{100} = \{z \mid \mathrm{Im}(z) > 100\} \cup \{\infty\}$), such that $\forall \gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma \cdot U \cap U \neq \emptyset \iff \gamma = \pm\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ for some $n \in \mathbb{Z}$. Let $\pi : \mathbb{H}^* \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$ be the natural map, under which $\infty \mapsto \mathrm{SL}_2(\mathbb{Z})\infty$. We have the homeomorphisms

$$\begin{aligned} \pi(U) \simeq \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle \backslash U &\xrightarrow{\sim} B(0, e^{-2\pi \cdot 100}) \\ z &\mapsto q(z) = e^{2\pi i z} \end{aligned}$$

and $(U\,, q)$ is a local chart at ∞.

The union of all local charts defines a complex structure on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$.

1.2.2 Complex Structure on $\Gamma\backslash\mathbb{H}^*$ for $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$

Let Γ be a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$. Then ∞ is a cusp for Γ. There exists $n \in \mathbb{N}$, such that $T^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$ (as $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] < \infty$). $T^n\infty = \infty$ and T^n is parabolic. We find that ∞ is a cusp for Γ.

On $\Gamma\backslash\mathbb{H}$ the complex structure is defined as in the case of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. It is possible that there exists no elliptic points for Γ (if Γ contains no elliptic elements).

Exercise 1.8. If $N \geq 3$, $\Gamma(N)$ contains no elliptic elements.

We have $\Gamma\backslash\mathbb{P}^1(\mathbb{Q}) = \{c_1, c_2, \ldots, c_r\}$, $r = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$. Let h be the smallest integer larger than 0 such that $T^h \in \Gamma$. We have the map

$$\begin{aligned} \pi(U_N) \simeq \langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \rangle \backslash U_N &\xrightarrow{\sim} B(0, e^{-2\pi N}) \\ z &\mapsto q_h(z) = e^{2\pi i z/h} \end{aligned}$$

and the function q_h defines a local chart at ∞.

If $c = \sigma \cdot \infty$ with some $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, then $\sigma(U_N)$ is a neighborhood of c. Then it is easy to see that

$$\sigma^{-1}\mathrm{Fix}_\Gamma(c)\sigma = \mathrm{Fix}_{\sigma^{-1}\Gamma\sigma}(\infty) = \pm\{\left(\begin{smallmatrix} 1 & nh_c \\ 0 & 1 \end{smallmatrix}\right)\,;\, n \in \mathbb{Z}\}.$$

Let $q_c(z) = e^{\frac{2\pi i z}{h_c}}$, then $\sigma(U_N) \to \mathbb{C}\ ; z \mapsto q_c(\sigma^{-1} \cdot z)$ defines a local chart near c. The number h_c is called the ***width*** of c, and we will write

$$\begin{cases} Y(\Gamma) = \Gamma\backslash\mathbb{H} \\ X(\Gamma) = \Gamma\backslash\mathbb{H}^* \end{cases} \quad \text{and} \quad \begin{cases} X(\Gamma(N)) = X(N) \\ X(\Gamma_0(N)) = X_0(N) \\ X(\Gamma_1(N)) = X_1(N)\ . \end{cases}$$

1.3 Review of the Theory of Compact Riemann Surfaces

1.3.1 Holomorphic and Meromorphic Functions

Let X be a compact Riemann Surface and $\mathcal{V} = (U_i\,, z_i)_{i\in I}$ be a complex structure on X. A function $f : U \subset X \longrightarrow \mathbb{C}$ is said to be ***holomorphic*** (or ***meromorphic***) if for any $i \in I$, $f \circ z_i^{-1} : z_i(U \cap U_i) \longrightarrow \mathbb{C}$ is holomorphic (or meromorphic).

A map $f : X \longrightarrow X'$ between two Riemann surfaces is said to be ***holomorphic*** (or ***meromorphic***) if for all $P \in X$, there exists a local chart $(U\,, z)$ at P and a local chart $(U'\,, z')$ at $f(P)$ such that $f(U) \subset U'$ and $z' \circ f \circ z^{-1} : z(U) \longrightarrow z'(U')$ is holomorphic (or meromorphic).

Remark 1.3. A meromorphic map $f : X \longrightarrow \mathbb{C}$ can be extended to a holomorphic map of compact Riemann surfaces: $f : X \longrightarrow \mathbb{P}^1(\mathbb{C})$ sending the poles to ∞.

Lemma 1.3.1. *Any holomorphic map $f : X \longrightarrow \mathbb{C}$ is constant.*

1.3.2 Differential Forms

A ***holomorphic*** (or ***meromorphic***) ***differential form*** on an open set U of $\mathbb{C}$ is an expression of the form $f(z)dz$ with f holomorphic (or meromorphic).

Let $f : U \longrightarrow \mathbb{C}$ be a holomorphic map. Then $df := \frac{df}{dz}dz$ is called the ***associated differential form*** to f.

Let $\omega : U \longrightarrow U'$ be a holomorphic map $z' = \omega(z)$ and let $\alpha = f(z')dz'$ be a differential form on U'. We denote by $\omega^*(\alpha)$ the differential form on U defined by $\omega^*(\alpha) = f(\omega(z))\frac{d\omega}{dz}dz$.

Let X be a compact Riemann Surface and $(U_i\,, z_i)_{i\in I}$ a complex structure. A ***holomorphic differential form*** on X is given by a family $(\alpha_i)_{i\in I}$ of differential forms $\alpha_i = f_i(z_i)dz_i$ on $z_i(U_i)$ $, \forall i \in I$ such that if $\omega_{ij} := z_i \circ z_j^{-1} : z_j(U_i \cap U_j) \to z_i(U_i \cap U_j)$ denote the holomorphic maps given by

the definition of a complex structure. Then $\omega_{ij}^*(\alpha_i) = \alpha_j$ (or equivalently, $f_j(z_j)dz_j = f_i(\omega_{ij}(z_j))\omega'_{ij}(z_j)dz_j$).

1.3.3 Some Definitions and Notations

a. $\mathcal{M}(X)$ will denote the field of meromorphic functions on X.
b. The abelian group

$$\mathrm{Div}(X) := \Big\{ \sum_{P\in X} n_P \cdot [P] \,|\, n_P \in \mathbb{Z} \text{ and } n_P = 0 \text{ for almost all } P \Big\}$$

is called the group of ***divisors*** of X.
c. A divisor $D = \sum_{P\in X} n_P \cdot [P] \in \mathrm{Div}(X)$ is said to be ***effective*** (or ***non-negative***) if $n_P \geq 0$ for every $P \in X$. We write $D \geq 0$ in this case. If $D\,, D' \in \mathrm{Div}(X)$, we write $D \geq D'$ if $D - D' \geq 0$.
d. The ***degree*** map

$$\begin{aligned} \deg : (\mathrm{Div}(X)\,, +) &\longrightarrow (\mathbb{Z}\,, +) \\ \sum_{P\in X} n_P[P] &\mapsto \sum_{P\in X} n_P \end{aligned}$$

is a morphism of abelian groups. We write

$$\mathrm{Ord}_P(f) = \begin{cases} m\,; & \text{if } f \text{ has a zero of order } m \text{ at } P \\ -m\,; & \text{if } f \text{ has a pole of order } m \text{ at } P \end{cases}.$$

Let $z : U \longrightarrow z(U)$ be a local chart at P, then $f \circ z^{-1} : z(U) \longrightarrow \mathbb{C}$ is meromorphic and $\mathrm{Ord}_P(f)$ is defined as $\mathrm{Ord}_{z(P)}(f \circ z^{-1})$.
e. Let $f \in \mathcal{M}(X)$, then the divisor of f, $\mathrm{div}(f)$ is defined as $\mathrm{div}(f) = \sum_{P\in X} \mathrm{Ord}_P(f)[P] \in \mathrm{Div}(X)$. As $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$, we find that

$$\mathrm{Div}_{\mathrm{princ}}(X) := \{\mathrm{div}(f) \mid f \in \mathcal{M}(X)\}$$

is a subgroup of $\mathrm{Div}(X)$, called the group of ***principal divisors***.

Proposition 1.3.2. *For any $f \in \mathcal{M}(X)$, $\deg(\mathrm{div}(f)) = 0$.*

Idea of proof. Let $f : X \longrightarrow \mathbb{P}^1$ be the corresponding holomorphic function. (See Remark.1.3), then if f is not constant, $f^{-1}(\alpha) = \{\, \alpha_1\,, \ldots, \alpha_r \,\}$ is finite, and if we count with the right "multiplicities" n_i, then $f^*\alpha = \sum_{i=1}^r n_i[\alpha_i]$ is defined in such a way that $d = \sum_{i=1}^r n_i$ is independent of α. Such a d is called the ***degree*** of f. Therefore, $\deg(\mathrm{div}(f)) = \deg(f^*0) - \deg(f^*\infty) = 0$. □

f. Two divisors are said to be ***linearly equivalent*** if there exists an $f \in \mathcal{M}(X)$ such that $D_1 = D_2 + \mathrm{div}(f)$. If $D \in \mathrm{Div}(X)$, we denote by $|D|$ the set of divisors $D' \in \mathrm{Div}(X)$ that are linearly equivalent to D.
g. Divisor of a differential form. Let ω be a differential form on X. Let $P \in X$ and $(U\,, z)$ be a local chart at P. Then $\omega := f(z)dz$ on U.

Lemma 1.3.3. *The order at P of f: $\mathrm{Ord}_{z(P)}(f \circ z^{-1})$ is independent of local charts.*

Proof. Let $(U_1\,, z_1)$, $(U_2\,, z_2)$ be two local charts at P. Write $\omega_1 = f_1(z_1)dz_1$ on U_1 and $\omega = f_2(z_2)dz_2$ on U_2. The map

$$w_{1\,,2} := z_1 \circ z_2^{-1} : z_2(U_1 \cap U_2) \longrightarrow z_1(U_1 \cap U_2)$$

is a biholomorphic isomorphism. Therefore, $w'_{1\,,2}$ does not vanish. As $f(z_2)dz_2 = f_1(w_{1\,,2}(z_2))w'_{1\,,2}(z_1)dz_1$, $\mathrm{Ord}_{z_2(P)}f_2(z_2) = \mathrm{Ord}_{z_1(\mathrm{P})}f_1(z_1)$. □

We therefore define $\mathrm{Ord}_P(\omega) = \mathrm{Ord}_P(f)$. The divisor of a differential form ω is $\mathrm{div}(\omega) := \sum_{P\in X} \mathrm{Ord}_P(\omega) \cdot [P]$.

By the definitions of meromorphic functions and differential forms on X, we see that for any holomorphic differential forms ω_1, ω_2 on X, there exists $f \in \mathcal{M}(X)$ such that $\omega_2 = f \cdot \omega_1$. As $\mathrm{div}(f\omega) = \mathrm{div}(f) + \mathrm{div}(\omega)$, we see that the linearly equivalence class $|\mathrm{div}(\omega)|$ of ω is independent of the choice of ω. We write $K = \mathrm{div}(\omega)$, and we say the K is a ***canonical divisor***.

1.3.4 The Riemann-Roch Theorem

Let X be a compact Riemann surface, $D \in \mathrm{Div}(X)$. We define $\mathscr{L}(D) = \{\, f \in \mathcal{M}(X) \,|\, \mathrm{div}(f) + D \geq 0 \,\} \cup \{\, 0 \,\}$. Then $\mathscr{L}(D)$ is a $\mathbb{C}$-vector space and we have the following

Theorem 1.3.4. *The dimension of $\mathscr{L}(D)$ is finite for all $D \in \mathrm{Div}(X)$.*

If $g \in \mathcal{M}(X)$ and $D' = D + \mathrm{div}(g)$. Then the map

$$\mathscr{L}(D) \longrightarrow \mathscr{L}(D')\ ;\ \ f \mapsto fg^{-1}$$

is an isomorphism between $\mathscr{L}(D)$ and $\mathscr{L}(D')$. Therefore, $\dim \mathscr{L}(D) = \dim \mathscr{L}(D')$. We write $\ell(|D|) = \ell(D) = \dim \mathscr{L}(D)$.

Theorem 1.3.5 (Riemann-Roch)**.** *There exists $g = g_X \in \mathbb{N}$ such that for any $D \in \mathrm{Div}(X)$,*

$$\ell(D) - \ell(K - D) = \mathrm{deg}D + 1 - g$$

where $\ell(D) = \dim \mathscr{L}(D)$, K is the canonical divisor, i.e, $K = \mathrm{div}(\omega)$ where ω is a differential form on X.

Remark 1.4. $\mathscr{L}(0) \cong \mathbb{C} \cong \{$ constant functions $f : X \longrightarrow \mathbb{C}\}$ as any holomorphic map on a compact Riemann surface is constant. Therefore, $\ell(0) = 1$.

Corollary 1.3.6. *(a)* $\deg K = 2g - 2$*;*

(b) $\ell(K) = g$*. This means, the space of holomorphic differential forms on* X *is of dimension* g*. In fact,*

$$\begin{aligned}\mathscr{L}(K) &= \{\, f \in \mathcal{M}(X) \,|\, \mathrm{div}(f) + \mathrm{div}(\omega) \geq 0 \,\} \\ &= \{\, f \in \mathcal{M}(X) \,|\, \mathrm{div}(f\omega) \geq 0 \,\} \\ &\cong \{\, \textit{holomorphic differential forms on } X \,\}\end{aligned} \quad .$$

Proof. For (b), use the Riemann-Roch formula for $D = 0$:

$$1 - \ell(K) = \ell(0) - \ell(K) = 1 - g + 0.$$

Therefore, $\ell(K) = g$.

(a) Use the Riemann-Roch formula for $D = K$:

$$g - 1 = \ell(K) - \ell(0) = 1 - g + \deg K \ .$$

Therefore, $\deg K = 2g - 2$. □

Remark 1.5. If $\deg D < 0$, then $\ell(D) = 0$.

Proof. Let $f \in \mathscr{L}(D) - \{\, 0 \,\}$, then $\mathrm{div}(f) + D \geq 0$. This implies $\deg(\mathrm{div}(f) + D) = \deg D \geq 0$. □

Remark 1.6. If $\deg D = 0$ and $|D| \neq |0|$, then $\mathscr{L}(D) = \{\, 0 \,\}$.

Proof. Let $f \in \mathscr{L}(D) - \{\, 0 \,\}$, then $\mathrm{div}(f) + D \geq 0$ and $\deg(\mathrm{div}(f) + D) = \deg D = 0$. At the same time, $\mathrm{div}(f) + D \geq 0$. This implies $D + \mathrm{div}(f) = 0$ and hence $D = -\mathrm{div}(f) = \mathrm{div}(1/f)$. Therefore, $|D| = |0|$. □

Remark 1.7. If $g \geq 1$ and $D = P - Q$, then $|D| \neq |0|$.

Proof. If $D = P - Q = \mathrm{div}(f)$, for some $f \in \mathcal{M}(X)$, then $f : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ is such that $f^{-1}(0) = P$ and $f^{-1}(\infty) = Q$. Therefore $\deg f = 1$, and f is an isomorphism of compact Riemann surfaces. So the genus $g(X) = g(\mathbb{P}^1_{\mathbb{C}}) = 0$. □

Corollary 1.3.7. *If* $\deg D > 2g - 2$*, then* $\ell(D) = 1 - g + \deg D$*.*

Proof. $\deg(K - D) < 0 \Longrightarrow \ell(K - D) = 0$. Then the Riemann-Roch formula gives the result. □

Example 1.6 (Equation for elliptic curves)**.** Let $(E\,, O_E)$ be an elliptic curve. E is a Riemann surface of genus $g = 1$ and $O_E \in E(\mathbb{C})$. Thus $\deg(K) = 2g - 2 = 0$.

For any $r \in \mathbb{N} - \{\,0\,\}$, $\ell(rO_E) - \ell(K - rO_E) = 1 - g + \deg(rO_E)$. Note that $\deg(K - rO_E) < 0$ and hence $\ell(K - rO_E) = 0$. Therefore $\ell(rO_E) = 1 - 1 + r = r$. Thus we have the following:

$\mathscr{L}(O_E) \cong \mathbb{C} \cong \{\,\text{constant functions}\,\}$.

There exists $x \in \mathscr{L}(2O_E) - \mathscr{L}(O_E)$ (x is a meromorphic function with a pole of order 2 at O_E and no other poles) such that $\mathscr{L}(2O_E) = \mathbb{C} \oplus \mathbb{C}x$.

There exists $y \in \mathscr{L}(3O_E) - \mathscr{L}(2O_E)$ (y is meromorphic function with a pole of order 3 at O_E and no other poles) such that $\mathscr{L}(3O_E) = \mathbb{C} \oplus \mathbb{C}x \oplus \mathbb{C}y$.

$\mathscr{L}(4O_E) = \mathbb{C} \oplus \mathbb{C}x \oplus \mathbb{C}y \oplus \mathbb{C}x^2$.

$\mathscr{L}(5O_E) = \mathbb{C} \oplus \mathbb{C}x \oplus \mathbb{C}y \oplus \mathbb{C}x^2 \oplus \mathbb{C}xy$.

$\mathscr{L}(6O_E) = \mathbb{C} + \mathbb{C}x + \mathbb{C}y + \mathbb{C}x^2 + \mathbb{C}xy + \mathbb{C}y^2 + \mathbb{C}x^3$. The seven elements $1\,, x\,, y\,, x^2\,, xy\,, y^2\,, x^3 \in \mathscr{L}(6O_E)$ must be linearly dependent over $\mathbb{C}$. Therefore we have an equation (changing x to $\alpha x + \beta$ if necessary) of the form

$$y^2 + a_1xy + a_3 = x^3 + a_4x^2 + a_6x\ .$$

1.3.5 The Riemann-Hurwitz Formula

Let $f : Y \longrightarrow X$ be a holomorphic function of compact Riemann surfaces. Suppose that f is non-constant. Let $d = \deg(f)$. Then for almost all $P \in X$, $|f^{-1}(P)| = d$.

Let $Q \in Y$, $P = f(Q) \in X$. One may choose local charts $(U_Q\,, z_Q) \longrightarrow D := B(0\,, 1)$ such that $Q \mapsto 0$ and $(U_P\,, z_P) \longrightarrow D = B(0\,, 1)$ such that $P \mapsto 0$. Then

$$g = z_P \circ f \circ z_Q^{-1} \,:\, z_Q(U_Q) \longrightarrow z_P(U_P)$$

is holomorphic and $g(0) = 0$.

By definition, the ***ramification index*** $e_{Q/P}$ is the order at 0 of g. (This is independent of the choice of the local charts.) That is,

$$g(z) = az^{e_{Q/P}} + (\text{higher order terms}), \qquad \text{with } a \neq 0.$$

If $f^{-1}(P) = \{\,Q_1\,, \ldots\,, Q_r\,\}$, then $\sum_{i=1}^{r} e_{Q_i/P} = d$. A point $P \in X$ such that $|f^{-1}(P)| < d$ is called a ***ramification point*** of f. A point $Q \in Y$ such that $e_{Q/P} > 1$ is also called a *ramification point*.

Theorem 1.3.8 (***Riemann-Hurwitz Formula***)**.**

$$2g_Y - 2 = d(2g_X - 2) + \sum_{P \in X} \sum_{Q \mapsto P} (e_{Q/P} - 1).$$

Proof. Let ω be a meromorphic differential form on X without poles or zeroes at the ramification points.

Exercise 1.9. Prove the existence of such ω.

Let $Q \in Y$ be a point such that $f(Q) = P \in X$. If P is a point at which ω has no pole or zero and $e_{Q/P} = 1$, then $f^*\omega$ has no pole or zero at Q. If ω has a pole or a zero of order r at P (therefore $e_Q = 1$, by hypothesis), then $f^*\omega$ has a pole or zero of order r at Q. If $e_Q > 1$, $g = z_P \circ f \circ z_Q^{-1}$ has a zero of order $e_{Q/P}$ at 0. If $\omega = \theta(z_P)dz_P$ on $z_P(U_P)$, then $g^*\omega = \theta(g(z_Q))g'(z_Q)dz_Q$ has a zero of order $e_{Q/P} - 1$ at Q, as θ has no zero or pole at P.

Putting all these together, we reach the conclusion

$$2g_Y - 2 = \deg(f^*\omega) = r \cdot \deg(\omega) + \sum_P \sum_{Q \mapsto P} (e_{Q/P} - 1).$$

□

Example 1.7. Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index and $X(\Gamma) = \Gamma\backslash\mathbb{H}^* = \Gamma\backslash\mathbb{H} \cup \{ c_1, \ldots, c_r \}$. Let $\varphi : X(\Gamma) \longrightarrow X(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$ be the natural map, then

$$\deg\varphi = \begin{cases} [\mathrm{SL}_2(\mathbb{Z}) : \Gamma] & \text{if } -1 \in \Gamma \\ \frac{1}{2}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] & \text{if} -1 \notin \Gamma \end{cases}.$$

That is,

$$\deg\varphi = d := \left| \mathrm{SL}_2(\mathbb{Z})/\pm\Gamma \right| = \left| \mathrm{PSL}_(\mathbb{Z})/\overline{\Gamma} \right|$$

where $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm \mathrm{Id}\}$ and $\overline{\Gamma}$ is the image of Γ in $\mathrm{PSL}_2(\mathbb{Z})$.

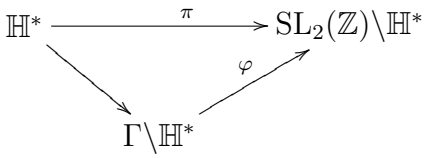
Theorem 1.3.9. *Let $\varphi : X(\Gamma) \longrightarrow X(1)$ be the natural map and $d = \deg\varphi$. Let ν_2 be the number of Γ-orbits of elliptic points of order 2 for Γ, ν_3 be the number of Γ-orbits of elliptic points of order 3 for Γ, and ν_∞ be the number of Γ-orbits of cusps. Then*

$$g = g(X(\Gamma)) = 1 + \frac{d}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}.$$

(ex. $g(\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*) = 0$, as $d = \nu_2 = \nu_3 = \nu_\infty = 1$.)

Proof. We'll give later a proof of the fact that $g(\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*) = 0$. This will be a consequence of the existence of the j-map: $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^* \longrightarrow \mathbb{P}^1(\mathbb{C})$, having only a simple pole at ∞ and $\deg(j) = 1$.

We have a factorization



Let $Q \in \Gamma\backslash\mathbb{H}^*$ be the image of a point $R \in \mathbb{H}^*$ and $P = \varphi(Q) = \pi(R)$.

Exercise 1.10. When the ramification indices are finite, we have $e_{R/P} = e_{R/Q} \cdot e_{Q/P}$.

If $P = \pi(\mathrm{i})$ ($\mathrm{i} = \sqrt{-1}$), then $e_{R/P} = 2$ and

$$\text{either } Q \text{ is of type I}: \begin{cases} e_{Q/P} = 1 \\ e_{R/Q} = 2 \end{cases} \quad \text{or } Q \text{ is of type II}: \begin{cases} e_{Q/P} = 2 \\ e_{R/Q} = 1 \end{cases} .$$

In the first case, Q is elliptic of order 2 and φ is unramified at Q. In the second case, φ is ramified of order 2 at Q. So ν_2 is the number of the points of type I. Let k be the number of points of type II. Then $\nu_2 + 2k = d$, hence $k = \frac{d-\nu_2}{2}$ and

$$\sum_{Q \mapsto \pi(\mathrm{i})} (e_{Q/\pi(\mathrm{i})} - 1) = k = \frac{d - \nu_2}{2} .$$

If $P = \pi(\rho)$ then

$$\text{either } Q \text{ is of type I}': \begin{cases} e_{Q/P} = 3 \\ e_{R/Q} = 1 \end{cases} \quad \text{or } Q \text{ is of type II}': \begin{cases} e_{Q/P} = 1 \\ e_{R/Q} = 3 \end{cases} .$$

Let l be the number of elements of the type II′. Then $\nu_3 + 3l = d$ and therefore $l = \frac{d-\nu_3}{3}$,

$$\sum_{Q \mapsto \pi(\rho)} (e_{Q/\pi(\rho)} - 1) = 2l = \frac{2d - 2\nu_3}{3}.$$

If $P = \pi(\infty)$, there are ν_∞ points of $X(\Gamma)$ above P and

$$\sum_{Q \mapsto \pi(\infty)} (e_{Q/P} - 1) = \sum_{Q \mapsto \pi(\infty)} e_Q - \sum_{Q \mapsto \pi(\infty)} 1 = d - \nu_\infty .$$

By the Riemann-Hurwitz Formula, we have, using $-2 = 2g(\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*) - 2$,

$$2g - 2 = d \cdot (-2) + \frac{d - \nu_2}{2} + \frac{2}{3}(d - \nu_3) + d - \nu_\infty$$

from which it follows

$$g = g_\Gamma = 1 + \frac{d}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2} \ .$$

□

Exercise 1.11. (1) Let $\lambda_N : \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ be the natural map. Prove that λ_N is a surjective map with kernel $\Gamma(N)$ which is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

(2) If $N = \prod_p p^{e_p}$, then $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \prod_p \mathrm{SL}_2(\mathbb{Z}/p^{e_p}\mathbb{Z})$.

(3) $|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})| = N^3 \prod_{p\,|\,N}(1 - \frac{1}{p^2})$.

(4) Let $\pi_N : X(N) = X(\Gamma(N))$ be the natural map, then

$$\deg(\pi_N) = \begin{cases} \frac{N^3}{2} \prod_{p\,|\,N}(1 - \frac{1}{p^2}) & \text{if } N \geq 3 \\ 6\,, & \text{if } N = 2 \end{cases}.$$

(5)

$$\nu_\infty = \begin{cases} \frac{N^2}{2} \prod_{p\,|\,N}(1 - \frac{1}{p^2}) & \text{if } N = 3 \\ 2\,, & \text{if } N = 2 \end{cases}.$$

(6) If $N > 2$, $\Gamma(N)$ has no elliptic points (i.e, $\nu_2 = \nu_3 = 0$).

(7) $g(X(N)) = g = 1 + \frac{N^2}{24}(N-6) \prod_{p\,|\,N}(1 - \frac{1}{p^2})$ for $N > 2$.

1.4 Modular Functions and Modular Forms

1.4.1 Definitions

Let $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ and let Γ be a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$.

Definition 1.10. A ***modular function*** for Γ is a meromorphic function on the compact Riemann surface $X(\Gamma) = \Gamma\backslash\mathbb{H}^*$. A modular function is given by a function f on $\mathbb{H}^*$ such that

(a) $\forall \gamma \in \Gamma$, $\forall z \in \mathbb{H}^*$, $f(\gamma \cdot z) = f(z)$;

(b) $f(z)$ is meromorphic on $\mathbb{H}$;

(c) $f(z)$ is "meromorphic" at the cusps of Γ.

At the cusp $c = \Gamma \cdot \infty = \infty$,

$$\mathrm{Fix}_\Gamma(\infty) = \pm\Big\{ \begin{pmatrix} 1 & nh \\ 0 & 1 \end{pmatrix} \ \Big|\ n \in \mathbb{Z} \Big\}.$$

As $f(\left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right)z) = f(h+z) = f(z)$, f defines a function $\bar{f}$ on $\mathrm{Fix}_\Gamma(\infty)\backslash U_N$ which is a neighborhood of ∞, and we have a Fourier expansion in the local parameter $q = e^{2\pi \mathrm{i} z/h}$. We write $f^*(q) = \sum_{n\in\mathbb{Z}} a_n q^n$ for this expansion. Then by definition, "f is meromorphic at ∞" means $\bar{f}$ is meromorphic at ∞, which is equivalent to $f^*(q) = \sum_{n\geq N_0} a_n q^n$ for some $N_0 \in \mathbb{Z}$. And by definition, "f is holomorphic at ∞" means $f^*(q) = \sum_{n\geq 0} a_n q^n$.

At a cusp $c = \sigma\cdot\infty$, for some $\sigma \in \mathrm{SL}_2(\mathbb{Z})$,

$$\mathrm{Fix}_\Gamma(c) = \mathrm{Fix}_{\sigma^{-1}\Gamma\sigma}(\infty) = \pm\Big\{\begin{pmatrix}1 & nh_c\\ 0 & 1\end{pmatrix} \Big| n\in\mathbb{Z}\Big\}.$$

The function $f_\sigma = f(\sigma z)$ is invariant by $\sigma^{-1}\Gamma\sigma$ and therefore has a Fourier expansion in the parameter $q = e^{2\pi \mathrm{i} z/h_c}$. The condition "$f$ is holomorphic or meromorphic at c" is checked using this Fourier expansion.

Example 1.8. As $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ is generated by $S = \left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$, the condition (a) in definition.1.10 for Γ is equivalent to

(a′) $f(-\frac{1}{z}) = f(z) = f(z+1)$, $\forall z \in \mathbb{H}^*$.

Definition 1.11. A ***weight*** $2k$ ***modular form*** for Γ is a function f on $\mathbb{H}$ such that

(a) if $\gamma = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in\Gamma$, then $f(\gamma z) = (cz+d)^{2k} f(z)$, $\forall z\in\mathbb{H}$;

(b) $f(z)$ is holomorphic in $\mathbb{H}$;

(c) "$f(z)$ is holomorphic at the cusps of $X(\Gamma)$".

Explanation for (c): Once more taking $\gamma = \left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right)\in\Gamma$ (as for modular functions) we see that $f(\gamma\cdot z) = f(z+h) = f(z)$. Therefore f defines a function $\bar{f}$ on $\mathrm{Fix}_\Gamma(\infty)\backslash U_N$. We say that "$f$ is holomorphic or meromorphic at ∞" if $\bar{f}$ is holomorphic or meromorphic at ∞. We just write the Fourier expansion $f^*(q) = \sum_{n\in\mathbb{Z}} a_n q^n$ to check (c).

Definition 1.12. A modular form is said to be ***cuspidal*** if its value at all cusps is 0.

Definition 1.13. A meromorphic function on $\mathbb{H}^*$ verifying (a) of definition.1.11 is said to be a ***meromorphic modular form***.

With this terminology, "modular function" is equivalent to "weight 0 meromorphic form".

Lemma 1.4.1. *Let $\omega = f(z)dz$ be a meromorphic differential form on $\mathbb{H}$. $\gamma = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in\Gamma$. Then $\gamma^*\omega = \omega \Longleftrightarrow f(\gamma\cdot z) = (cz+d)^2 f(z)$ and hence ω is Γ-invariant $\Longleftrightarrow$ f is a meromorphic weight 2 modular form.*

In this situation, let $\pi_\Gamma : \mathbb{H}^* \longrightarrow \Gamma\backslash\mathbb{H}^*$ be the natural map, then there exists a meromorphic differential form α on $\Gamma\backslash\mathbb{H}^*$ such that $\omega = \pi_\Gamma^*\alpha$.

Proof.

$$\mathrm{d}(\gamma\cdot z)=\mathrm{d}(\frac{az+b}{cz+d})=\frac{a(cz+d)-c(az+b)}{(cz+d)^2}\mathrm{d}z=\frac{\mathrm{d}z}{(cz+d)^2}.$$

Therefore, $\gamma^*\omega=f(\gamma\cdot z)\mathrm{d}(\gamma\cdot z)=\frac{f(\gamma z)}{(cz+d)^2}\mathrm{d}z$. □

Exercise 1.12. Prove that f is holomorphic in $\mathbb{H}$ if and only if α is holomorphic on $\Gamma\backslash\mathbb{H}$. (Caution: Be careful with elliptic points of Γ.)

Lemma 1.4.2. *f is holomorphic at a cusp c if and only if α has a pole of order at most 1 at c, and $f(c)=0$ if and only if α is holomorphic at c.*

Proof. Assume $c=\infty$, $\omega=f(z)dz$. For $q=e^{2\pi\mathrm{i}z/h}$, $dq=\frac{2\pi\mathrm{i}}{h}qdz$.

$$\begin{aligned} f \text{ holomorphic at } \infty &\iff f^*(q)=\sum_{n\geq 0}a_nq^q \\ &\iff \alpha=\frac{h}{2\pi\mathrm{i}}(\sum_{n\geq 0}a_nq^n)\frac{dq}{q}. \end{aligned}$$

□

We therefore get the following proposition.

Proposition 1.4.3.

$\mathcal{M}_2(\Gamma):=\{$ *weight 2 modular forms for* $\Gamma\}$
$\cong\{$*meromorphic differential forms on* $X(\Gamma)$ *which are holomorphic in* $\Gamma\backslash\mathbb{H}$ *with at most simple poles at cusps of* $\Gamma\}$.

$\mathcal{S}_2(\Gamma):=\{$ *weight 2 cuspidal modular forms for* $\Gamma\}\cong\{$*holomorphic differential forms on* $X(\Gamma)\}$.

Theorem 1.4.4. *(a)* $\dim\mathcal{S}_2(\Gamma)=g$ *where* $g=g(X(\Gamma))$ *is the genus of* $X(\Gamma)$*;*
(b) $\dim\mathcal{M}_2(\Gamma)=g-1+\nu_\infty$ *where* ν_∞ *is the number of cusps for* Γ.

Proof. (a) $\dim\mathcal{S}_2(\Gamma)=\ell(K)=g$ by Riemann-Roch theorem.
(b)

$$\dim\mathcal{M}_2(\Gamma)=\ell(K+\sum_{c\text{ cusps}}c)=1-g+2g-2+\nu_\infty=g-1+\nu_\infty\ .$$

□

1.4.2 The Dimensions of $\mathcal{M}_{2k}(\Gamma)$ and $\mathcal{S}_{2k}(\Gamma)$

More generally, we can interpret weight $2k$ modular forms in terms of k-differential forms on $X(\Gamma)$.

A k-differential form is written locally $\omega = f(z)dz^{\otimes k}$ with f meromorphic with the rule

$$\theta^*(\omega) = f(\theta(z))(d\theta(z))^{\otimes k} = f(\theta(z))\theta'(z)^k dz^{\otimes k}.$$

Lemma 1.4.5. *The space of weight $2k$ meromorphic forms for Γ is isomorphic to the space of meromorphic k-differential forms on $\Gamma\backslash\mathbb{H}^*$.*

Proof. Just use $d(\gamma \cdot z)^{\otimes k}\frac{dz^{\otimes k}}{(cz+d)^{2k}}$ to do the computation. □

Let $f(z)dz^{\otimes k} = \pi_\Gamma^*\alpha$, we need to discuss the relation between the holomorphy of f and the holomorphy of α.

Remark 1.8.

$$\mathcal{M}_0(\Gamma) = \{\text{holomorphic functions on } \Gamma\backslash\mathbb{H}^*\} \cong \mathbb{C}.$$

$\mathcal{S}_0(\Gamma) = \{\text{holomorphic functions on } \Gamma\backslash\mathbb{H}^* \text{ such that } f = 0 \text{ at all cusps }\} = \{\,0\,\}$.

Theorem 1.4.6. *Let $k \geq 1$.*

(a)

$$\dim \mathcal{M}_{2k}(\Gamma) = (2k-1)(g-1) + \sum_{P \text{ elliptic on } \Gamma\backslash\mathbb{H}} [k(1-\frac{1}{e_P})] + k\nu_\infty\ .$$

(b)

$$\dim \mathcal{S}_{2k}(\Gamma) = \begin{cases} g, & \text{if } k = 1 \\ (2k-1)(g-1) + \sum\limits_{P \text{ elliptic on } \Gamma\backslash\mathbb{H}} [k(1-\frac{1}{e_P})] + \nu_\infty(k-1), & \text{if } k > 1 \end{cases}$$

with ν_∞ the number of cusps of $X(\Gamma)$, e_P the ramification index at P(so $e_P = \#\{\,\mathrm{Stab}_\Gamma(P)/\{\,\pm\mathrm{Id}\,\}\,\}$) and $[\alpha]$ =the integer part of α.

The proof of this theorem is an application of the Riemann-Roch formula.

Lemma 1.4.7. *Let $\varphi : D_0 = D \longrightarrow D_1 = D$ be the map: $z \mapsto z^e$, with $D = \{\, z \in \mathbb{C} \,|\, |z| < 1 \,\}$. Let f be a meromorphic function on D_1 and let $\omega = f(z_1)(dz_1)^{\otimes k}$ and $\omega^* = \varphi^*\omega$. Then*

(a) $\mathrm{Ord}_0(\varphi^* f) = e\mathrm{Ord}_0(f)$;

(b) $\mathrm{Ord}_0(\varphi^*\omega) = e\mathrm{Ord}_0(\omega) + k(e-1)$.

Proof. If $f(z_1) = az_1^m(1+o(1))$ with $a \neq 0$, then $\varphi^*(f)(z) = f(\varphi(z)) = f(z^e) = az_1^{em}(1+o(1))$. This proves (a).

(b) $\varphi^*\omega = f(z^e)(ez^{e-1})^k dz^{\otimes k}$. Therefore $\mathrm{Ord}_0(\varphi^*\omega) = e\mathrm{Ord}_0(\omega) + k(e-1)$. □

Lemma 1.4.8. *Let f be a modular form of weight $2k$ on $\mathbb{H}$. Let $\omega = f(z)dz^{\otimes k}$ the associated k-differential form on $\mathbb{H}^*$. Suppose the map $\pi_\Gamma : \mathbb{H}^* \longrightarrow \Gamma\backslash\mathbb{H}^*$ sends a point $Q \in \mathbb{H}^*$ to $P \in \Gamma\backslash\mathbb{H}^*$. Write $\omega = \pi_\Gamma^*\alpha$ with α a k-differential form on $X(\Gamma)$.*

(a) If P is an elliptic point of order e, then

$$\mathrm{Ord}_Q(f) = \mathrm{Ord}_Q(\omega) = e\mathrm{Ord}_P(\alpha) + k(e-1).$$

(b) If Q is a cusp then $\mathrm{Ord}_Q(f) = \mathrm{Ord}_P(\alpha) + k$.

Proof. (a) follows from Lemma.1.4.7 and the description of the complex structure on $X(\Gamma)$ near an elliptic point.

(b) Consider the function

$$q = e^{2\mathrm{i}\pi z/h} : \langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \rangle \backslash \{ z \in \mathbb{C} \mid \mathrm{Im}(z) > N \} \longrightarrow D = B(0, e^{-\frac{2\pi N}{h}})$$

Since $dz = \frac{h}{2\mathrm{i}\pi}\frac{dq}{q}$, $\alpha = f^*(q)(\frac{h}{2\mathrm{i}\pi q})^k dq^{\otimes k}$ and hence $\mathrm{Ord}_\infty(\alpha) = \mathrm{Ord}_\infty(f) - k$. □

Proof of Thm.1.4.6. Let $f \in \mathcal{M}_{2k}(\Gamma)$, $\omega = f(z)dz^{\otimes k} = \pi_\Gamma^*(\alpha)$. Then f is holomorphic in $\mathbb{H}^*$ if and only if

$$\begin{cases} \mathrm{Ord}_Q(f) = e_P\mathrm{Ord}_P(\alpha) + k(e_P - 1) \geq 0\,, & \text{if } P \text{ is in } \Gamma\backslash\mathbb{H}^* \\ \mathrm{Ord}_c(f) = \mathrm{Ord}_c(\alpha) + k \geq 0\,, & \text{if } c \text{ is a cusp of } \Gamma \end{cases}.$$

We fix a k-differential form α_0, and we write $\alpha = h\alpha_0$ for some $k \in \mathcal{M}(X)$. Then $\alpha \in \mathcal{M}_{2k}(\Gamma)$ if and only if

$$\begin{cases} \mathrm{Ord}_P(h) + \mathrm{Ord}_P(\alpha_0) + k(1 - \frac{1}{e_P}) \geq 0\,, & \text{if } P \text{ is in } \Gamma\backslash\mathbb{H}^* \\ \mathrm{Ord}_c(h) + \mathrm{Ord}_c(\alpha_0) + k \geq 0\,, & \text{if } c \text{ is a cusp of } \Gamma \end{cases}.$$

and hence if and only if $h \in \mathscr{L}(D)$ where

$$D = \mathrm{div}(\alpha_0) + \sum_{c \text{ cusps}} k \cdot [c] + \sum_{P \text{ elliptic}} [k(1 - \frac{1}{e_P})] \cdot [P]\,.$$

We have $\deg(D) = k(2g-2) + \nu_\infty k + \sum_{P \text{ elliptic}} [k(1-\frac{1}{e_P})]$ and by Riemann-Roch formula

$$\begin{aligned}\ell(D) &= 1 - g + \deg(D) \\ &= (g-1)(2k-1) + \nu_\infty k + \sum_{P \text{ elliptic}} [k(1-\frac{1}{e_P})] \,.\end{aligned}$$

Finally, for the case of $\mathcal{S}_{2k}(\Gamma)$, $\alpha = h\alpha_0 \in \mathcal{S}_{2k}(\Gamma) \Longleftrightarrow h \in \mathscr{L}(D)$ with

$$D = \operatorname{div}(\alpha_0) + \sum_{c \text{ cusps}} (k-1)\cdot[c] + \sum_{P \text{ elliptic}} [k(1-\frac{1}{e_P})]\cdot[P] \,.$$

Just apply Riemann-Roch formula once more, one gets the result. □

Proposition 1.4.9 (Location of zeroes)**.** *Let f be a weight $2k$ modular form for Γ. Then*

$$\sum_{Q \mapsto P \in \Gamma\backslash\mathbb{H}^*} \big(\frac{\operatorname{Ord}_Q(f)}{e_Q} - k(1-\frac{1}{e_Q})\big) = (2g-2)k + k\nu_\infty$$

where the sum is on points of $\Gamma\backslash\mathbb{H}^*$, Q is an arbitrary point above P and $e_Q = e_{Q/P}$ is the ramification index if $P \in \Gamma\backslash\mathbb{H}$ and $e_Q = 1$ if P is a cusp.

Proof. We write $\omega = f(z)dz^{\otimes k} = \pi_\Gamma^*\alpha$. By lemma.1.4.8,

$$\operatorname{Ord}_P(\alpha) = \begin{cases} \frac{\operatorname{Ord}_Q(f)}{e_Q} - k(1-\frac{1}{e_Q})\,, & \text{if } P \text{ is not a cusp} \\ \operatorname{Ord}_Q(f) - k\,, & \text{if } P \text{ is a cusp} \end{cases}.$$

Therefore,

$$\sum_P \operatorname{Ord}_P(\alpha) = k(2g-2) = \sum_Q \big(\frac{\operatorname{Ord}_Q(f)}{e_Q} - k(1-\frac{1}{e_Q})\big) - k\nu_\infty.$$

□

Example 1.9. Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, $f \in \mathcal{M}_{2k}(\Gamma)$. Then

$$\operatorname{Ord}_\infty(f) + \frac{\operatorname{Ord}_{\mathrm{i}}(f)}{2} + \frac{\operatorname{Ord}_\rho(f)}{3} + \sum_{P \in \Gamma\backslash\mathbb{H}, P \notin \{\Gamma\mathrm{i}, \Gamma\rho, \Gamma\infty\}} \operatorname{Ord}_P(f) = \frac{k}{6} \,.$$

Corollary 1.4.10. *Let* $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

(i)

$$\dim \mathcal{M}_{2k}(\Gamma) = \begin{cases} 1\,, & \text{if } k = 0 \\ 1 - k + \left[\frac{k}{2}\right] + \left[\frac{2k}{3}\right], & \text{if } k > 0 \end{cases}$$

or equivalently,

$$\dim \mathcal{M}_{2k}(\Gamma) = \begin{cases} \left[\frac{k}{6}\right], & \text{if } k \equiv 1 \pmod 6 \\ 1 + \left[\frac{k}{6}\right], & \text{if } k \not\equiv 1 \pmod 6 \end{cases}.$$

(ii) $\dim \mathcal{M}_4(\Gamma) = 1$. *Therefore, if* $f \in \mathcal{M}_4(\Gamma) - \{0\}$ *then*

$$\mathrm{Ord}_\infty(f) + \frac{\mathrm{Ord}_{\mathrm{i}}(f)}{2} + \frac{\mathrm{Ord}_\rho(f)}{3} + \sum_{P \in \Gamma\backslash\mathbb{H}, P \notin \{\Gamma\mathrm{i}, \Gamma\rho, \Gamma\infty\}} \mathrm{Ord}_P(f) = \frac{1}{3}\,.$$

This means f *has a simple zero at* ρ *and no other zeros.*

(iii) $\dim \mathcal{M}_6(\Gamma) = 1$. *Therefore, if* $f \in \mathcal{M}_6(\Gamma) - \{0\}$ *then* f *has a simple zero at* i *and no other zeros.*

(iv) $\dim \mathcal{S}_{12}(\Gamma) = 1$. *Therefore, if* $f \in \mathcal{S}_{12}(\Gamma) - \{0\}$ *then* f *has only one simple zero at some non-elliptic point.*

1.5 Examples of Modular Forms

1.5.1 $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ as a Moduli space for Lattices and Elliptic Curves

A lattice Γ in $\mathbb{C}$ is a discrete subgroup of $\mathbb{C}$ such that $\mathbb{C}/\Gamma$ is compact. There exists $\omega_1, \omega_2 \in \mathbb{C} - \{0\}$ such that $\Gamma = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ with $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. Changing ω_1 by $-\omega_1$ if necessary, we may assume that $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$.

Let $\mathscr{M} = \{(\omega_1, \omega_2)\,;\, \frac{\omega_1}{\omega_2} \notin \mathbb{R}\,, \mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0\}$ and let $\mathscr{R}$ be the space of lattices of $\mathbb{C}$. The map $\varphi : \mathscr{M} \to \mathscr{R}$; $(\omega_1, \omega_2) \mapsto \Gamma = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ is surjective.

$\mathbb{C}^*$ acts on $\mathscr{R}$ by multiplicity and we have an isomorphism

$$\mathbb{C}^*\backslash\mathscr{M} \cong \mathbb{H}$$
$$(\omega_1, \omega_2) \mapsto z = \frac{\omega_1}{\omega_2}\,.$$

We therefore get a surjective morphism $\mathbb{H} \to \mathscr{R}/\mathbb{C}^*$:= space of lattices modulo homotheties. There is also an action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathscr{M}$ given by

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\omega_1, \omega_2) = (a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$. The induced action on $\mathbb{H} = \mathbb{C}^*\backslash\mathscr{M}$ is the usual action.

If $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ and if (ω_1, ω_2) is a basis of Γ, then $\alpha \cdot (\omega_1, \omega_2)$ is a basis of Γ such that $\mathrm{Im}(\frac{a\omega_1+b\omega_2}{c\omega_1+d\omega_2}) > 0$.

If (ω_1, ω_2) and (ω_1', ω_2') are two basis of Γ with $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$, $\mathrm{Im}(\frac{\omega_1'}{\omega_2'}) > 0$, then there exists an $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ such that $(\omega_1', \omega_2') = \alpha \cdot (\omega_1, \omega_2)$.

So we have the isomorphisms $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \simeq$\{lattices of $\mathbb{C}$\}/ \{homotheties\} $= \mathscr{R}/\mathbb{C}^*$ and the following diagram

$$\begin{array}{ccccc} \mathscr{M} & \xrightarrow{\gamma} & \mathscr{M} & \xrightarrow{\varphi} & \mathscr{R} \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{H} = \mathbb{C}^*\backslash\mathscr{M} & \xrightarrow{\gamma} & \mathbb{H} = \mathbb{C}^*\backslash\mathscr{M} & \xrightarrow{\overline{\varphi}} & \mathbb{C}^*\backslash\mathscr{R} \simeq \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \end{array}$$

where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Link with the theory of elliptic curves

- For any lattice $\Gamma \subset \mathbb{C}$, $E = \mathbb{C}/\Gamma$ is a Riemann surface of genus 1, endowed with the structure of an abelian group with origin O.
- Two lattices Γ and Γ' define isomorphic elliptic curves $E = \mathbb{C}/\Gamma \simeq E' = \mathbb{C}/\Gamma'$ if and only if there exists an $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma = \alpha \cdot \Gamma'$.
- Any elliptic curve (a compact Riemann surface with a fixed origin) is obtained in this way.

Conclusion: $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \simeq$ {isomorphism classes of elliptic curves over $\mathbb{C}$} $\simeq$ {lattices of $\mathbb{C}$ module homotheties} $= \mathbb{C}^*\backslash\mathscr{R}$. That is, $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is the moduli space for lattices and elliptic curves.

Definition 1.14. A function $F : \mathscr{R} \to \mathbb{C}$ is said to be a "***lattice function of weight*** $2k$"(or *homogeneous of weight* $-2k$) if for any $\Gamma \in \mathscr{R}$ and any $\lambda \in \mathbb{C}^*$, we have $F(\lambda\Gamma) = \lambda^{-2k}F(\Gamma)$.

Let F be a lattice function of weight $2k$ and F_M the associated function on $\mathscr{M}$. $F_M((\omega_1, \omega_2)) := F(\varphi(\omega_1, \omega_2)) = F(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2)$. Then $F_M((\omega_1, \omega_2)) = F_M(\omega_2(\frac{\omega_1}{\omega_2})) = \omega_2^{-2k}F_M((\frac{\omega_1}{\omega_2}, 1))$. Let f be the assoicated function on $\mathbb{H}$ defined by $f(z) = F_M((z, 1))$.

Remark 1.9. For any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, $f(\frac{az+b}{cz+d}) = (cz + d)^{2k}f(z)$.

Proof.

$$\begin{aligned} f(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) &= F_M(((\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), 1)) = (cz+d)^{2k} F_M((az+b, cz+d)) \\ &= (cz+d)^{2k} F_M(\gamma \cdot (z,1)) \\ &= (cz+d)^{2k} F_M((z,1)) \qquad \text{as } F \text{ is invariant by } \mathrm{SL}_2(\mathbb{Z}) \\ &= (cz+d)^{2k} f(z) \end{aligned}$$

□

If f is a function on $\mathbb{H}$ such that $f(\frac{az+b}{cz+d}) = (cz+d)^{2k} f(z)$, then there exist a unique weight $2k$ lattice funciton $F : \mathscr{R} \to \mathbb{C}$ such that $f(z) = F_M((z,1)) = F(\mathbb{Z} \oplus \mathbb{Z}z)$.

Remark 1.10. It's not easy to check the holomorphy condition on the definition of lattice functions.

Example 1.10. Let Γ be a lattice and $k > 1$, we define

$$G_{2k}(\Gamma) = \sum_{\gamma \in \Gamma - \{0\}} \frac{1}{\gamma^{2k}} .$$

Then $G_{2k}(\Gamma)$ is a weight $2k$ lattice function. The associated modular function is

$$G_{2k}(z) = G_{2k}(\mathbb{Z} \oplus z\mathbb{Z}) = \sum_{(m,n) \neq (0,0)} \frac{1}{(nz+m)^{2k}} .$$

Exercise 1.13. Prove that the series

$$\sum_{\gamma \in \Gamma - \{0\}} \frac{1}{|\gamma|^{\sigma}}$$

is convergent if $\sigma > 2$.

Proposition 1.5.1. *$\forall k > 1$, G_{2k} is a weight $2k$-modular form for $\mathrm{SL}_2(\mathbb{Z})$ (i.e. it is holomorphic on $\mathbb{H}^*$) and $G_{2k}(\mathrm{i}\,\infty) = 2\zeta(2k)$.*

Proof. An exercise. Prove that it is correct to write

$$\lim_{z \to \mathrm{i}\infty} G_{2k}(z) = \sum_{(m\,,\,n) \neq (0\,,0)} \lim_{z \to \mathrm{i}\infty} \frac{1}{(nz+m)^{2k}} = \sum_{m \neq 0} \frac{1}{m^{2k}} = 2\zeta(2k) .$$

□

Definition 1.15. Let $g_4 = 60G_4$ and $g_6 = 140G_6$, then $\Delta = g_4^3 - g_6^2$ is a weight 12 cuspidal modular function for $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 1.5.2. *(a)* $\mathcal{M}_{2k}(\Gamma)$ *is of dimension* 1 *and is generated by* G_{2k} *for* $k = 2, 3, 4, 5$;

(b) the multiplication by Δ *defines an isomorphism* $\mathcal{M}_{2k}(\Gamma) \to \mathcal{S}_{2k}(\Gamma)\,;\ f \mapsto f \cdot \Delta\,;$

(c) $\bigoplus_{k\geq 0} \mathcal{M}_{2k}(\Gamma) = \mathbb{C}[G_4, G_6]$.

Proof. (a) An easy consequence of Riemann-Roch theorem and previous discussions.

(b) We know that $\Delta \in \mathcal{S}_{12}(\Gamma)$ and that Δ has a simple zero at ∞. Therefore, corollary 1.4.10 Δ has no other zeros. Then

$$\begin{aligned} \mathcal{S}_{2k}(\Gamma) &\longrightarrow \mathcal{M}_{2k-12}(\Gamma) \\ \alpha &\mapsto \alpha/\Delta \end{aligned}$$

is the inverse to $f \mapsto f \cdot \Delta$.

(c) We need to show that $\{G_4^n G_6^m | 4n + 6m = 2k\}$ is a basis for $\mathcal{M}_{2k}(\Gamma)$.

It is easy to check that there exist $n\,, m \in \mathbb{N}$ such that $4n + 6m = 2k$. Therefore, $g = G_4^n G_6^m \in \mathcal{M}_{2k}(\Gamma)$ and $g(\mathrm{i}\,\infty) \neq 0$. If $f \in \mathcal{M}_{2k}(\Gamma)$, then $f - \frac{f(\mathrm{i}\,\infty)}{g(\mathrm{i}\,\infty)} g \in \mathcal{S}_{2k}(\Gamma)$. Hence $f = \frac{f(\mathrm{i}\,\infty)}{g(\mathrm{i}\,\infty)} g + \Delta h$ with $h \in \mathcal{M}_{2k-12}(\Gamma)$. Using (a) and by induction, we see that $f \in \mathbb{C}[G_4, G_6]$.

We thus have a surjective morphism $\psi : \mathbb{C}[G_4, G_6] \longrightarrow \bigoplus_k \mathcal{M}_{2k}(\Gamma)$. If ψ is not an isomorphism, then there exists $R \in \mathbb{C}[X, Y]$ such that $R(G_4, G_6) = 0$. Using a "weight argument" (this will be explained later), there exists $P \in \mathbb{C}[X]$ such that $P\big(\frac{G_4^3}{G_6^2}\big) = 0$. So $\frac{G_4^3}{G_6^2}$ must be constant. This leads to a contradiction as $\begin{cases} G_6(\rho) = 0 \neq G_6(\mathrm{i}) \\ G_4(\rho) = 0 \neq G_4(\mathrm{i}) \end{cases}$ in view of corollary 1.4.10.

Weight Argument: Fix m_0 maximal such that $2n_0 + 3m_0 = k$. Then for any $n\,, m$ such that $2n + 3m = k = 2n_0 + 3m_0$ one has $\frac{n-n_0}{3} = \frac{m-m0}{2} \in \mathbb{N}$. Thus,

$$\sum_{2n+3m=k} \lambda_n G_4^n G_6^m = 0 \Leftrightarrow \sum_{2n+3m=k} \lambda_n \frac{G_4^{n-n_0}}{G_6^{m_0-m}} = 0 \Leftrightarrow \sum_{2n+3m=k} \lambda_n \big(\frac{G_4^3}{G_6^2}\big)^{\frac{n-n_0}{3}}\,.$$

Thus we find a $P \in \mathbb{C}[X]$ with the property required. □

Definition 1.16. Define

$$j := \frac{1728 g_4^3}{\Delta} = \frac{1728 g_4^3}{g_4^3 - 27 g_6^2}\,.$$

The function j is a modular function (of weight 0) with a simple pole at ∞ and a triple zero at ρ. The induced meromorphic function $j : \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^* \to \mathbb{P}^1(\mathbb{C})$ has a simple pole at ∞, a simple zero at $\Gamma\rho$ and no other poles or zeros. Therefore, j gives an isomorphism $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^* \to \mathbb{P}^1(\mathbb{C})$ and $g\big(\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*\big) = g\big(\mathbb{P}^1(\mathbb{C})\big) = 0$.

1.5.2 The Petersson Inner Product

Lemma 1.5.3. *The differential form* $d\mu_0 = \frac{dz\wedge dy}{2iy^2} = \frac{dx\wedge dy}{y^2}$ *is* $\mathrm{SL}_2(\mathbb{R})$*-invariant.*

Proof. For any $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$, we have

$$\mathrm{d}(\alpha z) = \frac{\mathrm{d}z}{(cz+d)^2} \ ; \ \ \mathrm{d}(\alpha\bar{z}) = \frac{\mathrm{d}\bar{z}}{(c\bar{z}+d)^2} \ ; \ \ \mathrm{Im}(\alpha z) = \frac{\mathrm{Im}(z)}{|cz+d|^2} \ .$$

Therefore, $\alpha^*(d\mu_0) = d\mu_0$. □

Definition 1.17. The associated metric $ds^2 = \frac{dx^2+dy^2}{y^2}$ and the associated volume form $d\mu_0 = \frac{dx\wedge dy}{y^2}$ are called the ***Poincaré metric*** and the ***Poincaré measure***.

Lemma 1.5.4. *Let* $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ *be a subgroup of finite index and* F *be a fundamental domain for* Γ*. Then* $\int_F \frac{dxdy}{y^2}$ *is independent of the choice of the fundamental domain and* $\int_F \frac{dxdy}{y^2} = \frac{\pi d}{3}$ *where* $d = \deg\varphi$*,* φ *is the natural map* $\Gamma\backslash\mathbb{H} \longrightarrow \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$.

Proof. Exercise. □

Lemma 1.5.5. *Let* f *be a weight* $2k$*-cuspidal modular form for* Γ*, then* $\forall\gamma \in \mathrm{SL}_2(\mathbb{Z})$*, there exists* $c = c_\gamma > 0$ *such that* $|f(\gamma\cdot z)| << e^{-cy}$ *,* $z = x+iy$.

Proof. We have a Fourier expansion $f(\gamma\cdot z) = \sum_{n=1}^{\infty} a_n e^{\frac{2\pi i n z}{h}}$ for some $h = h_\gamma \in \mathbb{N}^*$. Let $f(\gamma\cdot z) = a_{n_0} e^{\frac{2\pi i n_0 z}{h}}\cdot$(bounded function) with $a_{n_0} \neq 0$, then

$$\left| e^{\frac{2\pi i n_0 (x+\mathrm{i}y)}{h}} \right| = e^{-\frac{2\pi n_0 y}{h}} \ll e^{-cy} \ .$$

Hence $|f(\gamma\cdot z)| \ll e^{-cy}$. □

Lemma 1.5.6. *Let* $f, g \in \mathcal{M}_{2k}(\Gamma)$*, then the differential form* $f(z)\overline{g(z)}y^{2k-2}dxdy$ *is* Γ*-invariant.*

Proof. An easy exercise. □

Definition 1.18. Let F be a fundamental domain for Γ and $f, g \in \mathcal{S}_{2k}(\Gamma)$, then we define

$$\langle f, g\rangle_k := \int_F f(z)\overline{g(z)}y^{2k-2}dxdy\ .$$

This is independent of F and is well defined. $\langle\cdot,\cdot\rangle$ is a positive definite hermitian scalar product on $\mathcal{S}_{2k}(\Gamma)$, called the ***Petersson inner product***.

Remark 1.11. Actually, one can define $\langle f, g\rangle_k$ for $f \in \mathcal{S}_{2k}(\Gamma)$ and $g \in \mathcal{M}_{2k}(\Gamma)$.

1.5.3 Poincaré Series

We start with a function f on $\mathbb{H}$ and try $\sum_{\gamma\in\Gamma} f(\gamma\cdot z)$ which is formally invariant by Γ. But this is a never convergent process. However, if f is always invariant by a subgroup Γ_0, then $\sum_{\gamma\in\Gamma_0\backslash\Gamma} f(\gamma\cdot z)$ is well defined and invariant by Γ.

We want to do this for modular forms. Let $\overline{\Gamma}$ be the image of Γ in $\mathrm{PSL}_2(\mathbb{Z})$ and

$$\overline{\Gamma}_0 = \overline{\Gamma}\cap\left\{\left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right)\,\middle|\, n\in\mathbb{Z}\right\} = \left\{\left(\begin{smallmatrix}1 & nh\\ 0 & 1\end{smallmatrix}\right)\,\middle|\, n\in\mathbb{Z}\right\}$$

for some $h \in \mathbb{N}$.

Definition 1.19. The ***Poincaré series*** of weight $2k$ and character n for Γ is

$$\varphi_n(z) = \sum_{\bar\gamma\in\overline{\Gamma}_0\backslash\overline{\Gamma}} \frac{\exp(\frac{2\mathrm{i}\pi n\gamma z}{h})}{(cz+d)^{2k}}$$

where $\gamma = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$.

Observe that (a) $\left(\begin{smallmatrix}1 & nh\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) = \left(\begin{smallmatrix}a' & b'\\ c & d\end{smallmatrix}\right)$. Therefore, (c, d) depends on $\bar\gamma$ but not on a choice of a representative of γ in $\overline{\Gamma}$.

(b) $\forall\gamma_0 \in \overline{\Gamma}_0$, $\exp(\frac{2\pi\mathrm{i}n\gamma_0\gamma z}{h}) = \exp(\frac{2\pi\mathrm{i}n\gamma z}{h})$.

So $\varphi_n(z)$ is well-defined.

Theorem 1.5.7. *The Poincaré series $\varphi_n(z)$ for $n \geq 0$ and $2k > 2$ is absolutely uniformly convergent on compact subsets of $\mathbb{H}$ and is a weight $2k$-modular form for Γ. Moreover,*

(a) $\varphi_0(z)$ is zero at finite cusps of Γ and $\varphi_0(\mathrm{i}\,\infty) = 1$;

(b) $\forall n \geq 1$, $\varphi_n(z) \in \mathcal{S}_{2k}(\Gamma)$;

(c) The Poincaré series $\varphi_n(z)$ for $n \geq 1$ generates $\mathcal{S}_{2k}(\Gamma)$.

Proof. If $\bar{\gamma}_1 = \left(\begin{smallmatrix} a_1 & b_1 \\ c & d \end{smallmatrix}\right)$, $\bar{\gamma}_2 = \left(\begin{smallmatrix} a_2 & b_2 \\ c & d \end{smallmatrix}\right) \in \bar{\Gamma}$, then $\bar{\gamma}_1 = \bar{\gamma}_2$ in $\overline{\Gamma}_0 \backslash \overline{\Gamma}$. We therefore obtains

$$|\varphi_n(z)| \leq \sum_{\substack{(c,d)\neq(0,0) \\ \text{s.t. } \exists \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma}} \frac{1}{|cz+d|^{2k}} \leq \sum_{(c,d)\neq(0,0)} \frac{1}{|cz+d|^{2k}} < +\infty$$

when $2k > 2$ with a uniform and absolute convergence on any compact subset of $\mathbb{H}$.

Note that

$$\left| \exp\left(\frac{2\mathrm{i}\pi n\gamma z}{h}\right) \right| = \exp\left(-\frac{2\pi n}{h} \cdot \frac{y}{|cz+d|^2} \right) \leq 1 \ .$$

Lemma 1.5.8. *Define* $j : \Gamma \times \mathbb{H} \to \mathbb{C}$; $j(\gamma, z) = (cz+d)^2$, *then* $\jmath(\gamma, z)$ *is an automorphy factor* (*i.e.* $j(\gamma\gamma', z) = j(\gamma, \gamma' z) j(\gamma', z)$).

Proof. On the one hand, $(\gamma\gamma')^*(dz) = \frac{dz}{j(\gamma\gamma', z)}$. On the other hand,

$$(\gamma\gamma')^*(dz) = \gamma'^*(\gamma^* dz) = \gamma'^*(\frac{dz}{j(\gamma, z)}) = \frac{dz}{j(\gamma, \gamma' z) j(\gamma', z)} \ .$$

□

proof of (b). Let $\gamma' \in \overline{\Gamma}$, by the above lemma,

$$\begin{aligned} \varphi_n(\gamma' \cdot z) &= \sum_{\overline{\Gamma}_0 \backslash \overline{\Gamma}} \frac{\exp(\frac{2\mathrm{i}\pi n\gamma\gamma' z}{h})}{j(\gamma\,,\,\gamma' z)^k} \\ &= j(\gamma'\,,\,z)^k \sum_{\overline{\Gamma}_0 \backslash \overline{\Gamma}} \frac{\exp\left(\frac{2\mathrm{i}\pi n(\gamma\gamma')z}{h}\right)}{j(\gamma\gamma'\,,\,z)} \\ &= j(\gamma', z)^k \sum_{\overline{\Gamma}_0 \backslash \overline{\Gamma}} \frac{\exp(\frac{2\mathrm{i}\pi n\gamma z}{h})}{j(\gamma, z)^k} \\ &= j(\gamma', z)^k \varphi_n(z) = (cz+d)^{2k} \varphi_n(z) \ . \end{aligned}$$

proof of (a). At $K = i \cdot \infty$, let R be a system of representatives in $\overline{\Gamma}$ of $\overline{\Gamma}_0 \backslash \overline{\Gamma}$. We write $R = R_1 \bigsqcup R_2$ with $R_1 = \{\gamma \in R | c = 0\}$, $R_2 = \{\gamma \in R | c \neq 0\}$.

In fact R_1 is finite and $|R_1| = 1$, as if $c = 0$, then $d = \pm 1$ (note that here ad equals the determinant) and $\pm(c, d)$ determines the class modulo of $\overline{\Gamma}_0$.

We have

$$\sum_{\gamma\in R_2}\frac{|\exp(\frac{2i\pi n\gamma\gamma' z}{h})|}{|cz+d|^{2k}}\leq\sum_{\gamma\in R_2}\frac{1}{|cz+d|^{2k}}\longrightarrow 0$$

uniformly as $z\to i\infty$ (since $\mathrm{Re}(z)$ is bounded), and

$$\sum_{\gamma\in R_1}\frac{|\exp(\frac{2i\pi n\gamma\gamma' z}{h})|}{|cz+d|^{2k}}=\exp(-\frac{2\pi ny}{h})\longrightarrow\begin{cases}0\,, & \text{if } n>0\\ 1\,, & \text{if } n=0\end{cases}.$$

At a cusp $K\neq i\cdot\infty$, we fix $\gamma_K\in\mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_K\cdot K=\infty$. Let

$$\psi_n(z)=(\gamma z+\delta)^{-2k}\varphi_n(\gamma_K^{-1}\cdot z)\,,\qquad\text{where}\quad\gamma_k^{-1}=\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}\,.$$

We study ψ_n at $i\infty$.

$$\psi_n(z)=\sum_{\gamma\in R}\frac{\exp(\frac{2i\pi n\gamma\gamma_K z}{h})}{j(\gamma,\gamma_K z)^k j(\gamma,z)^k}=\sum_{\tau\in R\gamma_K}\frac{\exp(\frac{2i\pi n\tau z}{h})}{j(\tau,z)^k}\,.$$

One can check that a matrix in $R\cdot\gamma_K$ is never of the form $\pm\left(\begin{smallmatrix}1&*\\0&1\end{smallmatrix}\right)$.

The same proof gives $\psi_n(z)\to 0$ as $z\to i\infty$.

Proposition 1.5.9. *Let $f\in\mathcal{S}_{2k}(\Gamma)$, $f^*(q)=\sum_{n\geq 1}a_nq^n$, then*

$$\langle f,\varphi_n\rangle_k=\frac{h^{2k}(2k-2)!n^{1-2k}}{(4n)^{2k-1}}a_n\,.$$

This implies if $f\in\mathcal{S}_{2k}(\Gamma)$ and $f\perp\varphi_n$ for all $n\geq 1$, then $a_n=0\,,\ \forall n\geq 1$ and hence $f=0$. Therefore, (c) follows from the above proposition.

Proof of proposition.1.5.9. We have

$$\begin{aligned}\langle f\,,\,\varphi_n\rangle_k&=\sum_{\gamma\in\overline{\Gamma}_0\backslash\overline{\Gamma}}\int_F\frac{f(z)\exp\big(-\frac{2i\pi n\gamma\bar z}{h}\big)}{(c\bar z+d)^{2k}}y^{2k-2}dxdy\\&=\sum_{\gamma\in\overline{\Gamma}_0\backslash\overline{\Gamma}}\int_F f(\gamma z)\exp\big(-\frac{2i\pi n\gamma\bar z}{h}\big)\big(\frac{y}{|cz+d|^2}\big)^{2k}\frac{dxdy}{y^2}\\&=\sum_{\gamma\in\overline{\Gamma}_0\backslash\overline{\Gamma}}\int_F g(\gamma z)\frac{dxdy}{y^2}\end{aligned}$$

where

$$g(z)=f(z)\,\mathrm{Im}(z)^{2k}\exp\big(-\frac{2i\pi n\bar z}{h}\big)\,.$$

As g is invariant by $\overline{\Gamma}_0$ and as $\bigsqcup_{\gamma\in\overline{\Gamma}_0\backslash\overline{\Gamma}}\gamma\cdot F$ is a fundamental domain F_0 for $\overline{\Gamma}_0$, we may suppose $F_0=(0,h)\times\mathbb{R}_+^*$. Then

$$\begin{aligned}\langle f,\varphi_n\rangle_k &= \int_0^h\int_0^\infty f(z)e^{-\frac{2\mathrm{i}\pi n\bar{z}}{h}}y^{2k-2}dxdy\\ &= \sum_{l\geq 1}a_l\int_0^h \exp\big(\frac{2\mathrm{i}\pi x}{h}(l-n)\big)dx\int_0^\infty y^{2k-2}\exp\big(-\frac{2\pi}{h}(l+n)y\big)dy\\ &\Big(\text{ as }\ f(z)=\sum_{l\leq 1}a_l e^{\frac{2i\pi lz}{h}}\Big)\\ &= a_n h\int_0^\infty y^{2k-2}\exp(\frac{-4\pi n}{h}y)dy\end{aligned}$$

Exercise: Finish the remaining computation and justify the convergence. □

This finishes the proof of theorem.1.5.7. □

Remark 1.12. As $\dim\mathcal{S}_{2k}(\Gamma)<\infty$ and $\varphi_n\,|\,n\in\mathbb{N}$ is a system of generators of $\mathcal{S}_{2k}(\Gamma)$, there exist a lot of relations between the φ_n's.

Chapter 2

Hecke Operators and Hecke Algebras

2.1 Introduction

Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. We know that $\dim \mathcal{S}_{12}(\Gamma) = 1$ and that $\Delta = g_4^3 - 27g_6^2$ generates $\mathcal{S}_{12}(\Gamma)$. Let's write

$$\Delta = \sum_{n\geq 1} \tau(n) q^n = (2\pi)^{12} q \prod_{n=1}^{\infty} (1-q^n)^{24} .$$

We have $\tau(1) = 1$, $\tau(2) = -4$, $\tau(3) = 252$, $\tau(4) = -1472$, $\tau(11) = 534612$, $\tau(12) = -370944$.

Conjecture 2.1 (Ramanujan's Conjecture)**.** (*a*) *For any prime number* p, $|\tau(p)| \leq 2p^{11/2}$.

(*b*) *If* $\gcd(m,n) = 1$, $\tau(mn) = \tau(m)\tau(n)$.

(*c*) *For any prime number* p *and any* $n \geq 1$, $\tau(p)\tau(p^n) = \tau(p^n)\tau(p) = \tau(p^{n+1}) + p^{11}\tau(p^{n-1})$.

Definition 2.1. Let $f = \sum_{n\geq 1} a_n q^n$ be a Dirichlet series, the associated L-series is defined as

$$L(f,s) = \sum_{n\geq 1} \frac{a_n}{n^s} , \qquad s \in \mathbb{C} , \mathrm{Re}(s) \gg 0 .$$

Example 2.1. $L(\Delta , s) = \sum_{n\geq 1} \frac{\tau(n)}{n^s}$.

Proposition 2.1.1. *The conditions* (b) $\tau(mn)=\tau(m)\tau(n)$ *if* $\gcd(m,n)=1$ *and* (c) $\tau(p)\tau(p^n)=\tau(p^{n+1})+p^{11}\tau(p^{n-1})$ *are equivalent to the following*

$$L(\Delta\,,s)=\prod_{p\,prime}\frac{1}{1-\tau(p)p^{-s}+p^{11-2s}}.$$

This is the **Eulerian product** *for* $L(\Delta,s)$.

Proof. If we write $L_p(s)=\sum_{m\geq 0}\frac{\tau(p^m)}{p^{ms}}$, then the condition (b) implies $\prod_p L_p(s)=L(\Delta,s)=\sum_{n\geq 1}\frac{\tau(n)}{n^s}$. We need to prove that

$$L_p(s)=\frac{1}{1-\tau(p)p^{-s}+p^{11-2s}}.$$

We compute

$$\begin{aligned}&(1-\tau(p)p^{-s}+p^{11-2s})\sum_{m\geq 0}\tau(p^m)p^{-ms}\\ =&1-p^{-s}(\tau(p)-\tau(p))+\sum_{m\geq 1}\big(\tau(p^{m+1})-\tau(p)\tau(p^m)-p^{11}\tau(p^{m-1})\big)p^{-(m+1)s}\ .\end{aligned}$$

Using (c), we then get $L_p(s)=\frac{1}{1-\tau(p)p^{-s}+p^{11-2s}}$. This proves the $\Rightarrow$) part. The $\Leftarrow$) part can be proved using the same computation. □

Lemma 2.1.2. *Let's write* $1-\tau(p)X+p^{11}X^2=(1-aX)(1-a'X)$. *The Ramanujan Conjecture* (a) $|\tau(p)|\leq 2p^{11/2}$ *is equivalent to each of the following:* (a') $|a|=|a'|=p^{11/2}$ *and* (a'') $a'=\overline{a}$.

Proof. The condition (a) is equivalent to $\Delta=\tau(p)^2-4p^{11}\leq 0$, which implies (a''). The condition (a'') implies (a') since $aa'=p^{11}\Rightarrow |a|=|a'|=p^{11/2}$. As $\tau(p)=a+a'\Rightarrow|\tau(p)|\leq 2p^{11/2}$, $(a')\Rightarrow(a)$. □

(a) is proved by Deligne's proof of the Weil conjecture.

Our next goal is to construct for all $k\in\mathbb{N}$ some operators

$$T_k(n)=T(n)=T_n:\mathcal{M}_{2k}(\Gamma)\longrightarrow\mathcal{M}_{2k}(\Gamma)$$

with the following properties

(1) $T(m)\circ T(n)=T(mn)$, if $\gcd(m,n)=1$.

(2) $T(p)\circ T(p^n)=T(p^n)\circ T(p)=T(p^{n+1})+p^{2k-1}T(p^{n-1})$.

(3) $T(n)$ leaves $\mathcal{S}_{2k}(\Gamma)$ invariant and is a self-adjoint operator for the Petersson scalar product:

$$\forall f\,,g\in\mathcal{S}_{2k}(\Gamma)\,,\quad\langle T_nf\,,g\rangle_k=\langle f\,,T_ng\rangle_k\ .$$

(4) $\forall m,n\in\mathbb{N}$, $T(m)\circ T(n)=T(n)\circ T(m)$.

Exercise 2.1. Let V be a $\mathbb{C}$-vector space of finite dimension endowed with a hermitian scalar product $\langle\ ,\ \rangle$. Let $(\alpha_i)_{i\in I}$ be a family of self adjoint endomorphisms of V such that $\alpha_i \circ \alpha_j = \alpha_j \circ \alpha_i$; $\forall i\,, j \in I$. Then V admits a basis of eigenforms of all the $(\alpha_i)_{i\in I}$.

Application: As $\dim(\mathcal{S}_{12}(\Gamma)) = 1$, Δ is an eigenform of all the $T(n)$. If we normalize Δ such that $\Delta = q + \sum_{n\geq 2}\tau(n)q^n$, then $T(n)\Delta = \lambda_n\Delta$. We'll show that $\lambda_n = \tau(n)$ and the relations (b) and (c) conjectured by Ramanujan are consequences of the properties (1) and (2) of the operators $T(n)$.

2.2 Abstract Theory of Hecke Operators

We start by a definition of Hecke operators on the space $\mathscr{R}$ of lattices of $\mathbb{C}$. We'll have an induced action on lattice functions and therefore an action on modular forms.

Let $\mathbb{Z}[\mathscr{R}]$ be the free abelian group with basis the elements of $\mathscr{R}$:

$$\mathscr{D} := \mathbb{Z}[\mathscr{R}] = \Big\{ \sum_{\Lambda\in\mathscr{R}} n_\Lambda[\Lambda]\,|\, n_\Lambda \in \mathbb{Z}\,,\ n_\Lambda = 0 \text{ for almost all } \Lambda \in \mathscr{R} \Big\}.$$

and $\mathscr{D}\otimes\mathbb{C} = \mathbb{C}[\mathscr{R}]$. (Caution: $2\cdot[\Lambda] \neq [2\cdot\Lambda]$.)

Definition 2.2. For all $n \in \mathbb{N}$, we define a $\mathbb{Z}$-linear operator

$$T(n) : \mathscr{D} \longrightarrow \mathscr{D}\,; \quad T(n)([\Lambda]) = \sum_{[\Lambda:\Lambda']=n} [\Lambda']$$

where the sum is on all sublattices $\Lambda' \subset \Lambda$ such that $[\Lambda : \Lambda'] = n$ and extend it by $\mathbb{Z}$-linearity. For all $\lambda \in \mathbb{C}^*$, we define the $\mathbb{Z}$-linear map

$$\mathcal{R}(\lambda) : \mathscr{D} \longrightarrow \mathscr{D}\ ; \quad [\Lambda] \longmapsto [\lambda\Lambda]\ .$$

Remark 2.1. $T(n)$ is well defined: there are only finitely many lattices $\Lambda' \subset \Lambda$ with $[\Lambda : \Lambda'] = n$.

Proof. If $\Lambda' \subset \Lambda$ and $[\Lambda : \Lambda'] = n$ then $n\Lambda \subset \Lambda'$, therefore $n\Lambda\backslash\Lambda' \subset n\Lambda\backslash\Lambda \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. □

Lemma 2.2.1. *The sublattices $\Lambda' \subset \Lambda$ such that $[\Lambda : \Lambda'] = n$ are in one-one correspondence with the subgroups of index (or order) n in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.*

Proof. Let Ψ be a subgroup of index n of $n\Lambda\backslash\Lambda$ and $\pi : \Lambda \longrightarrow n\Lambda\backslash\Lambda$ be the canonical surjection, then $\pi^{-1}(\Psi) = \Lambda_\Psi$ is a sublattice of Λ such that $[\Lambda : \Lambda_\Psi] = n$. Then the maps $\Lambda' \longmapsto \pi(\Lambda)$ and $\Psi \longmapsto \Lambda_\Psi$ are mutually inverse and hence give the one-one correspondence. □

Lemma 2.2.2. *Let $\Gamma = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ and let S_n be the set of integer matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $\begin{cases} ad = n \\ 0 \leq b < n,\ a \geq 1 \end{cases}$. If $\sigma \in S_n$, we write Γ_σ the sublattice of Γ with basis $\begin{cases} \omega_1' = a\omega_1 + b\omega_2 \\ \omega_2' = d\omega_2 \end{cases}$, then $\sigma \longmapsto \Gamma_\sigma$ is a bijection between S_n and the set $\Gamma(n)$ of sublattices of Γ of index n.*

Proof. (a) $\forall \sigma \in S_n$, $\Gamma_\sigma \in \Gamma(n)$ as $\det_{(\omega_1,\omega_2)}(\omega_1', \omega_2') = n = [\Gamma : \Gamma_\sigma]$.

(b) Let $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_n$, $\sigma' = \left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right) \in S_n$. Suppose that $\Gamma_\sigma = \Gamma_{\sigma'}$. Then there exists $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

This gives $\gamma a = 0$. It then follows easily that $\gamma = 0$ and $\alpha = \delta = 1$ and $0 \leq b' = b + \beta d < d$. So we have $\beta = 0$ and $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$.

(c) Let Γ' be in $\Gamma(n)$. Let d be the smallest positive integer such that $d\omega_2 \in \Gamma'$, then $\omega_2' = d\omega_2$ is a primitive vector of Γ'. Therefore there exists $\omega_1'' = a\omega_1 + b\omega_2 \in \Lambda'$ such that (ω_1'', ω_2') is a basis of Λ'.

Then $ad = n$ and we may replace ω_1'' by $\omega_1' = \omega_1'' - \lambda\omega_2'$. in such a way that $\omega_1' = a\omega_1 + b\omega_2$ with $0 \leq b < d$. Therefore $\Gamma' = \Gamma_\sigma$ for $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_n$. □

Matrix Interpretation. Let M_n be the set of matrices in $M_2(\mathbb{Z})$ with determinant n.

Proposition 2.2.3.

$$(1)\ M_n = \bigsqcup_{\substack{ad=n \\ 0\leq b<d,\, a\geq 1}} \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \ ;\ (2)\ M_n = \bigsqcup_{\substack{ad=n \\ a|d,\, a\geq 1}} \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mathrm{SL}_2(\mathbb{Z}).$$

We leave the proof as an exercise. Note that (2) is equivalent to the following condition, which can be proved using the elementary divisor theorem:

$\forall \alpha \in M_n$, there exists a basis (θ_1, θ_2) of Λ and $ad = n$, $a|d$, $a \geq 1$ such that $(a\theta_1, d\theta_2)$ is a basis of $\Lambda' = \alpha \cdot \Lambda$.

Proposition 2.2.4. (*a*) *Let m, n be coprime integers, then $T(mn) = T(m) \circ T(n)$.*

(*b*) $T(p^n) \circ T(p) = T(p^{n+1}) + p\mathcal{R}(p)T(p^{n-1})$.

(*c*) $T(n)\mathcal{R}(\lambda) = \mathcal{R}(\lambda)T(n)$.

Proof. (a) By definition,

$$T(mn)[\Lambda] = \sum_{[\Lambda:\Lambda'']=nm} [\Lambda''] \; ; \quad \text{and} \;\; T(m) \circ T(n)[\Lambda] = \sum_{\substack{\Lambda'' \subset \Lambda' \subset \Lambda \\ [\Lambda:\Lambda']=n \, , \, [\Lambda':\Lambda'']=m}} [\Lambda''].$$

If $\Lambda'' \subset \Lambda$ is a sublattice of Λ of index mn, we must show that there exists a unique $\Lambda' \subset \Lambda$ such that $\begin{cases} \Lambda'' \subset \Lambda' \subset \Lambda \\ [\Lambda : \Lambda'] = n \, , \, [\Lambda' : \Lambda''] = m \end{cases}$. By lemma.2.2.1, Λ'' corresponds to a subgroup L of order nm in

$$\begin{aligned} \mathbb{Z}/nm\mathbb{Z} \oplus \mathbb{Z}/nm\mathbb{Z} &\simeq (\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}) \\ L &\simeq L_1 \oplus L_2 \end{aligned}$$

with $|L_1| = n$ and $|L_2| = m$. Then Λ' is the sublattice of Λ corresponding to the subgroup L_1 of $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \simeq n\Lambda\backslash\Lambda$.

(b) We have

$$T(p^n) \circ T(p) \cdot [\Lambda] = \sum [\Lambda''] \tag{2.1}$$

where the sum is on couples (Λ', Λ'') with $\Lambda'' \subset \Lambda' \subset \Lambda$ and $\begin{cases} [\Lambda : \Lambda'] = p \\ [\Lambda' : \Lambda''] = p^n \end{cases}$.

On the other hand,

$$T(p^{n+1}) \cdot [\Lambda] = \sum_{\substack{\Lambda'' \subset \Lambda \\ [\Lambda:\Lambda'']=p^{n+1}}} [\Lambda''] \tag{2.2}$$

and

$$\mathcal{R}(p)T(p^{n-1})[\Lambda] = \sum_{[\Lambda:\Lambda']=p^{n-1}} [p \cdot \Lambda'] \tag{2.3}$$

In (2.3), we have $[\Lambda : p\Lambda'] = [\Lambda : \Lambda'][\Lambda' : p\Lambda'] = p^{n-1} \cdot p^2 = p^{n+1}$.

The sums (2.1), (2.2) and (2.3) concern sublattices of Λ with index p^{n+1} in Λ. Let $\Lambda'' \subset \Lambda$ be such a lattice. We write

$$\begin{aligned} a(\Lambda'') = a &:= \text{number of times } \Lambda'' \text{ appears in the sum (2.1)} \\ b(\Lambda'') = b &:= \text{number of times } \Lambda'' \text{ appears in the sum (2.3)} \end{aligned} \tag{2.4}$$

Then we need to check $a = 1 + bp$.

Case 1: suppose $\Lambda'' \not\subset p\Lambda$. In this case $b(\Lambda'') = b = 0$ because if Λ'' appears in (2.3), then $[\Lambda''] = [p\Lambda']$ for some $\Lambda' \subset \Lambda$ and $\Lambda'' = p\Lambda' \subset p\Lambda$.

In (2.1), we have $p\Lambda \subset \Lambda'$ and $p\Lambda\backslash\Lambda'$ is a subgroup of order p in $p\Lambda\backslash\Lambda \simeq \mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}$. But $p\Lambda\backslash\Lambda'$ contains $p\Lambda\cap\Lambda''\backslash\Lambda''$ and $p\Lambda\cap\Lambda'' \neq \Lambda''$ (as $\Lambda'' \nsubseteq p\Lambda$). Therefore $p\Lambda\cap\Lambda''\backslash\Lambda'' = p\Lambda\backslash\Lambda'$ and Λ' corresponds to the subgroup (of order p) $p\Lambda\cap\Lambda''\backslash\Lambda''$ of $p\Lambda\backslash\Lambda$ which is determined by Λ''. So we have $a(\Lambda'') = 1$.

Case 2: suppose $\Lambda'' \subset p\Lambda$. Let $\Lambda' \subset \Lambda$ such that $[\Lambda : \Lambda'] = p$, then $\Lambda'' \subset p\Lambda \subset \Lambda' \subset \Lambda$, and $a(\Lambda'') = a$ is the number of possible such Λ'. Therefore a is the number of subgroups of index (or order) p in $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Thus,

$$\begin{aligned} a =& \text{number of sub } \mathbb{F}_p\text{-vector space of dimension 1 in } \mathbb{F}_p \oplus \mathbb{F}_p \\ =& \text{Card}\left(\frac{\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} - \{0\}}{(\mathbb{Z}/p\mathbb{Z})^\times}\right) = \frac{p^2-1}{p-1} = p+1. \end{aligned}$$

If $\Lambda'' \subset p\Lambda \subset \Lambda$, then $[p\Lambda : \Lambda''] = p^{n-1}$, $[\Lambda'']$ appears once in $T(p^{n-1})[p\Lambda]$. Therefore $b(\Lambda'') = 1$. □

Exercise 2.2. More generally, prove that

$$\begin{aligned} T(p^r) \circ T(p^s) &= \sum_{0\le i\le \min(r,s)} p^i \mathcal{R}(p^i) T(p^{r+s-2i}) \ ; \\ T(m) \circ T(n) = T(n) \circ T(m) &= \sum_{d\mid \gcd(m,n)\,,\, d>0} d\mathcal{R}(d) T(\frac{mn}{d^2}) \ . \end{aligned} \tag{2.5}$$

Corollary 2.2.5. *For all $n \in \mathbb{N}$, the $T(n)$'s are some polynomials in the $T(p)$'s and the $\mathcal{R}(p)$'s. The algebra generated by the $T(p)$'s and the $\mathcal{R}(p)$'s with p prime is commutative and contains all the $T(n)$'s.*

2.3 Hecke Operators on Spaces of Modular Forms

Let F be a lattice function $F : \mathscr{R} \longrightarrow \mathbb{C}$. By linearity we may extend F to $\mathscr{D}$, $F(\sum_{\Lambda\in\mathscr{R}} n_\Lambda[\Lambda]) = \sum_{\Lambda\in\mathscr{R}} n_\Lambda F([\Lambda])$. We may define

$$T_n \cdot F([\Lambda]) = \sum_{\Lambda'\in T_n[\Lambda]} F([\Lambda']) = \sum_{\substack{[\Lambda:\Lambda']=n \\ \Lambda'\subset\Lambda}} F([\Lambda']) \tag{2.6}$$

and

$$\mathcal{R}(n)F([\lambda]) = F([\lambda\Lambda]) \ . \tag{2.7}$$

If F is a weight-$2k$ lattice function,

$$\mathcal{R}(n)F([\Lambda]) = F([n\Lambda]) = n^{-2k}F([\Lambda]). \tag{2.8}$$

Proposition 2.3.1. *If F is a weight-$2k$ lattice function, then $T(n)\cdot F$ is also a weight-$2k$ lattice function, and*

$$T(m)\circ T(n)\cdot F = \sum_{d|\gcd(m,n)} d^{1-2k}T(\frac{mn}{d^2})F \ .$$

Proof. $T_n \cdot F$ is of weight $2k$ as $\mathcal{R}(\lambda)$ and $T(n)$ commute. □

Recall that we have an isomorphism

$$\begin{aligned}\{ \text{ weight } 2k \text{ lattice functions}\} \xrightarrow{\sim} &\{\text{functions on } \mathbb{H} \text{ verifying the modular identity} \\ &\text{of weight } 2k \text{ modular forms}\} \\ F \longmapsto &f(z) = F(\mathbb{Z}\oplus z\mathbb{Z}).\end{aligned}$$

Definition 2.3. Let $f(z)$ be a weight $2k$ modular form for $\mathrm{SL}_2(\mathbb{Z})$ and F the associated lattice function. Then $T_n \circ f(z)$ is the function associated to the lattice function $n^{2k-1}T_n \cdot F$.

Explicitly,

$$\begin{aligned} T_n f(z) = n^{2k-1}T_n F\big([\mathbb{Z}\oplus z\mathbb{Z}]\big) &= n^{2k-1}\sum_{\substack{ad=n\,,\,d\geq 1\\ 0\leq b<d}} F\big([(az+b)\mathbb{Z}\oplus d\mathbb{Z}]\big) \\ &= n^{2k-1}\sum_{\substack{ad=n\,,\,d\geq 1\\ 0\leq b<d}} d^{-2k}f(\frac{az+b}{d}) \end{aligned} \ . \tag{2.9}$$

Example 2.2.

$$T_p\cdot f(z) = p^{2k-1}\Big(f(pz) + p^{-2k}\sum_{i=0}^{p-1} f(\frac{z+i}{p})\Big) \ .$$

Proposition 2.3.2. *Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and let $f(z)\in\mathcal{M}_{2k}(\Gamma)$, $f = \sum_{m\geq 0} c(m)q^m$. Then $T_n f(z) = \sum_{m\geq 0}\gamma(m)q^m$ is a weight-$2k$ modular form and*

$$\gamma(m) = \sum_{a|\gcd(m,n)} a^{2k-1}c\big(\frac{mn}{a^2}\big).$$

In particular, $\gamma(1) = c(n)$, $\gamma(0) = \sigma_{2k-1}(n)c(0) = \sum_{d|n} d^{2k-1}c(0)$. If $f\in\mathcal{S}_{2k}(\Gamma)$, then $T_n f\in\mathcal{S}_{2k}(\Gamma)$.

Proof. We have

$$\begin{aligned} T_n f(z) &= n^{2k-1} \sum_{\substack{ad=n\,,\,d\geq 1\\ 0\leq b<d}} d^{-2k} f(\frac{az+b}{d}) \\ &= n^{2k-1} \sum_{\substack{ad=n\,,\,d\geq 1\\ 0\leq b<d}} d^{-2k} \sum_{m\geq 0} c(m) e^{2\mathrm{i}\pi m(\frac{az+b}{d})} \\ &= n^{2k-1} \sum_{m\geq 0} \sum_{ad=n} d^{-2k} c(m) \sum_{0\leq b<d} e^{2\mathrm{i}\pi m(\frac{az+b}{d})}. \end{aligned}$$

Note that

$$\sum_{0\leq b<d} e^{\frac{2i\pi bm}{d}} = \begin{cases} d & \text{if } d|m \\ 0 & \text{if } d\nmid m \end{cases}.$$

Therefore, writing $m' = \frac{m}{d}$, we get

$$T_n f(z) = n^{2k-1} \sum_{m'\geq 0} \sum_{ad=n} d^{-2k+1} c(m'd) e^{2\mathrm{i}\pi am'z}.$$

The coefficient $\gamma(t)$ of q^t is obtained for the couples (a, m') such that $\begin{cases} am' = t \\ ad = n \end{cases}$,

or equivalently $\begin{cases} a = \frac{n}{d} \\ m'd = \frac{tn}{a^2} \end{cases}$. So we get

$$\gamma(t) = \sum_{a|\gcd(n,t)} a^{2k-1} c(\frac{tn}{a^2}).$$

□

Proposition 2.3.3. *Let $f = \sum_{m\geq 0} c(m)q^m \neq 0$, $f \in \mathcal{M}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$. We suppose that f is an eigenform of all the T_n's. Let's write $T(n)f = \lambda(n)f$. Then*

(i) *$c(1) \neq 0$, so we may suppose that $c(1) = 1$. We then say that f is* **normalized**.

(ii) *If f is normalized, then $\forall n \in \mathbb{N}$, $\lambda(n) = c(n)$.*

Proof. The coefficient of q in $T_n f$ is $c(n)$ but is also $\lambda(n)c(1)$. Therefore $c(n) = \lambda(n)c(1)$.

If $c(1) = 0$, then $c(n) = 0$ for all n and $f = 0$.

If $c(1) = 1$, then $c(n) = \lambda(n)$ for all $n \in \mathbb{N}$. □

Corollary 2.3.4. *Let $f \in \mathcal{S}_{2k}(\Gamma)$ be a normalized eigenform of all the $T(n)$'s. Then*

$$\begin{cases} (1)\ \forall m,n \text{ such that } \gcd(m,n)=1,\ c(m)c(n)=c(mn), \\ (2)\ \forall \text{ prime } p,\ \forall n\in\mathbb{N},\ c(p)c(p^n)=c(p^{n+1})+p^{2k-1}c(p^{n-1}) \end{cases}$$

and these two conditions are equivalent to

$$L(f,s)=\sum_{n\geq 1}\frac{c(n)}{n^s}=\prod_p \frac{1}{1-c(p)p^{-s}+p^{2k-1-2s}}.$$

Proof. (1) and (2) are deduced from relations for T_n using that $c(n)=\lambda(n)$. We made the proof of the last equivalence in the case $2k=12$. The proof is exactly the same here. □

2.4 Hecke Operators and Petersson Scalar Product

Let $\mathrm{GL}_2(\mathbb{R})^+ = \{\alpha \in \mathrm{GL}_2(\mathbb{R})\,;\, \det(\alpha) > 0\}$, and $\mathrm{GL}_2(\mathbb{Q})^+ = \mathrm{GL}_2(\mathbb{Q}) \cap \mathrm{GL}_2(\mathbb{R})^+$.

Let f be a function on $\mathbb{H}$ and $\alpha \in \mathrm{GL}_2(\mathbb{R})^+$, we define the function

$$(f|_k\alpha)(z) = (\det\alpha)^k(cz+d)^{-2k} f\big(\frac{az+b}{cz+d}\big), \qquad \alpha=\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^+.$$

Remark 2.2. (a) If $\alpha=\begin{pmatrix} a & 0 \\ 0 & a\end{pmatrix}$, $f|_k\alpha = f$. (b) If $f\in\mathcal{M}_{2k}(\Gamma)$, and if $\gamma\in\Gamma$, then $f|_k\gamma = f$. (c) $f|_k\alpha\beta = (f|_k\alpha)|_k\beta$, $\forall\alpha,\beta\in\mathrm{GL}_2(\mathbb{R})^+$. (d) If $\Gamma=\mathrm{SL}_2(\mathbb{Z})$ and $f\in\mathcal{M}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$,

$$\begin{aligned} T_n f(z) &= n^{2k-1}\sum_{\substack{ad=n \\ 0\leq b<d}} d^{-2k} f\big(\frac{az+b}{d}\big) \\ &= n^{k-1}\sum_{\alpha\in \mathrm{SL}_2\,\mathbb{Z}\backslash M(n)} f|_k\alpha = n^{k-1}\sum_{i=1}^{r} f|_k\alpha_i\ . \end{aligned}$$

where

$$M(n)=\{M\in M_2(\mathbb{Z})\,;\ \det(M)=n\} = \bigsqcup_{i=1}^{r}\mathrm{SL}_2(\mathbb{Z})\alpha_i.$$

Theorem 2.4.1. $\forall f\,,\, g \in \mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$, $\langle T_n f\,,\, g\rangle_k = \langle f\,,\, T_n g\rangle_k$, *i.e,* T_n *is a self-adjoint operator on* $\mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$.

Lemma 2.4.2. $\forall \alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, $\forall f\,,\, g \in \mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$, $\langle f|_k\alpha, g|_k\alpha\rangle_k = \langle f, g\rangle_k$.

Proof. We write $\Omega(f,g) = f(z)\overline{g(z)}y^{2k-2}dx \wedge dy$. Then $\Omega(f|_k\alpha, g|_k\alpha) = \alpha^*\Omega(f,g)$. If $\mathcal{D}$ is a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$,

$$\int_{\mathcal{D}} \Omega(f|_k\alpha, g|_k\alpha) = \int_{\mathcal{D}} \alpha^*\Omega(f,g) = \int_{\alpha\mathcal{D}} \Omega(f,g) = \int_{\mathcal{D}} \Omega(f,g)\ .$$

We should remark that in the above computation the last "=" is not obvious as α is not necessary an element in $\mathrm{SL}_2(\mathbb{Z})$. We will finish the proof later. □

Remark 2.3. For all f, $g \in \mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$, $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ and any fundamental domain $\mathcal{D}_\Gamma$ for Γ,

$$\langle f, g\rangle_k = \frac{1}{[\,\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}\,]} \int\int_{\mathcal{D}_\Gamma} \Omega(f,g)$$

where $\overline{\Gamma}$ is the image of Γ in $\mathrm{PSL}_2(\mathbb{Z})$.

Remark 2.4. If $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ and if Γ and $\alpha\Gamma\alpha^{-1}$ are sublattices of $\mathrm{SL}_2(\mathbb{Z})$, then $[\,\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}\,] = [\,\mathrm{PSL}_2(\mathbb{Z}) : \overline{\alpha\Gamma\alpha^{-1}}\,]$.

Proof. Use the metric $d\mu_0 = \frac{dxdy}{y^2}$. The map $\psi_\alpha : \mathbb{H} \longrightarrow \mathbb{H}\ ; z \longmapsto \alpha \cdot z$ induces an isomorphism $\Gamma\backslash\mathbb{H} \simeq \alpha\Gamma\alpha^{-1}\backslash\mathbb{H}$. As ψ_α is an isometry, we get

$$\begin{aligned}&[\,\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}\,]\mathrm{Vol}(\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}) = \mathrm{Vol}(\Gamma\backslash\mathbb{H})\\ &= \mathrm{Vol}(\alpha\Gamma\alpha^{-1}\backslash\mathbb{H}) = [\,\mathrm{PSL}_2(\mathbb{Z}) : \overline{\alpha\Gamma\alpha^{-1}}\,]\mathrm{Vol}(\Gamma\backslash\mathbb{H})\end{aligned}\ .$$

This gives $[\,\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}\,] = [\,\mathrm{PSL}_2(\mathbb{Z}) : \overline{\alpha\Gamma\alpha^{-1}}\,]$. □

Remark 2.5. Let $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, there exists $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ (small enough) such that $\alpha\Gamma\alpha^{-1} \subset \mathrm{SL}_2(\mathbb{Z})$.

Proof. Changing α by $\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right)\alpha$ we may assume that $\alpha \in M_2(\mathbb{Z})$. If $\det(\alpha) = n$ (i.e, $\alpha \in M(n)$), we may assume that $\alpha = \left(\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\right)$ with $ad = n\,,\, 0 \le b < d$. Then we can check that $\alpha\Gamma(n)\alpha^{-1} \subset \mathrm{SL}_2(\mathbb{Z})$. □

Remark 2.6. If $\mathscr{F}$ is a fundamental domain for Γ, then $\alpha\cdot\mathscr{F}$ is a fundamental domain for $\alpha\Gamma\alpha^{-1}$.

Proof of lemma 2.4.2. By remark.2.4,

$$\langle f|_k\alpha\,,\, g|_k\alpha\rangle = \frac{1}{[\,\mathrm{PSL}_2(\mathbb{Z}):\overline{\Gamma}\,]}\int_{\alpha\mathcal{D}_\Gamma}\Omega(f,g)$$
$$=\frac{1}{[\mathrm{PSL}_2(\mathbb{Z}):\overline{\alpha\Gamma\alpha^{-1}}\,]}\int_{\alpha\mathcal{D}_\Gamma}\Omega(f,g)=\langle f,g\rangle_k\ .$$

as $\alpha\mathcal{D}_\Gamma$ is a fundamental domain for $\alpha\Gamma\alpha^{-1}$. □

Corollary 2.4.3. $\forall\alpha\in\mathrm{GL}_2(\mathbb{Q})^+$, $\forall f\,,\,g\in\mathcal{S}_{2k}\big(\mathrm{SL}_2(\mathbb{Z})\big)$, $\langle f|_k\alpha, g\rangle=\langle f, g|_k\alpha^{-1}\rangle$.

Proof. Note that $(f|_k\alpha)|_k\alpha^{-1}=f|_k\alpha\alpha^{-1}=f$ and apply lemma.2.4.2. □

As the $T(n)$'s are polynomials in the $T(p)$'s, we just need to prove theorem.2.4.1 for $n=p$ a prime number.

Lemma 2.4.4. *There exists a system of representatives* $\{\alpha_i\}$ *for* $\mathrm{SL}_2(\mathbb{Z})\backslash M(p)$ *which is also a system of representatives for* $M(p)/\mathrm{SL}_2(\mathbb{Z})$. *More generally for all* $\alpha\in\mathrm{GL}_2(\mathbb{Q})^+$, $\exists\ \alpha_1,\ \cdots,\ \alpha_r$ *such that*

$$\mathrm{SL}_2(\mathbb{Z})\alpha\,\mathrm{SL}_2(\mathbb{Z})=\bigsqcup_{i=1}^{r}\mathrm{SL}_2(\mathbb{Z})\alpha_i=\bigsqcup_{i=1}^{r}\alpha_i\,\mathrm{SL}_2(\mathbb{Z})\ .$$

Remark 2.7. $M(p)=\mathrm{SL}_2(\mathbb{Z})\begin{pmatrix}p&0\\0&1\end{pmatrix}\mathrm{SL}_2(\mathbb{Z})$.

Proof of lemma.2.4.4. Let α,β such that $\mathrm{SL}_2(\mathbb{Z})\alpha\,\mathrm{SL}_2(\mathbb{Z})=\mathrm{SL}_2(\mathbb{Z})\beta\,\mathrm{SL}_2(\mathbb{Z})$. Then there exists γ such that

$$\begin{cases}\mathrm{SL}_2(\mathbb{Z})\alpha=\mathrm{SL}_2(\mathbb{Z})\gamma\\ \beta\,\mathrm{SL}_2(\mathbb{Z})=\gamma\,\mathrm{SL}_2(\mathbb{Z})\end{cases}\ . \qquad (*)$$

By hypothesis, $\exists\ u,\ v,\ u',\ v'\in\mathrm{SL}_2(\mathbb{Z})$ such that $u\alpha v=u'\beta v'$. Let $\gamma:=u'^{-1}u\alpha=\beta v'v^{-1}$. Then it is easy to check γ satisfies the property $(*)$. If $\mathrm{SL}_2(\mathbb{Z})\alpha\,\mathrm{SL}_2(\mathbb{Z})=\bigsqcup_{i=1}^{s}\mathrm{SL}_2(\mathbb{Z})\alpha_i=\bigsqcup_{i=1}^{s}\beta_i\,\mathrm{SL}_2(\mathbb{Z})$, (note that we need to explain why the number of left cosets is equal to the number of right cosets later,) we may apply the last construction to all the couples (α_i,β_i) to produce a γ_i with the property $\begin{cases}\mathrm{SL}_2(\mathbb{Z})\gamma_i=\mathrm{SL}_2(\mathbb{Z})\alpha_i\\ \gamma_i\,\mathrm{SL}_2(\mathbb{Z})=\beta_i\,\mathrm{SL}_2(\mathbb{Z})\end{cases}$. □

Lemma 2.4.5. *Let* $\Gamma\subset\mathrm{SL}_2(\mathbb{Z})$, $\alpha\in\mathrm{GL}_2(\mathbb{Q})^+$. *If* $\Gamma\alpha\Gamma=\bigsqcup_{i=1}^{l}\Gamma\alpha_i=\bigsqcup_{j=1}^{m}\beta_j\Gamma$, *then* $l=m$.

Proof. A general proof will be given later. If $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and $\alpha = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$, then ${}^t(\Gamma\alpha\Gamma) = {}^t\,\Gamma\,{}^t\alpha\,{}^t\Gamma = \Gamma\alpha\Gamma$, where the superscript t denotes the transpose of matrices.

If $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^r \Gamma\alpha_i$, then $\Gamma\alpha\Gamma = {}^t\,(\Gamma\alpha\Gamma) = \bigsqcup_{i=1}^r {}^t\alpha_i\,{}^t\Gamma = \bigsqcup_{i=1}^r {}^t\alpha_i\Gamma$. □

Proof of theorem 2.4.1. Let $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(p)$, then $\alpha' = p\alpha^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M(p)$. Let $\alpha_1, \cdots, \alpha_r \in M(p)$ such that $M(p) = \bigsqcup_{i=1}^r \mathrm{SL}_2(\mathbb{Z})\alpha_i = \bigsqcup_{i=1}^r \alpha_i\,\mathrm{SL}_2(\mathbb{Z})$. Then

$$M(p) = pM(p)^{-1} = \bigsqcup_{i=1}^r p\alpha_i^{-1}\,\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i=1}^r \mathrm{SL}_2(\mathbb{Z})p\alpha_i^{-1}.$$

and

$$\begin{aligned}
\langle T(p)f, g\rangle &= p^{k-1}\sum_{i=1}^r \langle f|_k\alpha_i, g\rangle = p^{k-1}\sum_{i=1}^r \langle f, g|_k\alpha_i^{-1}\rangle \\
&= p^{k-1}\sum_{i=1}^r \langle f, g|_k\alpha_i^{-1}\rangle = p^{k-1}\sum_{i=1}^r \langle f, \left(g|_k \left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right)\right)_k \alpha_i^{-1}\rangle \\
&= \langle f, T(p)g\rangle.
\end{aligned}$$

□

Theorem 2.4.6. *There exists a basis $\{f_1, \cdots, f_r\}$ of $\mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ such that the f_i are eigenvectors of all the Hecke operators $T(n)$. The associated eigenvalues are real numbers and the $\{f_i\}$ are orthogonal for the Petersson scalar product. If we normalized the f_i by the condition $a_1(f_i) = 1$, then*

$$L(f_i, s) = \sum_{n\geq 1} \frac{a_n(f_i)}{n^s} = \prod_p \frac{1}{1 - a_p(f_i)p^{-s} + p^{2k-1-2s}}.$$

Proof. Let f_1 and f_2 be two eigenforms of all the $T(n)$'s. Then

$$\langle T(n)f_1, f_2\rangle = a_n(f_1)\langle f_1, f_2\rangle = \langle f_1, T(n)f_2\rangle = a_n(f_2)\langle f_1, f_2\rangle.$$

and therefore

$$(a_n(f_1) - a_n(f_2))\langle f_1, f_2\rangle = 0\,,\ \forall n \in \mathbb{N} \Longrightarrow \langle f_1, f_2\rangle = 0 \text{ if } f_1 \neq f_2.$$

□

Proposition 2.4.7. *Let* $f = \sum_{n\geq 1} a_n(f)q^n \in \mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ *and* $L(f,s) = \sum_{n\geq 1} \frac{a_n(f)}{n^s}$. *Then*

(a) $|a_n| \ll n^k$;

(b) $L(f,s)$ *is convergent for* $\mathrm{Re}(s) > k+1$.

Proof. We need only to prove(a). The function $g(z) = y^k|f(z)|$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant and $g(z) \to 0$ as $z \to \mathrm{i}\infty$ (as $|f(z)| \ll e^{-cy}, c > 0$). Therefore $g(z)$ is bounded in $\mathbb{H}$ and $|f(x+\mathrm{i}y)| << \frac{1}{y^k}$. For all $y > 0$,

$$\begin{aligned} |a_n|e^{-2\pi ny} &= \Big|\int_0^1 f(x+\mathrm{i}y)e^{-2\mathrm{i}\pi nz}e^{-2\pi ny}dz\Big| = \Big|\int_0^1 f(x+\mathrm{i}y)e^{-2\mathrm{i}\pi nx}dx\Big| \\ &\ll \frac{1}{y^k}, \end{aligned}$$

Take $y = \frac{1}{n}$, then we get $|a_n| \ll n^k$. □

Remark 2.8. The Ramanujan conjecture predicts that $|a_p| \leq 2p^{k-\frac{1}{2}}$. This is a nontrivial bound.

2.5 The Mellin Transform and Functional Equations

Let $f \in \mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$. The ***Mellin transform*** of f is defined as

$$M_f(s) := \int_0^\infty f(\mathrm{i}t)t^s\frac{dt}{t}.$$

As f is exponentially decreasing in 0 and in $\mathrm{i}\infty$, $M_f(s)$ is defined for all $s \in \mathbb{C}$ and is a holomorphic function of s.

Proposition 2.5.1.

$$M_f(s) = (2\pi)^{-s}L(f,s)\Gamma(s) \qquad \textit{where} \quad \Gamma(s) = \int_0^\infty e^{-t}t^s\frac{dt}{t}\ .$$

This gives an analytic definition for $L(f,s)$ *for all* $s \in \mathbb{C}$.

Proof. Using the Fourier expansion $f = \sum_{n\geq 1} a_n(f)q^n = \sum_{n\geq 1} a_n e^{2\mathrm{i}\pi nz}$, we have

$$\begin{aligned} M_f(s) &= \sum_{n\geq 1}\int_0^\infty a_n e^{-2\pi nt}t^s\frac{dt}{t} = \sum_{n\geq 1} a_n\int_0^\infty e^{-2\pi nt}t^s\frac{dt}{t} \\ &= (2\pi)^{-s}\sum_{n\geq 1}\frac{a_n}{n^s}\int_0^\infty e^{-t}t^s\frac{dt}{t} \qquad \big(\text{changing variables } t' = 2\pi nt\big)\ . \end{aligned}$$

□

Proposition 2.5.2. *We have the following functional equation*

$$M_f(s) = (-1)^k M_f(2k-s).$$

Proof. Make the change of variables $t' = \frac{1}{t}$ in the formula

$$M_f(s) = \int_0^\infty f(\mathrm{i}t) t^s \frac{dt}{t} .$$

Then we get

$$\begin{aligned} M_f(s) &= \int_0^\infty f(-\frac{1}{\mathrm{i}t}) t^{-s} \frac{dt}{t} = \int_0^\infty f\big(\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \cdot \mathrm{i}t \big) t^{-s} \frac{dt}{t} \\ &= \int_0^\infty (\mathrm{i}t)^{2k} f(\mathrm{i}t) t^{-s} \frac{dt}{t} \qquad \big(\text{by the modular equation for } f \in \mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))\ \big) \\ &= (-1)^k M_f(2k-s) \ . \end{aligned}$$

□

Theorem 2.5.3. *The eigenvalues of the Hecke operators acting on $\mathcal{M}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ are algebraic integers. In other words, if $T_n f = \lambda_n f$, then there exists a number field K such that $\lambda_n \in \mathcal{O}_K$.*

Lemma 2.5.4. *G_{2k} is an eigenform of all the Hecke operators $T(n)$ with eigenvalues $\sigma_{2k-1}(n) = \sum_{d|n} d^{2k-1}$. Therefore*

$$L\Big(\frac{G_{2k}(z)}{a_1(G_{2k})}, s\Big) = \sum_{n\geq 1} \frac{\sigma_{2k-1}(n)}{n^s} = \zeta(s)\zeta(s-2k+1), \quad \textit{where } \zeta(s) = \prod_p \frac{1}{1-p^{-s}} \ .$$

Proof. G_{2k} is associated to the lattice function

$$G_{2k}(\Lambda) = \sum_{\substack{\lambda\in\Lambda \\ \lambda\neq 0}} \frac{1}{\lambda^{2k}} \ .$$

So we have

$$T_p G_{2k} = \sum_{[\Lambda:\Lambda']=p} \sum_{\substack{\lambda\in\Lambda' \\ \lambda\neq 0}} \frac{1}{\lambda^{2k}} \ .$$

If $\lambda \in p\Lambda$, then $\lambda \in \Lambda'$ for all Λ' such that $[\Lambda : \Lambda'] = p$. If $\lambda \notin p\Lambda$, there exists a unique Λ' such that $[\Lambda : \Lambda'] = p$ and $\lambda \in \Lambda'$.

Therefore,

$$\begin{aligned} T_p G_{2k}(\Lambda) &= G_{2k}(\Lambda) + p \sum_{\substack{\lambda \in p\Lambda \\ \lambda \neq 0}} \frac{1}{\lambda^{2k}} \\ &= (1 + p^{1-2k}) G_{2k}(\Lambda). \end{aligned}$$

The associated function $G_{2k}(z)$ on $\mathbb{H}$ is therefore an eigenform of $T(p)$ with eigenvalue $p^{2k-1}(1 + p^{1-2k}) = 1 + p^{2k-1} = \sigma_{2k-1}(p)$. Hence, $T_n G_{2k}(z) = \sigma_{2k-1}(n) G_{2k}(z)$ and

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{\sigma_{2k-1}(n)}{n^s} &= \sum_{n=1}^{\infty} \frac{\sum_{d|n} d^{2k-1}}{n^s} = \sum_{\substack{a \geq 1 \\ d \geq 1}} \frac{d^{2k-1}}{a^s d^s} \\ &= \sum_{d \geq 1} \frac{1}{d^{s+1-2k}} \sum_{a \geq 1} \frac{1}{a^s} = \zeta(s + 1 - 2k)\zeta(s). \end{aligned}$$

Note that the result means the L-function of $\frac{G_{2k}(z)}{a_1(G_{2k}(z))}$ is a product of L-functions of degree 1. □

Remark 2.9. $\sigma_{2k-1}(p) \sim p^{2k-1} \gg 2p^{k-\frac{1}{2}}$.

Let

$$\mathcal{M}_{2k}(\mathbb{Z}) = \left\{ f \in \mathcal{M}_{2k}(\mathrm{SL}_2(\mathbb{Z})); \quad f = \sum_{n \geq 0} a_n q^n, \quad a_n \in \mathbb{Z}, \quad \forall n \in \mathbb{N} \right\}.$$

Theorem 2.5.5. *$\mathcal{M}_{2k}(\mathbb{Z})$ is a free $\mathbb{Z}$-module of rank $\dim_{\mathbb{C}}(\mathcal{M}_{2k}(\mathrm{SL}_2(\mathbb{Z})))$.*

Lemma 2.5.6.

$$G_{2k}(z) = 2\zeta(2k) + \frac{2(2\mathrm{i}\pi)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n. \tag{2.10}$$

Proof. We have proved that the first coefficient is $2\zeta(2k)$ and

$$L\Big(\frac{G_{2k}(\mathbb{Z})}{a_1(G_{2k}(\mathbb{Z}))}, s\Big) = \sum_{n=1}^{\infty} \frac{\sigma_{2k-1}(n)}{n^s}.$$

The only missing point is $a_1(G_{2k}(z)) = \frac{2(2i\pi)^{2k}}{(2k-1)!}$. This is left to the readers. □

Corollary 2.5.7.

$$E_4 = \frac{G_4(z)}{2\zeta(4)} \in \mathcal{M}_4(\mathbb{Z}), \quad E_6 = \frac{G_6(z)}{2\zeta(6)} \in \mathcal{M}_6(\mathbb{Z}) \ .$$

Proof. Use the facts that $\zeta(4) = \frac{\pi^4}{90}$, $\zeta(6) = \frac{\pi^6}{35\times 27}$ and the previous lemma. □

Proof of theorem 2.5.5. For all $k \geq 2$, $\mathcal{M}_{2k}(\mathbb{Z})$ contains the free $\mathbb{Z}$-module with basis $E_4^a E_6^b$ with $4a+6b = 2k$. Therefore $\mathcal{M}_{2k}(\mathbb{Z})$ is a $\mathbb{Z}$-module of rank at least $\dim_{\mathbb{C}}(\mathcal{M}_{2k}(\mathrm{SL}_2(\mathbb{Z})))$.

If $f \in \mathcal{M}_{2k}(\mathbb{Z})$ and $2k < 12$, then there exists $\lambda \in \mathbb{C}$ such that $f = \lambda E_4^a E_6^b = \lambda + a_1 q + \cdots$ This implies $\lambda \in \mathbb{Z}$ and hence $\mathrm{rank}_{\mathbb{Z}}(\mathcal{M}_{2k}(\mathbb{Z})) = \dim_{\mathbb{C}}(\mathcal{M}_{2k}(\mathrm{SL}_2(\mathbb{Z})))$.

Lemma 2.5.8. *We have* $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = q + \cdots$.

We omit the classical proof of the above lemma.

Thus we have $\Delta \in \mathcal{S}_{12}(\mathbb{Z}) \subset \mathcal{M}_{12}(\mathbb{Z})$.

Let $f \in \mathcal{M}_{2k}(\mathbb{Z})$ with $2k \geq 12$, then $f = a_0 E_4^a E_6^b + \Delta g$ for some $4a+6b = 2k$ and $g \in \mathcal{M}_{2k-12}(\mathrm{SL}_2(\mathbb{Z}))$. Suppose $f = a_0 + qa_1 + \cdots$, then $a_0 \in \mathbb{Z}$.

Let's write $\Delta = \sum_{n\geq 1}\tau(n)q^n$; $\tau(n) \in \mathbb{Z}$ and $g = \sum_{n\geq 0} c(n)q^n$; $c(n) \in \mathbb{C}$. Then

$$\Delta g = \sum_{n\geq 1}\sum_{r=0}^{n-1} c(r)\tau(n-r)q^n \ .$$

Thus,

$$\begin{cases} \tau(1)c(0) = c(0) \in \mathbb{Z} \\ c(n-1) + \sum_{r=0}^{n-2} c(r)\tau(n-r) \in \mathbb{Z}, \quad \text{if } n \geq 2 \end{cases}$$

By induction $c(n) \in \mathbb{Z}$ for all $n \in \mathbb{N}$. Therefore $g \in \mathcal{M}_{2k-12}(\mathbb{Z})$. By induction one can prove $\mathrm{rank}_{\mathbb{Z}}\mathcal{M}_{2k}(\mathbb{Z}) = \dim_{\mathbb{C}}(\mathcal{M}_{2k}(\mathrm{SL}_2(\mathbb{Z})))$ for all k. □

Sketch of a more advanced proof. $\mathrm{SL}_2(\mathbb{Z}))\backslash\mathbb{H}$ has a model $\mathfrak{X}$ over $\mathrm{Spec}(\mathbb{Z})$ and $\mathcal{M}_{2k}(\mathbb{Z})$ can be interpreted as the section of a line bundle on $\mathfrak{X}$. Then a classical theorem (base change) gives the statement of thm 2.5.5. □

Proof of thm 2.5.3. $\mathcal{M}_{2k}(\mathbb{Z})$ is stabled by the $T(n)$'s as

$$T(n)f(z) = \sum_{m\geq 0}\gamma(m)q^m \qquad \text{with } \gamma(m) = \sum_{\substack{a\mid \gcd(m,n)\\ n\geq 1}} a^{2k-1}c(\frac{mn}{a^2}) \in \mathbb{Z}.$$

Let $\{f_1, \ldots, f_r\}$ be a $\mathbb{Z}$-basis of $\mathcal{M}_{2k}(\mathbb{Z})$, then $\mathrm{Mat}_{\{f_1,\cdots,f_r\}}(T_n) \in M_r(\mathbb{Z})$. (Here $M_r(\mathbb{Z})$ denotes the set of square matrices of order r.) The characteristic polynomial of $T(n)$ is normalized with integral coefficients. Therefore, the eigenvalues of $T(n)$ are algebraic integers. □

Remark 2.10. More generally if A is a ring such that $\mathbb{Z} \subset A \subset \mathbb{C}$, and $\mathcal{M}_{2k}(A) = \left\{ f \in \mathcal{M}_{2k}(\mathrm{SL}_2(\mathbb{Z})) \ ; \ f = \sum_{n\geq 0} a_n q^n \, , a_n \in A \ , \forall \ n \right\}$. Then $\mathcal{M}_{2k}(A) = \mathcal{M}_{2k}(\mathbb{Z}) \otimes_{\mathbb{Z}} A$.

Proposition 2.5.9. *The eigenvalues of $T(n)$ are totally real algebraic numbers.*

Proof. The eigenvalues of $T(n)$ are real as $T(n)$ is a self adjoint operator for the Petersson scalar product. □

2.6 Hecke Algebras

Let $\mathbb{Z} \subset A \subset \mathbb{C}$, and let $\mathcal{H}_{2k,A}$ be the subalgebra of $\mathrm{End}_A(\mathcal{S}_{2k}(A))$ generated by the Hecke operators.

We have $\mathcal{H}_{2k,A} = \mathcal{H}_{2k,\mathbb{Z}} \otimes_{\mathbb{Z}} A$. We call $\mathcal{B}_{2k} = \{f_1, \cdots, f_r\}$ the basis of $\mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ of normalized eigenfunctions of all the Hecke operators acting on $\mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$.

Lemma 2.6.1. *The map*

$$\begin{aligned} \psi_i : \mathcal{H}_{\mathbb{C}} = \mathcal{H}_{2k,\mathbb{C}} &\longrightarrow \mathbb{C} \\ T &\longmapsto \psi_i(T) \end{aligned}$$

where $\psi_i(T)$ is defined by $T \cdot f_i = \psi_i(T) f_i$ is a morphism of algebra (so ψ_i is a character of the Hecke algebra $\mathcal{H}_{\mathbb{C}}$).

Proof. By definition,

$$(TT')f_i = \psi_i(TT')f_i \ \text{ and } \ T(\psi_i(T')f_i) = \psi_i(T')Tf_i = \psi_i(T')\psi_i(T)f_i \ .$$

Therefore $\psi_i(TT') = \psi_i(T)\psi_i(T')$. □

Lemma 2.6.2. *The map*

$$\begin{aligned} \mathcal{H}_{\mathbb{C}} &\longrightarrow \mathbb{C}^r \\ T &\longmapsto (\psi_1(T), \cdots, \psi_r(T)) \end{aligned}$$

is an isomorphism of algebra.

Proof. Clearly, $\mathrm{Mat}_{\mathcal{B}_{2k}}(T) = \begin{pmatrix} \psi_1(T) & & 0 \\ \dots & \dots & \dots \\ 0 & & \psi_r(T) \end{pmatrix}$. Therefore ψ is an injective morphism of algebra. (If $\psi_i(T) = 0$, $\forall\, i$ then $\mathrm{Mat}_{\mathcal{B}_{2k}}(T) = 0$ and $T = 0$.)

The surjectivity of ψ is a consequence of the following.

Lemma 2.6.3. *Let $(\psi_1, \cdots, \psi_r)$ be distinct characters of an algebra A over a field k. Then the ψ_i's are linearly independent.*

We leave the classical proof of this lemma as an exercise. □

Corollary 2.6.4. *$\mathcal{S}_{2k}(\mathbb{C}) := \mathcal{S}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ is a $\mathcal{H}_{2k,\mathbb{C}}$-free module of rank 1 with basis $f = f_1 + \cdots + f_r$.*

Proof. For any $g = \sum_{i=1}^{r} \lambda_i f_i \in \mathcal{S}_{2k}(\mathbb{C})$, there exists uniquely a $T \in \mathcal{H}_{2k,\mathbb{C}}$ such that $T \cdot f = \sum \lambda_i f_i = g$. □

Theorem 2.6.5. *The map*

$$\begin{aligned} \langle\ ,\ \rangle :\ & \mathcal{S}_{2k}(\mathbb{C}) \times \mathcal{H}_{2k,\mathbb{C}} \longrightarrow \mathbb{C} \\ & (f\ , T) \mapsto \langle f, T\rangle := a_1(T \cdot f) = \textit{the first coefficient of } Tf \end{aligned}$$

is a perfect pairing of $\mathcal{H}_{2k,\mathbb{C}}$-free modules of rank 1.

Proof. (a) If $f \in \mathcal{S}_{2k}(\mathbb{C})$ and $\langle f, T_n\rangle = 0$, $\forall\, n \in \mathbb{N}$, then $a_1(T_n f) = a_n(f) = 0$ and therefore $f = 0$.

(b) If $T \in \mathcal{H}_{2k,\mathbb{C}}$ is such that $\langle f, T\rangle = 0$, $\forall\, f \in \mathcal{S}_{2k}(\mathbb{C})$, then $\mathrm{Mat}_{\mathcal{B}_{2k}}(T) = \begin{pmatrix} a_1(Tf_1) & & 0 \\ \dots & \dots & \dots \\ 0 & & a_1(Tf_r) \end{pmatrix} = 0$ and therefore $T = 0$. □

Corollary 2.6.6.

$$\begin{aligned} \mathcal{S}_{2k}(\mathbb{C}) &\xrightarrow{\sim} \mathrm{Hom}_{\mathcal{H}_{2k,\mathbb{C}}}(\mathcal{H}_{2k,\mathbb{C}}, \mathbb{C}) \\ f &\mapsto (T \mapsto \langle f, T\rangle = a_1(Tf)) \end{aligned}$$

is an isomorphism of $\mathcal{H}_{2k,\mathbb{C}}$-modules of rank 1. Here $\mathbb{C}$ is viewed as a trivial $\mathcal{H}_{2k,\mathbb{C}}$-module and the $\mathcal{H}_{2k,\mathbb{C}}$-module structure on $\mathrm{Hom}(\mathcal{H}_{2k,\mathbb{C}}, \mathbb{C})$ is given by

$$T_0 V(T) = V(T_0 T)\ ; \qquad \textit{for}\quad T_1\ , T_0 \in \mathcal{H}_{2k,\mathbb{C}}\ \textit{ and }\ V \in \mathrm{Hom}(\mathcal{H}_{2k,\mathbb{C}}, \mathbb{C})\ .$$

Theorem 2.6.7. *The pairing*

$$\begin{aligned} \mathcal{S}_{2k}(\mathbb{Z}) \times \mathcal{H}_{2k,\mathbb{Z}} &\longrightarrow \mathbb{Z} \\ (f, T) &\longmapsto \langle f, T\rangle = a_1(Tf) \end{aligned}$$

is a perfect pairing, or equivalently, $\mathcal{S}_{2k}(\mathbb{Z}) \simeq \mathrm{Hom}(\mathcal{H}_{2k,\mathbb{Z}}, \mathbb{Z})$ as $\mathcal{H}_{2k,\mathbb{Z}}$-modules.

Proof. Let $\psi \in \mathrm{Hom}(\mathcal{H}_{2k,\mathbb{Z}}, \mathbb{Z})$, then (by theorem 2.6.5) there exists an $f \in \mathcal{S}_{2k}(\mathbb{C})$ such that $\forall\ T \in \mathrm{Hom}(\mathcal{H}_{2k,\mathbb{C}}, \mathbb{C})$, $\psi(T) = \langle f, T\rangle$. Therefore,$\psi(T_n) = \langle f, T_n\rangle = a_1(T_n f) = a_n(f) \in \mathbb{Z}$ and $f \in \mathcal{S}_{2k}(\mathbb{Z})$. □

Remark 2.11. $\mathcal{H}_{2k,\mathbb{Z}} \subset \mathrm{End}_{\mathbb{Z}}(\mathcal{S}_{2k}(\mathbb{Z}))$ is a free $\mathbb{Z}$-module of finite rank. We may find $T_{n_1}, \cdots, T_{n_r}$ generating a free $\mathbb{Z}$-submodule of $\mathcal{H}_{2k,\mathbb{Z}}$ of maximal rank.

Let f be a normalized eigenform of all the Hecke operators T_n. Let $\lambda_{n_1}, \cdots, \lambda_{n_r}$ such that $T_{n_i} f = \lambda_{n_i} f$. Let $K = \mathbb{Q}(\lambda_{n_1}, \cdots, \lambda_{n_r})$. Then K is a totally real number field and for all $n \in \mathbb{N}$, $T_n f = \lambda_n f$ for some $\lambda_n \in K$.

Conclusion. Let $f \in \mathcal{S}_{2k}(\mathbb{C})$ be a normalized eigenform of all the Hecke operators. $f = \sum_{n\geq 1} a_n q^n$. Then $K = \mathbb{Q}(a_1, \cdots, a_n, \cdots)$ is a totally real number field and $a_n \in \mathcal{O}_K$ for all $n \in \mathbb{N}$.

Chapter 3

Geometric Interpretation and Double Cosets

3.1 Commensurability

Let $\Gamma \subset \mathrm{GL}_2(\mathbb{R})^+$ be a discrete subgroup. We say then Γ is a ***lattice*** of $\mathbb{H}$ if $\mathrm{Vol}_{\frac{dxdy}{y^2}}(\Gamma\backslash\mathbb{H}) < \infty$.

Two lattices Γ and Γ' are said to be ***commensurable*** (and written as $\Gamma \approx \Gamma'$) if $[\Gamma : \Gamma \cap \Gamma'] < \infty$ and $[\Gamma' : \Gamma \cap \Gamma'] < \infty$. It is easy to check that commensurability is an equivalence relation.

Let $\tilde{\Gamma} = \mathrm{Comm}_{\mathrm{GL}_2(\mathbb{R})^+}(\Gamma) := \{\gamma \in \mathrm{GL}_2(\mathbb{R})^+ \mid \gamma\Gamma\gamma^{-1} \approx \Gamma\}$. Then

(a) if $\Gamma \approx \Gamma'$, then $\tilde{\Gamma} = \tilde{\Gamma}'$.

(b) $\tilde{\Gamma}$ is a subgroup of $\mathrm{GL}_2(\mathbb{R})^+$.

Proposition 3.1.1. *Let Γ be a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$, then $\tilde{\Gamma} = \mathbb{R}^* \times \mathrm{GL}_2(\mathbb{Q})^+$.*

Proof. We may assume that $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. If $\alpha = c \cdot \beta$ with $c \in \mathbb{R}^*, \beta \in \mathrm{GL}_2(\mathbb{Q})^+$, then $\alpha\Gamma\alpha^{-1} = \beta\Gamma\beta^{-1}$ and we may assume that $\beta \in M_{2,2}(\mathbb{Z})$. Let $m = \det(\beta) \in \mathbb{Z}$.

Lemma 3.1.2. *We have $\Gamma(m) \subset \Gamma \cap \beta\Gamma\beta^{-1} \subset \Gamma = \mathrm{SL}_2(\mathbb{Z})$.*

Proof. Let $\gamma \in \Gamma(m)$, then $m\beta^{-1} \in M_{2,2}(\mathbb{Z})$ and $(m\beta^{-1}) \cdot \gamma\beta \equiv m\beta^{-1}\beta \equiv \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \mod m$.

Therefore $m\beta^{-1}\gamma\beta = m\delta$ for some $\delta \in M_{2,2}(\mathbb{Z})$ and $\det(\delta) = 1$. This implies $\beta^{-1}\Gamma(m)\beta \subset \Gamma = \mathrm{SL}_2(\mathbb{Z})$ and hence $\Gamma(m) \subset \beta\Gamma\beta^{-1} \cap \Gamma \subset \Gamma = \mathrm{SL}_2(\mathbb{Z})$. □

As a consequence, $[\Gamma : \Gamma \cap \beta\Gamma\beta^{-1}] < +\infty$ and applying the same proof with β^{-1} instead of β, we get

$$[\beta\Gamma\beta^{-1} : \beta\Gamma\beta^{-1} \cap \Gamma] = [\Gamma : \Gamma \cap \beta^{-1}\Gamma\beta] < +\infty \ .$$

It then follows $\beta \in \tilde{\Gamma}$. As $\alpha\Gamma\alpha^{-1} = \beta\Gamma\beta^{-1}$, we have $\alpha \in \tilde{\Gamma}$.

Conversely, if $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \tilde{\Gamma}$, then $\alpha \cdot \infty = \frac{a}{c}$ is a cusp of $\alpha\Gamma\alpha^{-1}$, and $\alpha \cdot 0 = \frac{b}{d}$ is also a cusp of $\alpha\Gamma\alpha^{-1}$. Thus, $\frac{a}{c}, \frac{b}{d}$ are cusps of $\Gamma \cap \alpha\Gamma\alpha^{-1}$ and also cusps of Γ. Therefore, $\frac{a}{c}, \frac{b}{d} \in \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.

If $\Gamma \approx \alpha\Gamma\alpha^{-1}$, then ${}^t\Gamma = \Gamma \approx ({}^t\alpha)^{-1}{}^t\Gamma{}^t\alpha$. Hence ${}^t\alpha = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \tilde{\Gamma}$. We can then get $\frac{a}{b}, \frac{c}{d} \in \mathbb{P}^1(\mathbb{Q})$ just by playing the same trick.

Write $b = ab_1, c = ac_1, d = ad_1$ with $b_1, c_1, d_1 \in \mathbb{Q}$, then $\alpha = a \cdot \begin{pmatrix} 1 & b_1 \\ c_1 & d_1 \end{pmatrix} \in \mathbb{R}^* \times \mathrm{GL}_2(\mathbb{Q})^+$. This finishes the proof of proposition 3.1.1. □

Lemma 3.1.3. *Let $\alpha \in \tilde{\Gamma} = \mathbb{R}^* \times \mathrm{GL}_2(\mathbb{Q})^+$. If $\Gamma = \bigsqcup_{i=1}^r (\Gamma \cap \alpha\Gamma\alpha^{-1}\beta_i$, for some $\beta_i \in \Gamma$, then $\Gamma\alpha\Gamma = \{\lambda_1\alpha\lambda_2 | \lambda_1, \lambda_2 \in \Gamma\} = \bigsqcup_{i=1}^r \Gamma\alpha\beta_i$.*

Proof. We have

$$\begin{aligned} \alpha^{-1}\Gamma\alpha\Gamma &= \bigsqcup_{i=1}^{r} \alpha^{-1}\Gamma\alpha(\Gamma \cap \alpha\Gamma\alpha^{-1})\beta_i \\ &\overset{(*)}{=} \bigsqcup_{i=1}^{r} ((\alpha^{-1}\Gamma\alpha\Gamma) \cup (\alpha^{-1}\Gamma\alpha))\beta_i = \bigsqcup_{i=1}^{r} \alpha^{-1}\Gamma\alpha\beta_i \ . \end{aligned}$$

So $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^r \Gamma\alpha\beta_i$. For the proof of the identity $(*)$, we leave to the readers the following exercise.

Exercise 3.1. Prove that $\Gamma'(\Gamma \cap \Gamma') = (\Gamma'\Gamma) \cap \Gamma'$.

In fact, if $\alpha \in \Gamma'(\Gamma \cap \Gamma')$, then $\alpha \in \Gamma'$ and $\alpha = \gamma'\gamma''$ with $\gamma' \in \Gamma'$ and $\gamma'' \in \Gamma \cap \Gamma'$. Therefore, $\alpha \in \Gamma'\Gamma \cap \Gamma'$. The other direction is left to the readers. □

3.2 Algebraic correspondence on a Riemann surface

Let X be a Riemann surface.

Definition 3.1. An ***algebraic correspondence*** on X is a curve $C \hookrightarrow X \times X$(possibly singular) such that the two projections $\pi_1, \pi_2 : C \to X$ are surjective and proper.

Let $d_1 = \deg\pi_1, d_2 = \deg\pi_2$. We may define two maps $T_1 : X \to X^{(d_1)}$, $T_2 : X \to X^{(d_2)}$ where $X^{(d)} = X^d/S_d$ and S_d is the symmetric group in d variables. Therefore $X^{(d)}$ is the set of unordered d-tuples of points of X.

For all $x \in X$, we write $\pi_1^* x = (x_1, \cdots, x_{d_1})$ for the set of points in $\pi_1^*(\{x\})$ counted with multiplicity. Then we define $T_1 \cdot x = \pi_{2*}\pi_1^*\{x\} = \big(\pi_2(x_1), \cdots, \pi_2(x_{d_1})\big)$. $T_2 \cdot x = \pi_{1*}\pi_2^* x$. We say that T_2 is the ***adjoint correspondence*** of T_1.

3.3 Modular correspondence

Let Γ be a lattice in $\mathbb{H}$ and $\alpha \in \tilde{\Gamma}$. We write $\Gamma_\alpha = \Gamma \cap \alpha^{-1}\Gamma\alpha$ and $X_\alpha = \Gamma_\alpha\backslash\mathbb{H}$. As $[\Gamma : \Gamma_\alpha] < +\infty$, we have a finite and surjective map $\pi_1 : \Gamma_\alpha\backslash\mathbb{H} \to \Gamma\backslash\mathbb{H}$, $\Gamma_\alpha x \mapsto \Gamma x$.

Lemma 3.3.1. *There is a well-defined surjective proper morphism of Riemann surfaces*

$$\pi_2 \ : \ \Gamma_\alpha\backslash\mathbb{H} \to \Gamma\backslash\mathbb{H} \ ; \quad \Gamma_\alpha \cdot x \mapsto \Gamma \cdot \alpha x$$

Proof. Let $\gamma \in \Gamma_\alpha$. $\pi_2(\Gamma_\alpha \cdot \gamma x) = \Gamma \cdot \alpha\gamma x = \Gamma \cdot \alpha\gamma\alpha^{-1}\alpha x = \Gamma \cdot \alpha x$ as $\alpha\Gamma\alpha^{-1} \subset \Gamma$ and $\alpha \in \Gamma \cap \alpha^{-1}\Gamma\alpha$. This implies $\pi_2(\Gamma_\alpha\gamma x) = \pi_2(\Gamma_\alpha)x$. All the rest is clear. □

Lemma 3.3.2. *There is a commutative diagram*

$$\begin{array}{ccc} \mathbb{H} & \xrightarrow{\psi} & \mathbb{H} \times \mathbb{H} \\ \downarrow & & \downarrow \\ \Gamma_\alpha\backslash\mathbb{H} & \xrightarrow{\bar{\psi}} & \Gamma\backslash\mathbb{H} \times \Gamma\backslash\mathbb{H} \end{array}$$

where $\psi : z \mapsto (z, \alpha z)$ *and* $\bar{\psi} = (\pi_1, \pi_2)$.

Proof. An easy exercise using lemma.3.3.1. □

Definition 3.2. Let $X_\alpha = \Gamma_\alpha\backslash\mathbb{H}$. Then $Y_\alpha := \bar{\psi}(X_\alpha) \subset \Gamma\backslash\mathbb{H} \times \Gamma\backslash\mathbb{H}$ is an algebraic correspondence. We say that Y_α is a ***modular correspondence*** .

Proposition 3.3.3. *The modular correspondence $T_{1,\alpha} = T_\alpha$ associated with $Y_\alpha \subset \bar{\psi}(X_\alpha)$ is*

$$T_\alpha(\Gamma x) = [\Gamma\alpha\Gamma]\cdot x = \bigsqcup_{\beta_i \in R(\Gamma_\alpha\backslash\Gamma)} \Gamma\alpha\beta_i x$$

where $R(\Gamma_\alpha\backslash\Gamma)$ is a system of representatives in Γ for $\Gamma_\alpha\backslash\Gamma$.

Proof. We have clearly

$$\pi_1^*(\Gamma x) = \bigsqcup_{\beta_i \in R(\Gamma_\alpha\backslash\Gamma)} \Gamma_\alpha\beta_i x$$

and therefore

$$\pi_{2*}\pi_1^*(\Gamma x) = \bigsqcup_{\beta_i \in R(\Gamma_\alpha\backslash\Gamma)} \Gamma\alpha\beta_i x = [\Gamma\alpha\Gamma]\cdot x\ .$$

□

Proposition 3.3.4. *Let $\Gamma = \mathrm{SL}_2(\mathbb{Z}), \alpha = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. Then $\Gamma_\alpha = \Gamma \cap \alpha\Gamma\alpha^{-1} = \Gamma_0(p)$, and the modular correspondence associated to $\bar{\psi}\big(\Gamma_0(p)\backslash\mathbb{H}\big)$ is the correspondence "T_p".*

Proof. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_\alpha$. Then

$$\gamma = \begin{pmatrix} p^{-1} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 & \frac{b_1}{p} \\ pc_1 & d \end{pmatrix}$$

with $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Thus, $\gamma \in \Gamma_0(p)$. A similar proof gives $\Gamma_0(p) \subset \Gamma_\alpha$, so that $\Gamma_\alpha = \Gamma_0(p)$. The associated modular correspondence is

$$\Big[\Gamma\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\Gamma\Big]\cdot x = \bigsqcup_{ad=p,\quad 0\le b<d} \Gamma\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\cdot x = T_p\cdot x$$

as

$$\Gamma\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\Gamma = \bigsqcup_{ad=p,\quad 0\le b<d} \Gamma\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\ .$$

□

More generally , " T_n" $= \bigsqcup_{ad=n\ ,\ d|a\ ,a>0} \Big[\Gamma\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\Gamma\Big]$ is a finite union of double cosets. (Here " $\bigsqcup$ " denotes sum of modular correspondences.)

Remark 3.1. If Γ acts without fixed points on $\mathbb{H}$, then $\pi_1 : \Gamma_\alpha\backslash\mathbb{H} \longrightarrow \Gamma\backslash\mathbb{H}$ and $\pi_2 : \Gamma_\alpha\backslash\mathbb{H} \longrightarrow \Gamma\backslash\mathbb{H}$ are étale morphisms.

Exercise 3.2. Let $C \hookrightarrow \Gamma\backslash\mathbb{H} \times \Gamma\backslash\mathbb{H}$ be such that $\pi_1 : C \to \Gamma\backslash\mathbb{H}$ and $\pi_2 : C \to \Gamma\backslash\mathbb{H}$ are étale. Prove that C is a modular correspondence.

Remark 3.2. When $[\mathrm{Comm}_{\mathrm{SL}_2(\mathbb{R})}(\Gamma) : \Gamma] = \infty$, we say that Γ is an ***arithmetic lattice*** of $\mathbb{H}$. For example, when $\Gamma = \mathrm{SL}_2(\mathbb{Z}), \mathrm{Comm}_{\mathrm{SL}_2(\mathbb{R})}(\Gamma) = \mathrm{SL}_2(\mathbb{Q}) \times \mathbb{R}^*$. So $\mathrm{SL}_2(\mathbb{Z})$ is an arithmetic lattice.

By a theorem of Kasdham and Margulis, there exists a totally real number field F and a quaternion algebra B/F such that $B \otimes \mathbb{R} = M_2(\mathbb{R}) \times \mathbb{H}^{r-1}$ with $r = [F : \mathbb{Q}]$, such that Γ is commensurable with $\mathcal{O}_B^{*,1} := \{z \in \mathcal{O}_B^* | \mathrm{Nm}(z) = 1\}$ where $\mathcal{O}_B^*$ is the group of units in a maximal order $\mathcal{O}_B$ of B.

3.4 The Ring $\mathcal{R}(\Gamma)$

Definition 3.3. Let $\mathcal{R}(\Gamma)$ be the free $\mathbb{Z}$-module with basis the $\Gamma\alpha\Gamma$'s with $\alpha \in \tilde{\Gamma}$. That is, $\mathcal{R}(\Gamma)$ is the set of finite sums $\sum_{\alpha\in\tilde{\Gamma}} c_{\Gamma\alpha\Gamma}[\Gamma\alpha\Gamma]$ with $c_{\Gamma\alpha\Gamma} \in \mathbb{Z}$.

Let $\deg(\Gamma\alpha\Gamma)$ be the number of left Γ-cosets in $\Gamma\alpha\Gamma$. Therefore $\deg(\Gamma\alpha\Gamma) = [\Gamma : \Gamma\alpha^{-1}\Gamma\alpha\cap\Gamma]$. We may extend by linearity to obtain a map $\deg : \mathcal{R}(\Gamma) \to \mathbb{Z}$ by

$$\deg(\sum c_{\Gamma\alpha\Gamma}[\Gamma\alpha\Gamma]) = \sum c_{\Gamma\alpha\Gamma}\deg([\Gamma\alpha\Gamma]) \ .$$

We then define a multiplication $\mathcal{R}(\Gamma) \times \mathcal{R}(\Gamma) \to \mathcal{R}(\Gamma)$ in the following way: If $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^r \Gamma\alpha_i$, $\Gamma\beta\Gamma = \bigsqcup_{j=1}^s \Gamma\beta_j$, then $\Gamma\alpha\Gamma\beta\Gamma = \bigsqcup_{i,j} \Gamma\alpha_i\beta_j$. Therefore, $\Gamma\alpha\Gamma\beta\Gamma$ is a finite union of double cosets $\Gamma\theta\Gamma$ with $\theta \in \tilde{\Gamma}$.

Definition 3.4. We define

$$[\Gamma\alpha\Gamma] \cdot [\Gamma\beta\Gamma] = \sum n_{\Gamma\theta\Gamma}[\Gamma\theta\Gamma] \ .$$

The sum is over the double cosets $\Gamma\theta\Gamma \subset \Gamma\alpha\Gamma\beta\Gamma$ and $n_{\Gamma\theta\Gamma}$ is defined as $n_{\Gamma\theta\Gamma} := \#\{(i,j) \big| \ \Gamma\theta = \Gamma\alpha_i\beta_j\}$.

Proposition 3.4.1. *The definition is independent of the choice of the α_i, β_j and θ.*

Proof. If $\Gamma\alpha_i\beta_j = \Gamma\theta$, then $\Gamma\alpha_i = \Gamma\theta\beta_j^{-1}$. Therefore, if j is fixed there exists at most one $i \in \{1, \ldots, r\}$ such that $\Gamma\alpha_i = \Gamma\theta\beta_j^{-1}$, and there exists one if

and only if $\theta\beta_j^{-1} \in \Gamma\alpha\Gamma$. Thus,

$$\begin{aligned}\#\{(i,j)|\Gamma\alpha_i\beta_j = \Gamma\theta\} &= \#\{j|\Gamma\alpha_i = \Gamma\theta\beta_j^{-1}\} = \#\{j|\theta\beta_j^{-1} \in \Gamma\alpha\Gamma\} \\ &= \#\{j|\beta_j\theta^{-1} \in \Gamma\alpha^{-1}\Gamma\} = \#\{j|\beta_j \in \Gamma\alpha^{-1}\Gamma\theta\} \\ &= \text{number of left cosets } \Gamma\varepsilon \text{ in } \Gamma\beta\Gamma \cap \Gamma\alpha^{-1}\Gamma\theta \ ,\end{aligned}$$

which is independent of α_i and β_j .

If $\Gamma\theta\Gamma = \Gamma\theta'\Gamma$, then $\theta = \lambda_1\theta'\lambda_2$ with $\lambda_i \in \Gamma$. Then

$$\Gamma\beta\Gamma \cap \Gamma\alpha^{-1}\Gamma\theta' = \Gamma\beta\Gamma \cap \Gamma\alpha^{-1}\Gamma\theta\lambda_2 = \bigsqcup \Gamma\varepsilon\lambda_2 \ .$$

If $\Gamma\beta\Gamma \cap \Gamma\alpha^{-1}\Gamma\theta = \bigsqcup \Gamma\varepsilon$, then $n_{\Gamma\theta\Gamma} = n_{\Gamma\theta'\Gamma}$. The proposition is thus proved. □

Remark 3.3. We may extend by linearity this definition to obtain a multiplication $\mathcal{R}(\Gamma) \times \mathcal{R}(\Gamma) \to \mathcal{R}(\Gamma)$.

Lemma 3.4.2. *If* $[\Gamma\alpha\Gamma] \cdot [\Gamma\beta\Gamma] = \sum n_{\Gamma\theta\Gamma}[\Gamma\theta\Gamma]$, *then*

$$\deg([\Gamma\theta\Gamma]) \cdot n_{\Gamma\theta\Gamma} = \#\{(i,j)|\Gamma\alpha_i\beta_j\Gamma = \Gamma\theta\Gamma\} \ .$$

Proof. We write $\Gamma\theta\Gamma = \bigsqcup_{k=1}^{f} \Gamma\theta_k$. Then $f = \deg(\Gamma\theta\Gamma)$ and $\Gamma\alpha_i\beta_j\Gamma = \Gamma\theta\Gamma$ if and only if there exists a unique $k \in \{1, \ldots, f\}$ such that $\Gamma\alpha_i\beta_j = \Gamma\theta_k$. Therefore,

$$\begin{aligned}\#\{(i,j)|\Gamma\alpha_i\beta_j\Gamma = \Gamma\theta\Gamma\} &= \sum_{k=1}^{f} \#\{(i,j)|\Gamma\alpha_i\beta_j = \Gamma\theta_k\} \\ = \sum_{k=1}^{f} n_{\Gamma\theta_k\Gamma} &= f \cdot n_{\Gamma\theta_k\Gamma} = \deg(\Gamma\theta\Gamma) \cdot n_{\Gamma\theta_k\Gamma} \ .\end{aligned}$$

□

Proposition 3.4.3. *For any* $x, y \in \mathcal{R}(\Gamma)$, $\deg(x \cdot y) = \deg(x) \cdot \deg(y)$.

Proof. In fact,

$$\begin{aligned}\deg([\Gamma\alpha\Gamma] \cdot [\Gamma\beta\Gamma]) &= \sum_{\Gamma\theta\Gamma} n_{\Gamma\theta\Gamma} \cdot \deg(\Gamma\theta\Gamma) \\ = \sum_{\Gamma\theta\Gamma} &\#\{(i,j)|\Gamma\alpha_i\beta_j\Gamma = \Gamma\theta\Gamma\} \\ = &\#\{(i,j)\} = \deg(\Gamma\alpha\Gamma) \cdot \deg(\Gamma\beta\Gamma) \ .\end{aligned}$$

□

Proposition 3.4.4. *The multiplication on $\mathcal{R}(\Gamma)$ is associative.*

For the proof, the readers may refer to Shimura's book [?].

Definition 3.5. Let Δ be a semi-group with $\Gamma \subset \Delta \subset \tilde{\Gamma}$, let $\mathcal{R}(\Gamma\,,\,\Delta)$ be the $\mathbb{Z}$-free module with basis $\{[\Gamma\alpha\Gamma] \mid \alpha \in \Delta\}$. Then $\mathcal{R}(\Gamma\,,\,\Delta)$ is endowed with the structure of an associative unit ring with unit element $[\Gamma 1\Gamma]$.

Proposition 3.4.5. *If $\tilde{\Gamma}$ has an antiautomorphism $\alpha \mapsto \alpha^*$ such that*

$$(1)\ (\alpha\cdot\beta)^* = \beta^*\cdot\alpha^*\ ; \quad (2)\ \Gamma^* = \Gamma\ ; \quad (3)\ \forall\alpha\in\Delta\,,(\Gamma\alpha\Gamma)^* = \Gamma\alpha\Gamma = \Gamma\alpha^*\Gamma\ .$$

Then $\mathcal{R}(\Gamma\,,\,\Delta)$ is a commutative ring.

Proof. We write $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^{d}\Gamma\alpha_i = \bigsqcup_{i=1}^{d}\alpha_i\Gamma$ and $\Gamma\beta\Gamma = \bigsqcup_{j=1}^{e}\Gamma\beta_j = \bigsqcup_{j=1}^{e}\beta_j\Gamma$. Then

$$\Gamma\alpha\Gamma = \Gamma\alpha^*\Gamma = \bigsqcup_{i=1}^{d}\Gamma\alpha_i^*\ ;\ \text{and}\quad \Gamma\beta\Gamma = \Gamma\beta^*\Gamma = \bigsqcup_{j=1}^{e}\Gamma\beta_j^*\ .$$

If $\Gamma\alpha\Gamma\beta\Gamma = \bigsqcup_\theta \Gamma\theta\Gamma$, then

$$\Gamma\alpha\Gamma\beta\Gamma = \Gamma\beta^*\Gamma\alpha^*\Gamma = (\Gamma\alpha\Gamma\beta\Gamma)^* = \bigsqcup_\theta(\Gamma\theta\Gamma)^* = \bigsqcup_\theta\Gamma\theta^*\Gamma\ .$$

Suppose $[\Gamma\alpha\Gamma]\cdot[\Gamma\beta\Gamma] = \sum n_{\Gamma\theta\Gamma}[\Gamma\theta\Gamma]$ and $[\Gamma\beta\Gamma]\cdot[\Gamma\alpha\Gamma] = \sum n'_{\Gamma\theta\Gamma}[\Gamma\theta\Gamma]$. We have

$$\begin{aligned} n_{\Gamma\theta\Gamma}\deg([\Gamma\theta\Gamma]) &= \#\{(i,j)|\Gamma\alpha_i\beta_j\Gamma = \Gamma\theta\Gamma\} \\ =\#\{(i,j)|\Gamma\beta_j^*\alpha_i^*\Gamma = \Gamma\theta\Gamma\} &= n'_{\Gamma\theta\Gamma}\deg([\Gamma\theta\Gamma])\ . \end{aligned}$$

Hence, $n_{\Gamma\theta\Gamma} = n'_{\Gamma\theta\Gamma}$, and the commutivity is proved. □

Example 3.1. Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, $\Delta = M_{2,2}(\mathbb{Z})^+$, and let $\mathcal{R}(\Gamma\,,\,\Delta)$ be the free abelian group with basis $\{T(a,d) = \left[\Gamma\left(\begin{smallmatrix}a&0\\0&d\end{smallmatrix}\right)\Gamma\right]\ ;\ a>0, d>0, d|a\}$.

In this description, $T_p = T(p,1)$ when p is prime and more generally, as

$$M(n) = \{\alpha\in M_{2,2}(\mathbb{Z})|\det(\alpha) = n\} = \bigsqcup_{d|a\ ad=n\ a>0}\Gamma\begin{pmatrix}a&0\\0&d\end{pmatrix}\Gamma\ ,$$

we find that

$$T_n = \sum_{d\,|\,a\,,\ ad=n\ \ ,a>0}\left[\Gamma\begin{pmatrix}a&0\\0&d\end{pmatrix}\Gamma\right]\ .$$

The map

$$M_{2,2}(\mathbb{Z})^+ \to M_{2,2}(\mathbb{Z})^+ \; ; \quad \alpha \mapsto \alpha^* = {}^t\alpha$$

satisfies $\Gamma = \Gamma^*$, $(\Gamma\alpha\Gamma)^* = \Gamma\alpha\Gamma$ and $(\alpha\beta)^* = \beta^*\alpha^*$. So $\mathcal{R}(\mathrm{SL}_2(\mathbb{Z}), M_{2,2}(\mathbb{Z})^+)$ is commutative.

If $f \in \mathcal{M}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$, we have an induced action for $\alpha \in M_{2,2}(\mathbb{Z})^+$. Write $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^r \Gamma\alpha_i$, then

$$[\Gamma\alpha\Gamma] \cdot f = \det(\alpha)^{k-1} \sum_{i=1}^{r} f|_{2k}\alpha_i \; ,$$

where as usual

$$f|_{2k}\alpha(z) = \frac{\det(\alpha)^k}{(cz+d)^{2k}} f(\alpha \cdot z) \quad \text{if} \quad \alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) .$$

3.5 Modular forms for congruence subgroups

3.5.1 Congruence Subgroups

Let N be a positive integer. We have defined the groups: $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(1) = \Gamma_1(1) = \Gamma(1)$. By definition, a subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is said to be a ***congruence subgroup***, if $\exists N \in \mathbb{N}$ such that $\Gamma(N) \subset \Gamma \subset \mathrm{SL}_2(\mathbb{Z})$.

Proposition 3.5.1. *The map*

$$\psi \; : \; \Gamma_0(N) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^* \; ; \quad \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d \mod N$$

is well-defined and induces an isomorphism $\Gamma_1(N)\backslash\Gamma_0(N) \simeq (\mathbb{Z}/N\mathbb{Z})^*$.

Proof. From $ad - bNc = 1$, we get $ad \equiv 1 \mod N$ and then d is invertible in $\mathbb{Z}/n\mathbb{Z}$. If

$$\gamma = \left(\begin{smallmatrix} * & * \\ Nc & d \end{smallmatrix}\right) \in \Gamma_0(N) \; , \; \gamma' = \left(\begin{smallmatrix} * & * \\ Nc' & d' \end{smallmatrix}\right) \in \Gamma_0(N) \; ,$$

then $\gamma\gamma' = \left(\begin{smallmatrix} * & * \\ * & Ncb'+dd' \end{smallmatrix}\right)$. Therefore $\psi(\gamma\gamma') = \psi(\gamma)\psi(\gamma')$. This implies ψ is a homomorphism. It is clear that $\mathrm{Ker}\psi = \Gamma_1(N)$.

If $\gcd(d\,, N) = 1$, then there exist $a\,, b \in \mathbb{Z}$ such that $ad - bN = 1$. Thus, $\left(\begin{smallmatrix} a & b \\ N & d \end{smallmatrix}\right) \in \Gamma_0(N)$ and $\psi(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) = d \mod N$. This means ψ is surjective. □

Let Γ be a congruence subgroup. There exists $N \in \mathbb{N}$ such that $\Gamma(N) \subset \Gamma$. Thus, $\mathcal{M}_{2k}(\Gamma) \subset \mathcal{M}_{2k}(\Gamma(N))$, and $\mathcal{S}_{2k}(\Gamma) \subset \mathcal{S}_{2k}(\Gamma(N))$. In principle, we just need to study $\mathcal{M}_{2k}(\Gamma(N))$.

Lemma 3.5.2. *Let $f(z) \in \mathcal{M}_{2k}(\Gamma(N))$ and $g(z) = f(Nz)$, then $g(z) \in \mathcal{M}_{2k}(\Gamma_1(N^2))$. If the Fourier expansion of f at ∞ is $f(z) = \sum_{n=0}^{\infty} a_n e^{\frac{2i\pi nz}{N}}$, then $g(z) = \sum_{n=0}^{\infty} a_n e^{2i\pi nz}$.*

As a result, we need only to study $\mathcal{M}_{2k}(\Gamma_1(N))$ for all N.

Proof. We remark that

$$\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}\Gamma(N)\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)= \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N^2},\ a \equiv d \equiv 1 \pmod{N} \right\}.$$

Therefore, $\Gamma_1(N^2) \subset \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}\Gamma(N)\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Let $\gamma \in \Gamma_1(N^2),\ \gamma = \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}\alpha\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for some $\alpha \in \Gamma(N)$. We then have

$$\begin{aligned} & g|_{2k}\gamma(z) = N^{-k}(f|_{2k}\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right))|_{2k}\gamma(z) \\ =& N^{-k}(f|_{2k}\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right))|_{2k}\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}\alpha\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)(z) \\ =& N^{-k}f|_{2k}\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}\alpha\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)(z) = N^{-k}f|_{2k}\alpha\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)(z) \\ =& N^{-k}f|_{2k}\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)(z) = f(Nz) = g(z)\,. \end{aligned}$$

□

3.5.2 Dirichlet Characters

Let $N \in \mathbb{N}^*$, $\tilde{\chi}$ be a character of $(\mathbb{Z}/N\mathbb{Z})^*$. We have an induced map $\chi : \mathbb{Z} \to \mathbb{C}$ given by

$$\chi(n) = \begin{cases} \tilde{\chi}(n \mod N), & \text{if } \gcd(n, N) = 1 \\ 0, & \text{if } \gcd(n, N) > 1 \end{cases}.$$

with the properties

$$\begin{cases} \chi(nm) = \chi(n)\chi(m) & \\ \chi(m) = \chi(n) & \text{if } m \equiv n \mod N \\ \chi(n) \neq 0 & \text{if and only if } \gcd(n, N) = 1 \end{cases}$$

A map $\chi : \mathbb{Z} \to \mathbb{C}$ with the above properties is always given by a unique character $\tilde{\chi} : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$. We say that χ is a ***Dirichlet character*** modulo N.

If $N \mid M$, and if χ is a Dirichlet character modulo N, then we may define a Dirichlet character $\chi' \mod M$ by

$$\begin{cases} \chi'(n) = \chi(n), & \text{if } \gcd(n, M) = 1 \\ \chi'(n) = 0, & \text{if } \gcd(n, M) > 1 \end{cases}.$$

We then say that χ' *is induced from* χ. If χ is not induced from a character of level $N'|N$, then we say that χ is a ***primitive Dirichlet character***. There exists a smallest integer $n_\chi|N$ such that χ is induced from a primitive character $\mod n_\chi$. We say that n_χ is the ***conductor*** of χ.

For any Dirichlet character $\chi \mod n$, we define a character of $\Gamma_0(N)$ (also denoted by χ) by the formula

$$\chi(\left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right)) = \chi(d) \ .$$

Let $f \in \mathcal{M}_{2k}(\Gamma_1(N))$, then for all $\alpha \in \Gamma_1(N)$, $f|_{2k}\alpha = f$.

Lemma 3.5.3. *If $\beta \in \Gamma_0(N)$ and $f \in \mathcal{M}_{2k}(\Gamma_1(N))$, then $f_{2k}\beta \in \mathcal{M}_{2k}(\Gamma_1(N)$.*

Proof. Let $\alpha \in \Gamma_1(N)$. Then $(f|_{2k}\beta)|_{2k}\alpha = f|_{2k}\beta\alpha = f|_{2k}\beta\alpha\beta^{-1}|_{2k}\beta = f|_{2k}\beta$. □

Thus, we have an action of $\Gamma_1(N)\backslash\Gamma_0(N) \equiv (\mathbb{Z}/N\mathbb{Z})^*$ on $\mathcal{M}_{2k}(\Gamma_1(N)$.

For any Dirichlet character $\chi \mod N$, we write

$$\mathcal{M}_{2k}\big(\Gamma_1(N)\,,\chi\big) = \{f \in \mathcal{M}_{2k}(\Gamma_1(N)) \ \big| \ f|_{2k}\beta = \chi(\beta)f\,, \forall\ \beta \in \Gamma_0(N)\} \ .$$

Proposition 3.5.4. *There is a decomposition*

$$\mathcal{M}_{2k}(\Gamma_1(N)) = \bigoplus_{\chi \mod N} \mathcal{M}_{2k}(\Gamma_0(N), \chi)$$
$$\mathcal{S}_{2k}(\Gamma_1(N)) = \bigoplus_{\chi \mod N} \mathcal{S}_{2k}(\Gamma_0(N), \chi)$$

Proof. This is just the decomposition of the representation of $\Gamma_1(N)\backslash\Gamma_0(N) \cong (\mathbb{Z}/N\mathbb{Z})^*$ on $\mathcal{M}_{2k}(\Gamma_1(N))$ or $\mathcal{S}_{2k}(\Gamma_1(N))$. □

Proposition 3.5.5. *Let χ be a Dirichlet character $\mod N$.*

(1) *If $\chi(-1) \neq 1$, then $\mathcal{M}_{2k}(\Gamma_0(N), \chi) = 0$.*

(2) *Let $w_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$, then the map $f \mapsto f|_{2k}w_N$ induces an isomorphism $\mathcal{M}_{2k}(\Gamma_0(N), \chi) \cong \mathcal{M}_{2k}(\Gamma_0(N), \bar{\chi})$.*

Proof. (1) Let $f \in \mathcal{M}_{2k}(\Gamma_0(N)\,,\chi)$. Then $\chi(-1)f = f|_{2k}\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = f$. Thus, $f = 0$ if $\chi(-1) \neq 1$.

(2) Let $g = f|_{2k}w_N\,, \gamma = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right) \in \Gamma_0(N)$, then $w_N\gamma w_N^{-1} = \left(\begin{smallmatrix} d & -c \\ -Nb & a \end{smallmatrix}\right) \in \Gamma_0(N)$. In particular, w_N normalizes $\Gamma_0(N)$.

If $f \in \mathcal{M}_{2k}(\Gamma_0(N), \chi)$, then

$$(g|_{2k})\gamma = (f|_{2k}w_N)|_{2k}\gamma = (f|_{2k}w_N\gamma w_N^{-1}))|_{2k}w_N = \chi(a)f|_{2k}w_N \ .$$

As $ad \equiv 1 \mod N$, we find $\chi(a) = \bar{\chi}(d)$, and therefore,

$$g|_{2k}\gamma = \bar{\chi}(d) \cdot g \Longleftrightarrow g \in \mathcal{M}_{2k}(\Gamma_0(N), \bar{\chi}) \ .$$

□

Other formulation.

For any $d \in (\mathbb{Z}/N\mathbb{Z})^*$, we fix a $\sigma_d \in \Gamma_0(N)$ such that $\sigma_d \equiv \left(\begin{smallmatrix} \bar{d} & * \\ 0 & d \end{smallmatrix}\right) \mod N$ with $d\bar{d} = 1 \mod N$. We write $\langle d \rangle_{2k}$ for the action of $(\mathbb{Z}/N\mathbb{Z})^*$ on $\mathcal{M}_{2k}(\Gamma_1(N))$ given by $\langle d \rangle_{2k} \cdot f := f|_{2k}\sigma_d$. One can show that it is a well-defined action independent of the choice of the σ_d.

3.6 Modular Interpretation

We know that $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is a moduli space for isomorphism classes $\mathcal{E}$ of elliptic curves over $\mathbb{C}$:

$$\begin{aligned} &\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \longrightarrow \mathcal{E} = \{ \text{ isomorphism classes of elliptic curves over } \mathbb{C}\} \\ &\mathrm{SL}_2(\mathbb{Z}) \cdot \tau \mapsto E_\tau \cong \mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z} \ . \end{aligned}$$

3.6.1 Case of $Y_1(N)$

Proposition 3.6.1. *The modular curve $Y_1(N) = \Gamma_1(N)\backslash\mathbb{H}$ parameterizes the set $\mathcal{E}_1(N)$ of isomorphism classes of couples (E, P) with E an elliptic curve over $\mathbb{C}$, and P a point of $E(\mathbb{C})$ of order N.*

Proof. Let $\Gamma = \Gamma_1(N)$ and $x = \Gamma \cdot \tau \in \Gamma\backslash\mathbb{H}$. We may associate to such an x the elliptic curve $E_\tau = \mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z}$.

Lemma 3.6.2. *For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, the map*

$$\begin{aligned} \mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z} = E_\tau &\to E_{\gamma\tau} = \mathbb{C}/\mathbb{Z} \oplus \gamma\tau\mathbb{Z} \\ z &\mapsto \frac{z}{c\tau + d} \end{aligned}$$

is a well-defined isomorphic $E_\tau \cong E_{\gamma\tau}$ of elliptic curves.

Proof. Define a linear map $v_\gamma : \mathbb{C} \to \mathbb{C}$, $z \mapsto \frac{z}{c\tau+d}$. Then

$$\begin{cases} v_\gamma(a\tau + b) = \frac{a\tau+b}{c\tau+d} = \gamma\tau \ , \\ v_\gamma(c\tau + d) = 1 \ . \end{cases}$$

As $\{a\tau + b, c\tau + d\}$ is a basis of $\mathbb{Z} \oplus \tau\mathbb{Z}$, $v_\gamma(\mathbb{Z} \oplus \tau\mathbb{Z}) = \mathbb{Z} \oplus \gamma\tau\mathbb{Z}$. Hence, $\bar{v}_\gamma$ is an isomorphisms $E_\tau \cong E_{\gamma\tau}$. □

Observe that

$$v_\gamma(\frac{1}{N}) - \frac{1}{N} = \frac{1}{N(c\tau+d)} - \frac{1}{N} = \frac{\frac{c}{N} + \frac{d-1}{N}}{c\tau+d}$$

and

$$\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N) \iff \frac{c}{N} \in \mathbb{Z},\ \frac{d-1}{N} \in \mathbb{Z} \iff v_\gamma(\frac{1}{N}) - \frac{1}{N} \in v_\gamma(\mathbb{Z} \oplus \tau\mathbb{Z})$$

Therefore

$$\gamma \in \Gamma_1(N) \iff v_r(\frac{1}{N}) = \frac{1}{N} \mod \mathbb{Z} \oplus \gamma\tau\mathbb{Z}\ .$$

The conclusion is, the map

$$\Gamma_1(N)\backslash\mathbb{H} \longrightarrow \mathcal{E}_1(N)\ ; \quad \Gamma_1(N)\cdot\tau \mapsto \big(E_\tau = \mathbb{C}/\mathbb{Z}\oplus\tau\mathbb{Z}, P_\tau = \frac{1}{N}\big)$$

is an isomorphism.

We leave it to the reader to check that if E is an elliptic curve over $\mathbb{C}$ and P is a point of order N, then there exists $\tau \in \mathbb{H}$ and $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ such that $\big(E_{\alpha\tau}, v_\alpha(\frac{1}{N})\big) \simeq (E, P)$. □

3.6.2 Case of $Y_0(N)$

Proposition 3.6.3. *$Y_0(N) = \Gamma_0(N)\backslash\mathbb{H}$ is a moduli space for the set $\mathcal{E}_{0,N}$ of isomorphism classes of couples (E, H) where E is an elliptic curve over $\mathbb{C}$ and H is a cyclic subgroup of order N in $E(\mathbb{C})$. More precisely, the map*

$$\begin{aligned} &\Gamma_0(N)\backslash\mathbb{H} \longrightarrow \mathcal{E}_{0,N} \\ &\Gamma_0(N)\tau \mapsto \big(E_\tau = \mathbb{C}/\mathbb{Z}\oplus\tau\mathbb{Z},\ H_\tau = \{0, \frac{1}{N}, \ldots, \frac{N-1}{N}\}\big) \end{aligned}$$

is an isomorphism.

Proof. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, then $\gcd(d, N) = 1$ as $ad - bc = 1$ and $c \equiv 0 \mod N$. If $i \equiv jd \mod N$, then

$$v_\gamma(\frac{i}{N}) - \frac{j}{N} = \frac{\frac{i-jd}{N} - j\frac{c}{N}\tau}{c\tau+d} \in v_\gamma(\mathbb{Z}\oplus\tau\mathbb{Z})\ .$$

We see also that $\Gamma_0(N)$ is the set of matrices in $\mathrm{SL}_2(\mathbb{Z})$ preserving the subgroup $H = \{0, \frac{1}{N}, \ldots, \frac{N-1}{N}\}$. Moreover, for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $v_\gamma\big(\{0, \frac{1}{N}, \ldots, \frac{N-1}{N}\}\big)$ is a cyclic subgroup of order N of E, and any such subgroup is obtained in this way. □

$Y_0(N) = \Gamma_0(N)\backslash\mathbb{H}$ is also a moduli space for isomorphic classes $\mathcal{E}'_{0\,,N}$ of couples (E, E') for some ellliptic curves E and E' over $\mathbb{C}$ such that there exists a cyclic isogeny $\varphi : E \to E'$ of order N. And we have

$$\begin{aligned} \mathcal{E}_{0,N} &\xrightarrow{\sim} \mathcal{E}'_{0,N} \\ (E, H) &\mapsto (E\ , E' = E/H\ , E \to E') \\ (E, \mathrm{Ker}\varphi) &\leftarrow\!\shortmid (E,\ E',\ \varphi : E \to E')\ . \end{aligned}$$

As $\mathcal{E}'_{0,N} \subset \mathcal{E} \times \mathcal{E}$, we get $Y_0(N) \subset \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \times \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$.

We can show also that $\Gamma(N)\backslash\mathbb{H}$ is a moduli space for isomorphism classes of triples $(E\,, P_1\,, P_2)$ with E an elliptic curve over $\mathbb{C}$, P_1, P_2 a basis of $E[N]$ such that $e_N(P_1, P_2)$ is a fixed N-th root of unity, where

$$E[N] := \{P \in E(\mathbb{C}) \,|\, [N]P = 0\ \} \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$$

and $e_N : E[N] \times E[N] \to \mu_N$ is the *Weil paring*.

Chapter 4

Hecke Algebras for $\Gamma_1(N)$

4.1 The Algebras $\mathcal{R}(N)$ and $\mathcal{R}^*(N)$

Let $\Gamma = \Gamma_0(N)$. We define two semigroups $\Delta_0(N)$ and $\Delta_0^*(N)$ in $\mathrm{GL}_2(\mathbb{Q})^+$ by

$$\Delta_0(N) = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \,|\, c \equiv 0 \mod N \,, ad - bc > 0 \,, \gcd(a\,, N) = 1 \},$$

$$\Delta_0^*(N) = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \,|\, c \equiv 0 \mod N \,, ad - bc > 0 \,, \gcd(d\,, N) = 1 \}.$$

Clearly $\Gamma_0(N) \subset \Delta_0(N) \subset \widetilde{\Gamma}_0(N)$ and $\Gamma_0(N) \subset \Delta_0^*(N) \subset \widetilde{\Gamma}_0(N)$. We write $\mathcal{R}(N) = \mathcal{R}(\Gamma_0(N)\,, \Delta_0(N))$ and $\mathcal{R}^*(N) = \mathcal{R}(\Gamma_0(N)\,, \Delta_0^*(N))$ for the corresponding Hecke algebras.

Lemma 4.1.1. *For any $\alpha \in \Delta_0(N)\big($resp. $\alpha \in \Delta_0^*(N)\big)$, there exists positive integers $l\,, m$ determined by α such that*
(1) *$l \,|\, m$, $\gcd(l\,, N) = 1$, $lm = \det\alpha$, and*
(2) *$\Gamma_0(N)\alpha\Gamma_0(N) = \Gamma_0(N)\left(\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right)\Gamma_0(N)\big($ resp. $\Gamma_0(N)\alpha\Gamma_0(N) = \Gamma_0(N)\left(\begin{smallmatrix} m & 0 \\ 0 & l \end{smallmatrix}\right)\Gamma_0(N)\big)$.*
Moreover, if $\gcd(lm\,, N) = 1$, then

$$\Gamma_0(N)\left(\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right)\Gamma_0(N) = \Gamma_0(N)\left(\begin{smallmatrix} m & 0 \\ 0 & l \end{smallmatrix}\right)\Gamma_0(N).$$

Proof. Exercise. Using the *theorem of elementary divisors*. □

Proposition 4.1.2. *$\mathcal{R}(N)$ and $\mathcal{R}^*(N)$ are commutative algebras.*

Proof. We just need to find an antiautomorphism $\alpha \mapsto \alpha^*$ of $\Delta_0(N)$ such that (i) $(\alpha\beta)^* = \beta^*\alpha^*$; (ii) $\Gamma^* = \Gamma$ ($\Gamma = \Gamma_0(N)$ here) and (iii) $\forall \alpha \in \Delta_0(N)$, $(\Gamma\alpha\Gamma)^* = \Gamma\alpha\Gamma$.

If $\alpha = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right)$, we define $\alpha^* = \left(\begin{smallmatrix} a & c \\ Nb & d \end{smallmatrix}\right)$. Then it's easy to see $\Gamma^* = \Gamma$. For (i), just check by computation, verifying $\alpha^* = w_N \alpha^{-1} w_N^{-1}$ where $w_N = \left(\begin{smallmatrix} 0 & 1 \\ -N & 0 \end{smallmatrix}\right)$. For (iii), we have, by lemma.4.1.1,

$$(\Gamma\alpha\Gamma)^* = \left(\Gamma\left(\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right)\Gamma\right)^* = \Gamma^*\left(\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right)^*\Gamma^* = \Gamma\left(\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right)\Gamma.$$

□

Now our goal is to *define an action of* $\mathcal{R}(N)$ *and* $\mathcal{R}^*(N)$ *on the space* $\mathcal{S}_{2k}(N, \chi) := \mathcal{S}_{2k}(\Gamma_0(N), \chi)$. Here $\chi : (\mathbb{Z}/N\mathbb{Z})^* \cong \Gamma_1(N)\backslash\Gamma_0(N) \longrightarrow \mathbb{C}^*$ is a Dirichlet character.

Definition 4.1. Let $\chi : \Gamma_0(N) \longrightarrow \mathbb{C}^*$ be the character $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \chi(\alpha) := \chi(d)$ defined by a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{C}^*$. We define $\widetilde{\chi} : \Delta_0(N) \longrightarrow \mathbb{C}^*$ by $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \bar{\chi}(a)$ and $\chi^* : \Delta_0^*(N) \longrightarrow \mathbb{C}^*$ by $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \chi(d)$.

We remark that $\widetilde{\chi}|_{\Gamma_0(N)} = \chi = \chi^*|_{\Gamma_0(N)}$ and $\begin{cases} \widetilde{\chi}(\alpha\beta) = \widetilde{\chi}(\alpha)\widetilde{\chi}(\beta) \\ \chi^*(\alpha\beta) = \chi^*(\alpha)\chi^*(\beta) \end{cases}$.

Definition 4.2. Let $f \in \mathcal{S}_{2k}(N, \chi)$ and $\alpha \in \Delta_0(N)$. We write $\Gamma_0(N)\alpha\Gamma_0(N) = \coprod_v \Gamma_0(N)\alpha_v$ and define

$$[\Gamma_0(N)\alpha\Gamma_0(N)] \cdot f := \det(\alpha)^{k-1} \sum_v \overline{\widetilde{\chi}(\alpha_v)} f|_{2k}\alpha_v. \tag{4.1}$$

Sometimes we write $[\Gamma_0(N)\alpha\Gamma_0(N)] \cdot f = T_{N,k,\chi}(\alpha) \cdot f$.

Remark 4.1. The formula (4.1) is independent of the choice of representatives α_v.

Proof. Let $\alpha_v' = \beta_v\alpha_v$ with $\beta_v \in \Gamma_0(N)$. Then

$$\begin{aligned} \overline{\widetilde{\chi}}(\beta_v)\overline{\widetilde{\chi}}(\alpha_v) f|_{2k}\beta_v\alpha_v &= \overline{\widetilde{\chi}}(\beta_v)\overline{\widetilde{\chi}}(\alpha_v)(f|_{2k}\beta_v)|_{2k}\alpha_v \\ &= \chi(\beta_v)\overline{\chi}(\beta_v)\overline{\widetilde{\chi}(\alpha_v)} f|_{2k}\alpha_v = \overline{\widetilde{\chi}(\alpha_v)} f|_{2k}\alpha_v \end{aligned}$$

□

Remark 4.2. We must verify that $g := [\Gamma_0(N)\alpha\Gamma_0(N)] \cdot f \in \mathcal{S}_{2k}(N, \chi)$.

Proof. Let $\beta \in \Gamma_0(N)$. Then $\Gamma_0(N)\alpha\Gamma_0(N) = \coprod_v \Gamma_0(N)\alpha_v = \coprod_v \Gamma_0(N)\alpha_v\beta$. By remark.(4.1), we have

$$\begin{aligned} g|_{2k}\beta &= \det(\alpha)^{k-1} \sum_v \overline{\widetilde{\chi}}(\alpha_v)(f|_{2k}\alpha_v)|_{2k}\beta \\ &= \chi(\beta)\det(\alpha)^{k-1} \sum_v \overline{\widetilde{\chi}}(\alpha_v\beta) f|_{2k}\alpha_v\beta = \chi(\beta) g \end{aligned}$$

This implies $g \in \mathcal{S}_{2k}(N\,,\chi)$. □

Remark 4.3. For $\alpha \in \Delta_0^*(N)$ with $\Gamma_0(N)\alpha\Gamma_0(N) = \coprod_v \Gamma_0(N)\alpha_v$, we define

$$[\Gamma_0(N)\alpha\Gamma_0(N)] \cdot f := \det(\alpha)^{k-1} \sum_v \overline{\chi^*(\alpha_v)} f|_{2k}\alpha_v. \tag{4.2}$$

Definition 4.3. For all couples $(l\,,m)$ such that $\begin{cases} l \mid m\,, l > 0\,, m > 0 \\ \gcd(l\,,\, N) = 1 \end{cases}$, we define $T(l\,,m) \in \mathcal{R}(N)$ and $T(n) \in \mathcal{R}(N)$ by

$$T(l,m) = [\Gamma_0(N)\left(\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right)\Gamma_0(N)]\,, \quad T(n) = \sum_{lm=n} T(l,m).$$

We also define $T^*(l\,,m) \in \mathcal{R}^*(N)$ and $T^*(n) \in \mathcal{R}^*(N)$ by

$$T^*(m,l) = [\Gamma_0(N)\left(\begin{smallmatrix} m & 0 \\ 0 & l \end{smallmatrix}\right)\Gamma_0(N)]\,, \quad T^*(n) = \sum_{lm=n} T^*(m,l).$$

If $\gcd(n\,,N) = 1$, then $\left(\begin{smallmatrix} n & 0 \\ 0 & n \end{smallmatrix}\right) \in \Delta_0^*(N) \cap \Delta_0(N)$ and $\Gamma_0(N)\left(\begin{smallmatrix} n & 0 \\ 0 & n \end{smallmatrix}\right)\Gamma_0(N) = \Gamma_0(N)\left(\begin{smallmatrix} n & 0 \\ 0 & n \end{smallmatrix}\right)$. Therefore $T(n\,,n)T(l,m) = T(nl,nm)$ and $T^*(n,n)T^*(m,l) = T^*(nm,nl)$.

Theorem 4.1.3. (1) *For all* $f \in \mathcal{S}_{2k}(N,\chi)$,

$$\begin{cases} T^*(m\,,l)f = \bar{\chi}(lm)T(l\,,m)f & \text{if } \gcd(lm\,,N) = 1 \\ T^*(n)f = \bar{\chi}(n)T(n)f & \text{if } \gcd(n\,,N) = 1 \end{cases}$$

(2) $T(l\,,m)$ *and* $T^*(m\,,l)$ *are mutual adjoint operators with respect to the Petersson scalar product on* $\mathcal{S}_{2k}(N\,,\chi)$.
(3) $\mathcal{S}_{2k}(N\,,\chi)$ *has a basis of eigenfunctions for all the Hecke operators* $T(n)$ *with* $\gcd(n\,,N) = 1$ *and* $T(l\,,m)$ *with* $\gcd(lm\,,N) = 1$.

Proof. (1) We have

$$\Delta_0^*(N)\cap\Delta_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \pmod{N},\ \gcd(ad, N) = 1,\ ad - bc > 0 \right\}.$$

Therefore, if $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta_0^*(N) \cap \Delta_0(N)$ then

$$\chi^*(\alpha) = \chi(d) = \chi(ad)\bar{\chi}(a) = \chi(\det(\alpha))\widetilde{\chi}(\alpha).$$

If $\gcd(lm, N) = 1$, then $\Gamma_0(N)\left(\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right)\Gamma_0(N) = \Gamma_0(N)\left(\begin{smallmatrix} m & 0 \\ 0 & l \end{smallmatrix}\right)\Gamma_0(N) = \coprod_v \Gamma_0(N)\alpha_v$ for suitable α_v.

$$\begin{aligned} T^*(m, l)f &= (ml)^{k-1} \sum_v \overline{\chi^*}(\alpha_v) f|_{2k}\alpha_v = (ml)^{k-1}\bar{\chi}(lm) \sum_v \overline{\widetilde{\chi}}(\alpha_v) f|_{2k}\alpha_v \\ &= \bar{\chi}(lm) T(l, m) f \end{aligned}$$

The result for $T(n)$ is a consequence of the result for $T(l, m)$.

(2) Let $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})^+$. Define $\alpha' := \det(\alpha)\alpha^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$. Then $\alpha \mapsto \alpha'$ is an anti-isomorphism from $\Delta_0(N)$ to $\Delta_0^*(N)$.

We can find a coset decomposition $\Gamma_0(N)\left(\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right)\Gamma_0(N) = \coprod_v \Gamma_0(N)\alpha_v = \coprod_v \alpha_v\Gamma_0(N)$. Then

$$\Gamma_0(N)\left(\begin{smallmatrix} m & 0 \\ 0 & l \end{smallmatrix}\right)\Gamma_0(N) = \left(\Gamma_0(N)\left(\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right)\Gamma_0(N)\right)' = \coprod_v \Gamma_0(N)\alpha_v'$$

We proved that for any $f, g \in \mathcal{S}_{2k}(N, \chi)$ and $\alpha \in \Gamma_0(N) \in \Gamma_0(N)$, $\langle f|_{2k}\alpha,\ g\rangle = \langle f,\ g|_{2k}\alpha_v'\rangle$. Now we have

$$\begin{aligned} \langle T(lm)f,\ g\rangle &= (ml)^{k-1} \sum_v \overline{\widetilde{\chi}}(\alpha_v)\langle f|_{2k}\alpha_v,\ g\rangle = (ml)^{k-1}\langle f,\ \sum_v \widetilde{\chi}(\alpha_v) g|_{2k}\alpha_v'\rangle \\ &= \langle f,\ (ml)^{k-1} \sum_v \overline{\chi^*}(\alpha_v')g|_{2k}\alpha_v'\rangle = \langle f,\ T^*(m, l)g\rangle \end{aligned}$$

Note that in the above computation we have used the following

Lemma 4.1.4. $\widetilde{\chi}(\alpha) = \overline{\chi^*}(\alpha')$.

Proof.

$$\begin{aligned} \overline{\chi^*}(\alpha') &= \overline{\chi^*(\det(\alpha))\chi^*(\alpha^{-1})} = \overline{\chi^*(\det\alpha)}\chi^*(\alpha) \\ &= \overline{\chi^*(\det\alpha)}\chi(\det\alpha)\widetilde{\chi}(\alpha) = \widetilde{\chi}(\alpha). \end{aligned}$$

□

(3) As $T^*(m\,,l)$ and $T(l\,,m)$ commutes by (1), we see that $T(l\,,m)$ is a normal operator ("normal" means it commutes with its adjoint operator). As $\mathcal{R}(N)$ is a commutative algebra, we see that there is a basis of $\mathcal{S}_{2k}(N\,,\chi)$ of eigenfunctions of all the Hecke operators $T(l\,,m)$ with $\gcd(lm\,,N)=1$ and $T(n)$ with $\gcd(n\,,N)=1$. This is a consequence of the following lemma.

Lemma 4.1.5. *If T is a normal operator, then there exists a basis of eigenfunctions of T.*

□

Proposition 4.1.6. (1) $\mathcal{R}(N)=\mathcal{R}(\Gamma_0(N)\,,\Delta_0(N))$ *is as a $\mathbb{Z}$-algebra a polynomial ring in the variables $T(p)=T(1\,,p)$ for all prime number p and $T(p\,,p)$ for all* $\gcd(p\,,N)=1$.

(2) *If* $\gcd(m\,,n)=1$ *or if $m\,|\,N^\infty$ or $n\,|\,N^\infty$, then $T(m\,,n)=T(m)T(n)$.* (*We say $n\,|,N^\infty$ if $n=\prod_{p\,|\,N}p^{n_p}$.*)

(3) $\mathcal{R}(\Gamma_0(N)\,,\Delta_0(N))$ *is generated over $\mathbb{Q}$ by the Hecke operators $T(n)\,,n\in\mathbb{N}$.*

Remark 4.4. We have

$$T(p^\ell)=\begin{cases}\sum_{1\le r\le\ell}\left[\Gamma_0(N)\left(\begin{smallmatrix}p^r&0\\0&p^{\ell-r}\end{smallmatrix}\right)\Gamma_0(N)\right] & \text{if } \gcd(p\,,N)=1\\ T(1\,,p^\ell)=\left[\Gamma_0(N)\left(\begin{smallmatrix}1&0\\0&p^\ell\end{smallmatrix}\right)\Gamma_0(N)\right] & \text{if } p\,|\,N\end{cases}$$

When we work at a level N, we sometimes write $T_N(n)$ or $T_N(a\,,b)\in\mathcal{R}(\Gamma_0(N)\,,\Delta_0(N))$.

For example, if $N=1$, we find by (1) that $\mathcal{R}(\Gamma_0(N)\,,\Delta_0(N))=\mathbb{Z}[T_1(p)\,,T_1(p\,,p)]$ and there is a surjective morphism:

$$\begin{aligned}\mathcal{R}(1)&\longrightarrow\mathcal{R}(N)\\ T_1(p)&\mapsto T_N(p)\\ T_1(p\,,p)&\mapsto\begin{cases}T_N(p\,,p) & \text{if } \gcd(p\,,N)=1\\ 0 & \text{if } p\,|\,N\end{cases}\end{aligned}$$

The relation in level 1

$$T_1(m)T_1(n)=\sum_{d\,|\,\gcd(m\,,n)}dT_1(d\,,d)T_1\big(\frac{mn}{d^2}\big)$$

induces the relation

$$T_N(m)T_N(n)=\sum_{d\,|\,\gcd(m\,,n)}dT_N(d\,,d)T_N\big(\frac{mn}{d^2}\big)\,,\quad(T_N(d\,,d)=0\text{ if }\gcd(d\,,N)\neq1)\,.$$

Lemma 4.1.7. *Let p be a prime number and $\ell \geq 1$.*

(1)

$$T(p)T(1\,,p^{\ell}) = \begin{cases} T(1\,,p^{\ell}) + (p+1)T(p\,,p) & \text{if } \gcd(p\,,N) = 1\,, \ell = 1 \\ T(1\,,p^{\ell+1}) + pT(p\,,p)T(1\,,p^{\ell}) & \text{if } \gcd(p\,,N) = 1\,, \ell > 1 \\ T(1\,,p^{\ell+1}) & \text{if } p \,|\, N \end{cases}$$

(2)

$$T(p)T(p^{\ell}) = \begin{cases} T(p^{\ell+1}) + pT(p\,,p)T(1\,,p^{\ell-1}) & \text{if } \gcd(p\,,N) = 1 \\ T(p^{\ell+1}) & \text{if } p \,|\, N \end{cases}$$

(3) *If* $\gcd(\ell m\,, \ell' m') = 1$, *then*

$$T(\ell\,,m)T(\ell'\,,m') = T(\ell\ell'\,,mm')\,.$$

Remark 4.5. For $\gcd(p\,,N) = 1$, the results are the same as in level 1 and can be shown in the same way. So we may either adapt the proof or "think adelically". For $p \,|\, N$, there is only one formula to prove as $T(p^{\ell}) = T(1\,,p^{\ell})$.

We need to show

$$T(p^{\ell})T(p) = T(p^{\ell+1}) = T(1\,,p^{\ell})T(1\,,p) = T(1\,,p^{\ell+1})\,.$$

By definition,

$$\big[\Gamma_0(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p^{\ell}\end{smallmatrix}\right)\Gamma_0(N)\big]\big[\Gamma_0(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma_0(N)\big] = \sum n_{\theta}\big[\Gamma_0(N)\theta\Gamma_0(N)\big]$$

with

$$\Gamma_0(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p^{\ell}\end{smallmatrix}\right)\Gamma_0(N) = \bigsqcup \Gamma_0(N)\theta\Gamma_0(N)\,.$$

But then for such θ, we have $\det(\theta) = p^{\ell+1}$ and $\theta \in \Delta_0(N)$. Therefore,

$$\Gamma_0(N)\theta\Gamma_0(N) = \Gamma_0(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p^{\ell+1}\end{smallmatrix}\right)\Gamma_0(N)\,.$$

So we get $T(p^{\ell})T(p) = c \cdot T(p^{\ell+1})$. We must prove the constant $c = 1$. By the following lemma.4.1.8,

$$p^{\ell} \cdot p = \deg(T_{p^{\ell}})\deg(T_p) = c\det(T_{p^{\ell+1}}) = cp^{\ell+1}\,.$$

So we get $c = 1$.

Lemma 4.1.8. *If $p \,|\, N$, then*

$$\Gamma_0(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p^\ell\end{smallmatrix}\right)\Gamma_0(N) = \bigsqcup_{0\le n<p^\ell} \Gamma_0(N)\left(\begin{smallmatrix}1 & n\\ 0 & p^\ell\end{smallmatrix}\right).$$

In particular, $\deg(T_{p^\ell}) = p^\ell$.

Proof. Let $\beta = \left(\begin{smallmatrix}a & b\\ Nc & d\end{smallmatrix}\right) \in \Gamma_0(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p^\ell\end{smallmatrix}\right)\Gamma_0(N)$. As $\beta \in \Delta_0(N)$, $\gcd(a\,, N) = 1$. The relation $ad = bnc = p^\ell$ implies that

$$\gcd(a\,, Nc) = p^r \quad \text{with} \quad 0 \le r < \ell\,.$$

Since $p \nmid N$ and $\gcd(a\,, N) = 1$, $r = 0$. Therefore, $\gcd(a\,, Nc) = 1$ and there exists $\gamma_1 \in \Gamma_0(N)$ such that $\gamma_1 = \left(\begin{smallmatrix}* & *\\ -Nc & a\end{smallmatrix}\right)$ and

$$\gamma_1\beta = \left(\begin{smallmatrix}* & *\\ -Nc & a\end{smallmatrix}\right)\left(\begin{smallmatrix}a & b\\ Nc & d\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & n\\ 0 & p^\ell\end{smallmatrix}\right).$$

If we write $n = ep^\ell + m$ with $0 \le m < p^\ell$, then

$$\gamma_2 = \left(\begin{smallmatrix}1 & -e\\ 0 & 1\end{smallmatrix}\right) \in \Gamma_0(N) \ \text{ and } \ \gamma_2\gamma_1\beta = \left(\begin{smallmatrix}1 & m\\ 0 & p^\ell\end{smallmatrix}\right).$$

This shows

$$\Gamma_0(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p^\ell\end{smallmatrix}\right)\Gamma_0(N) = \bigcup_{0\le n<p^\ell} \Gamma_0(N)\left(\begin{smallmatrix}1 & n\\ 0 & p^\ell\end{smallmatrix}\right).$$

This union is disjoint: if $\gamma \in \Gamma_0(N)$ is such that $\gamma\left(\begin{smallmatrix}1 & m\\ 0 & p^\ell\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & m'\\ 0 & p^\ell\end{smallmatrix}\right)$ with $0 \le m\,, m' < p^\ell$, then $\gamma = \left(\begin{smallmatrix}1 & \frac{m'-m}{p^\ell}\\ 0 & 1\end{smallmatrix}\right)$. This implies $m \equiv m' \mod p^\ell$ and hence $m = m'$. □

Proof of Prop.4.1.6. (1) It is a consequence of lemma.4.1.7 using induction on ℓ: the relation

$$T(1\,, p^{\ell+1}) = T(p)T(p^\ell) - \begin{cases}(p+1)T(p\,,p) & \text{if } p \nmid N\,, \ell = 1\\ pT(p\,,p)T(1\,,p^\ell) & \text{if } p \nmid N\,, \ell > 1\end{cases}.$$

implies that if $T(1\,, p^\ell) \in \mathbb{Z}[T(1\,, p)\,, T(p\,, p)]$, then $T(1\,, p^{\ell+1}) \in \mathbb{Z}[T(1\,, p)\,, T(p\,, p)]$.

(2) is a consequence of the adelic description if $\gcd(m\,, n)$ and of the relation $T(p^e)T(p^f) = T(p^{e+f})$.

(3) is a consequence of (1) and the relation

$$pT(p\,,p) = T(p)^2 - T(p^2) \Longleftrightarrow T(p\,,p) = \frac{T(p)^2 - T(p^2)}{p}\,.$$

□

4.2 Adèlic Interpretation

This section is devoted to the explanation of the principle "any relation for $T(m)$ in level 1 induces a similar relation for $T_N(m)$ if $\gcd(m\,,N)=1$".

Let $\mathbb{A}=\mathbb{A}_f\times\mathbb{R}$ be the ring of adèles:

$x\in\mathbb{A}\Leftrightarrow x=(x_p)_{p\le\infty}$ with $x_p\in\mathbb{Q}_p$ and for almost all p, $x\in\mathbb{Z}_p$.

We then define the topological groups $\mathrm{GL}_2(\mathbb{A})$ and $\mathrm{GL}_2(\mathbb{A}_f)$. Let $\widehat{\mathbb{Z}}=\prod_{p<\infty}\mathbb{Z}_p$, then $\mathrm{GL}_2(\widehat{\mathbb{Z}})=\prod_{p<\infty}\mathrm{GL}_2(\mathbb{Z}_p)$ is a maximal open compact subgroup of $\mathrm{GL}_2(\mathbb{A}_f)$.

Let $K=\prod_{p<\infty}K_p\subset\mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an open compact subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. For all $p\gg 0$, $K_p=\mathrm{GL}_2(\mathbb{Z}_p)$ and for all p, $[\mathrm{GL}_2(\mathbb{Z}_p)\,:\,K_p]<\infty$.

We suppose that for all $p>0$, the map $\det\,:K_p\longrightarrow\mathbb{Z}_p^*$ is surjective. We write $\Gamma=K\cap\mathrm{GL}_2(\mathbb{Q})^+\subset\mathrm{GL}_2(\mathbb{Z})^+=\mathrm{SL}_2(\mathbb{Z})$, i.e,

$$\Gamma=\{\,g\in\mathrm{GL}_2(\mathbb{Q})^+\;\big|\;g_p\in K_p\,,\forall\,p\,\}\,.$$

Proposition 4.2.1. *We have*

$$\Gamma\backslash\mathbb{H}=\mathrm{GL}_2(\mathbb{Q})^+\backslash\mathbb{H}\times\mathrm{GL}_2(\mathbb{A}_f)/K$$

where $\mathrm{GL}_2(\mathbb{Q})^+$ *acts diagonally on* $\mathbb{H}\times\mathrm{GL}_2(\mathbb{A}_f)/K$.

Proof. The strong approximation theorem says that $\mathrm{SL}_2(\mathbb{Q})$ is dense in $\mathrm{SL}_2(\mathbb{A}_f)$. As $K\cap\mathrm{SL}_2(\mathbb{A}_f)$ is an open compact subgroup of $\mathrm{SL}_2(\mathbb{A}_f)$, $\mathrm{SL}_2(\mathbb{Q})\cdot K\cap\mathrm{SL}_2(\mathbb{A}_f)$ is open and dense. Therefore, $\mathrm{SL}_2(\mathbb{A}_f)=\mathrm{SL}_2(\mathbb{Q})\cdot(K\cap\mathrm{SL}_2(\mathbb{A}_f))$.

We know also that

$$\mathbb{Q}^*\backslash\mathbb{A}_f^*/\widehat{\mathbb{Z}}^*\cong\text{the class group of }\;\mathbb{Z}=\{\,1\,\}$$

then by the exact sequence

$$1\to 1=\mathrm{SL}_2(\mathbb{Q})\backslash\,\mathrm{SL}_2(\mathbb{A}_f)/K\cap\mathrm{SL}_2(\mathbb{A}_f)\to\mathrm{GL}_2(\mathbb{Q})\backslash\,\mathrm{GL}_2(\mathbb{A}_f)/K\overset{\det}{\to}\mathbb{Q}^*\backslash\mathbb{A}_f^*/\widehat{\mathbb{Z}}^*=1$$

we get $\mathrm{GL}_2(\mathbb{A}_f)=\mathrm{GL}_2(\mathbb{Q})\cdot K$.

We write $[z\,,gK]$ for an element of

$$\mathscr{S}:=\mathrm{GL}_2(\mathbb{Q})^+\backslash\mathbb{H}\times\mathrm{GL}_2(\mathbb{A}_f)/K\;.$$

Then $g=g_{\mathbb{Q}}\cdot k$ with $g_{\mathbb{Q}}\in\mathrm{GL}_2(\mathbb{Q})$, $k\in K$ and $[z\,,gK]=[g_{\mathbb{Q}}^{-1}z\,,\,1\cdot K]$. Therefore, any element of $\mathscr{S}$ has a representative of the form $[z\,,1\cdot K]$. If $[z_1\,,1\cdot K]=[z_2\,,1\cdot K]$, then there exist $k\in K$ and $g_{\mathbb{Q}}\in\mathrm{GL}_2(\mathbb{Q})^+$ such that $z_2=g_{\mathbb{Q}}z_1$ and $g_{\mathbb{Q}}\in K\cap\mathrm{GL}_2(\mathbb{Q})^+=\Gamma$. So we get $\mathscr{S}=\Gamma\backslash\mathbb{H}$. □

If more generally, $\det(K) \neq \widehat{\mathbb{Z}}^*$, then the connected components of $\mathscr{S} := \mathrm{GL}_2(\mathbb{Q})^+\backslash\mathbb{H} \times \mathrm{GL}_2(\mathbb{A}_f)/K$ are indexed by the finite set

$$\mathrm{GL}_2(\mathbb{Q})\backslash\, \mathrm{GL}_2(\mathbb{A}_f)/K \cong \mathbb{Q}^*\backslash\mathbb{A}_f^*/\det(K)$$

that is,

$$\mathscr{S} = \coprod_{g\in R} \Gamma_g\backslash\mathbb{H}$$

where R is a system of representatives in $\mathrm{GL}_2(\mathbb{A}_f)$ for $\mathrm{GL}_2(\mathbb{Q})^+\backslash\, \mathrm{GL}_2(\mathbb{A}_f)/K$ and $\Gamma_g = g^{-1}Kg \cap \mathrm{GL}_2(\mathbb{Q})^+$.

Example 4.1. Let $N = \prod p^{n_p}$ and $K_0(N) = \prod_{p|N} K_0(p^{n_p}) \times \prod_{p\nmid N} \mathrm{GL}_2(\mathbb{Z}_p)$ where

$$K_0(p^{n_p}) = K_p := \{\, k \in \mathrm{GL}_2(\mathbb{Z}_p) \,\big|\, k \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \mod p^{n_p} \,\}\ .$$

Then $\det(K_p) = \mathbb{Z}_p^*$ and

$$\mathrm{GL}_2(\mathbb{Q})^+\backslash\mathbb{H} \times \mathrm{GL}_2(\mathbb{A}_f)/K_0(N) = \Gamma_0(N)\backslash\mathbb{H}\ .$$

We shall omit the proof of the following proposition, which uses the strong approximation theorem.

Proposition 4.2.2. *Let $\alpha \in \mathrm{GL}_2(\mathbb{Q})$, $\Gamma\alpha\Gamma = \coprod \Gamma\alpha_i$, $K\alpha K = \coprod \beta_j K$. Let*

$$\begin{aligned} \psi : \Gamma\backslash\mathbb{H} &\xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Q})^+\backslash\mathbb{H} \times \mathrm{GL}_2(\mathbb{A}_f)/K \\ \Gamma z &\mapsto\ \psi(\Gamma z) := [z\,, 1\cdot K]\ . \end{aligned}$$

Then $\psi([\Gamma\alpha\Gamma]\cdot\Gamma z) = \psi(\Gamma z)\cdot[K\alpha K]$ where

$$[\Gamma\alpha\Gamma]\cdot\Gamma z = \coprod \Gamma\alpha_i z \quad \textit{and} \quad [z\,, gK]\cdot[K\alpha K] = \coprod [z\,, g\beta_j K]$$

As a conclusion, we find that for N prime to p, to compute $T_1(p)$ or $T_N(p)$ we just need to write out the coset decomposition of $\mathrm{GL}_2(\mathbb{Z}_p)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\mathrm{GL}_2(\mathbb{Z}_p)$ and this is independent of N.

We saw in level 1 the relation

$$T_1(m)T_1(n) = \sum_{\ell\,|\,\gcd(m\,,n)} \ell T_1(\ell\,,\ell) T_1\big(\frac{mn}{\ell^2}\big)$$

and this is formally equivalent to the existence of an Eulerian product

$$\sum_{n=1}^{\infty} T_1(n)s^{-s} = \prod_p \left(1 - T_1(p)p^{-s} + T_1(p\,,p)p^{1-2s}\right)^{-1}\ .$$

In level N, we obtain the relation

$$T_N(m)T_N(n) = \sum_{\ell \mid \gcd(m\,,n) \;\; \gcd(\ell\,,N)=1} \ell T_N(\ell\,,\ell) T_N\big(\frac{mn}{\ell^2}\big)$$

which is formally equivalent to

$$\sum_{n=1}^{\infty} T_N(n) s^{-s} = \prod_{p \nmid N} \big(1 - T_N(p)p^{-s} + T_N(p\,,p)p^{1-2s}\big)^{-1} \times \prod_{p \mid N} \big(1 - T_N(p)p^{-s}\big)^{-1} \,.$$

4.3 Eigenfunctions

Recall that if $f \in \mathcal{S}_{2k}\big(\Gamma_0(N)\,,\chi\big)$, $\alpha \in \Delta_0(N)$ and $\Gamma_0(N)\alpha\Gamma_0(N) = \coprod_v \Gamma_0(N)\alpha_v$, then

$$[\Gamma_0(N)\alpha\Gamma_0(N)] \cdot f(z) = \det(\alpha)^{k-1} \sum_v \overline{\tilde{\chi}}(\alpha_v) f|_{2k}\alpha_v(z) = \frac{\det(\alpha)^k}{(cz+d)^{2k}} f(\alpha \cdot z) \,.$$

If $\gcd(\ell\,,N) = 1$, then

$$T(\ell\,,\ell)f = \ell^{2k-1}\chi(\ell)f \,.$$

Theorem 4.3.1. (1) *Let $f \in \mathcal{S}_{2k}\big(\Gamma_0(N)\,,\chi\big)$. Write $f = \sum_{n\geq 1} c_n e^{2\mathrm{i}\pi nz}$. Suppose that $c_1 = 1$ and that f is an eigenfunction of all the Hecke operators $T(n)$ and $T(\ell\,,\ell)$ for $\gcd(n\,,N) = \gcd(\ell\,,N) = 1$. Then*

$$L(f\,,s) = \sum_{n\geq 1} \frac{c_n}{n^s} = \prod_{p \nmid N} \big(1 - c_p p^{-s} + \chi(p)p^{2k-1-2s}\big)^{-1} \times \prod_{n \mid N^\infty} c_n n^{-s}$$

(2) *There exists a basis of $\mathcal{S}_{2k}\big(\Gamma_0(N)\,,\chi\big)$ of eigenfunctions of the $T(n)\,, T(\ell)$ with $\gcd(n\,,N) = \gcd(\ell\,,N) = 1$.*

(3) *If f is an eigenfunction of all the operators $T(n)$, then $c_1 \neq 0$. If we normalized f by $c_1 = 1$, then we have the Eulerian product*

$$L(f\,,s) = \prod_{p \nmid N} \big(1 - c_p p^{-s} + \chi(p)p^{2k-1-2s}\big)^{-1} \times \prod_{p \mid N^\infty} \big(1 - c_p p^{-s}\big)^{-1} \,.$$

Lemma 4.3.2. *Let $f(z) = \sum_{n\geq 1} c_n e^{2\mathrm{i}\pi nz} \in \mathcal{S}_{2k}\big(\Gamma_0(N)\,,\chi\big)$ and $T_m f(z) = \sum_{n\geq 1} b_n e^{2\mathrm{i}\pi nz}$, then $b_1 = c_m$.*

Proof. If $\gcd(m\,,N)=1$, the proof given for $\mathrm{SL}_2(\mathbb{Z})$ will give

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

In particular, $b_1=c_m$.

Using the fact $T_{mn}=T_mT_n$ for $\gcd(m\,,n)=1$, we just need to study T_{p^e} for $p\,|\,N$. From the decomposition

$$\Gamma_0(N)\left(\begin{smallmatrix}1&0\\0&p^e\end{smallmatrix}\right)\Gamma_0(N)=\coprod_{o\le m<p^e}\Gamma_0(N)\left(\begin{smallmatrix}1&m\\0&p^e\end{smallmatrix}\right)\ ,$$

we get

$$\begin{aligned}T_{p^e}f=&\left[\Gamma_0(N)\left(\begin{smallmatrix}1&0\\0&p^e\end{smallmatrix}\right)\Gamma_0(N)\right]f=p^{e(k-1)}\sum_{m=0}^{p^e-1}\frac{p^{ek}}{p^{2ek}}f\Big(\frac{z+m}{p^e}\Big)\\
=&p^{-e}\sum_{n\ge1}c_n\Big(\sum_{m=0}^{p^e-1}e^{2\mathrm{i}\pi n\frac{z+m}{p^e}}\Big)\\
=&p^{-e}\sum_{n\ge1}c_ne^{2\mathrm{i}\pi nz/p^e}\Big(\sum_{m=0}^{p^e-1}e^{2\mathrm{i}\pi nm/p^e}\Big)\\
=&\sum_{n\ge1}c_{np^e}e^{2\mathrm{i}\pi nz}\end{aligned}$$

which implies immediately $b_1=c_{p6e}$. □

Proof of theorem.4.3.1. If $c_1=1$ and $T_mf=\lambda_mf$, then by the above lemma $\lambda_m=c_m$. As $T(p\,,p)f=\chi(p)p^{2k-2}f$, the relation

$$\sum_{n=1}^{\infty}T_N(n)n^{-s}=\prod_{p\nmid N}\left(1-T_N(p)p^{-s}+T_N(p\,,p)p^{1-2s}\right)^{-1}\cdot\prod_{p\,|\,N}\left(1-T_N(p)p^{-s}\right)^{-1}$$

induces the relation

$$L(f\,,s)=\prod_{p\nmid N}\left(1-T_N(p)p^{-s}+\chi(p)p^{2k-1-2s}\right)^{-1}\cdot$$

$$\begin{cases}\prod_{p\,|\,N}\left(1-T_N(p)p^{-s}\right)^{-1} & \text{if } f \text{ is an eigenfunction of } T(p)\,,p\,|\,N\\ \prod_{n\,|\,N}c_nn^{-s} & \text{if } f \text{ is an eigenfunction of } T(n) \text{ and}\\ & T(p\,,p)\,,\gcd(n\,,N)=\gcd(p\,,N)=1\end{cases}$$

If f is an eigenfunction of all the $T_N(n)$, the for all $n\in\mathbb{N}$, $c_n=\lambda c_1$ where $T_N(n)f=\lambda_nf$. Therefore, if $c_1=0$ then $f=0$. □

Main questions on this topic are concerning the existence of eigenfunctions of all the $T(n)$, or at least that of eigenfunctions of all the $T(n)$, $\gcd(n\,,N)=1$ but with $c_1=1$.

4.4 Primitive Forms

To simplify the exposition, let's work with $\mathcal{S}_{2k}\big(\Gamma_0(N)\big) = \mathcal{S}_{2k}\big(\Gamma_0(N)\,,\mathbb{1}\big)$ where $\mathbb{1}$ is the trivial character.

Lemma 4.4.1. *Let $f\in\mathcal{S}_{2k}\big(\Gamma_0(N)\big)$ and $\ell\in\mathbb{N}^*$. Then*

$$g_\ell(z) := f(\ell z)\in\mathcal{S}_{2k}\big(\Gamma_0(N\ell)\big)\ .$$

Proof. Write $\delta_\ell=\left(\begin{smallmatrix}\ell & 0\\ 0 & 1\end{smallmatrix}\right)$, $g=f|_{2k}\delta_\ell$ so that $g(z)=\ell^k f(\ell z)$. Let $\gamma=\left(\begin{smallmatrix}a & b\\ c\ell N & d\end{smallmatrix}\right)\in\Gamma_0(N\ell)$, then $\gamma_\ell\gamma\gamma_\ell^{-1}\in\Gamma_0(N)$. Thus,

$$g|_{2k}\gamma=(f|_{2k}\delta_\ell)\gamma=(f|_{2k}\delta_\ell\gamma\delta_\ell^{-1})\delta_\ell=f|_{2k}\delta_\ell=g\ .$$

So we have $g\in\mathcal{S}_{2k}\big(\Gamma_0(N\ell)\big)$. □

For all $M\,|\,N$ and all $\ell\,|\,\frac{N}{M}$, we write

$$\Psi_{M,N,\ell}:\mathcal{S}_{2k}\big(\Gamma_0(M)\big)\longrightarrow\mathcal{S}_{2k}\big(\Gamma_0(N)\big)\ ;\quad f(z)\mapsto f(\ell z)\ .$$

where we use the natural injections $\mathcal{S}_{2k}\big(\Gamma_0(m)\big)\subset\mathcal{S}_{2k}\big(\Gamma_0(m')\big)$ if $m\,|\,m'$.

Definition 4.4. Let $\mathcal{S}_{2k}^{\text{old}}\big(\Gamma_0(N)\big)$ be the subvectorspace of $\mathcal{S}_{2k}\big(\Gamma_0(N)\big)$ generated by the $\Psi_{M,N,\ell}\big(\mathcal{S}_{2k}(\Gamma_0(M))\big)$ for all $M\,|\,N$, $M\neq N$ and $\ell\,|\,\frac{N}{M}$. A form in $\mathcal{S}_{2k}^{\text{old}}\big(\Gamma_0(N)\big)$ is called an ***old form***.

Let $\mathcal{S}_{2k}^{\text{new}}\big(\Gamma_0(N)\big)$ be the orthogonal of $\mathcal{S}_{2k}^{\text{old}}\big(\Gamma_0(N)\big)$ for the Petersson's scalar product. A form in $\mathcal{S}_{2k}^{\text{new}}\big(\Gamma_0(N)\big)$ is called a ***new form*** or ***primitive form***.

We write $\mathcal{S}_{2k}(N)=\mathcal{S}_{2k}\big(\Gamma_0(N)\big)$ from here on.

Lemma 4.4.2. *Let $M\,|\,N$, $\ell\,|\,\frac{N}{M}$ and $n\in\mathbb{N}^*$ such that $\gcd(n\,,N)=1$. Then the diagram*

$$\begin{array}{ccc}\mathcal{S}_{2k}\big(\Gamma_0(M)\big) & \xrightarrow{T_M(n)} & \mathcal{S}_{2k}\big(\Gamma_0(M)\big)\\ \Big\downarrow{\scriptstyle\Psi_{M,N,\ell}} & & \Big\downarrow{\scriptstyle\Psi_{M,N,\ell}}\\ \mathcal{S}_{2k}(N) & \xrightarrow{T_N(n)} & \mathcal{S}_{2k}(N)\end{array}$$

is commutative.

Proof. This is clear for the adèlic point of view. To compute $T_N(n)$ or $T_M(n)$, we write these operators as a sum of double cosets which can be decomposed as products of double cosets of the form $\mathrm{GL}_2(\mathbb{Z}_p)\left(\begin{smallmatrix} m' & 0 \\ 0 & m \end{smallmatrix}\right)\mathrm{GL}_2(\mathbb{Z}_p)$ with $\gcd(N\,, pm'm) = 1$ and $m'm = n$, and the right coset decomposition in level M is the same as the decomposition in level N. □

We then get the following immediately.

Lemma 4.4.3. *Let $\mathcal{S}_{2k}^{\mathrm{old}}(N)$ is stable by the Hecke operators $T(n)$ for all n such that $\gcd(n\,, N) = 1$.*

As $T(n)$ is a self-adjoint operator ($T^*(n) = \chi(n)T(n) = T(n)$), we see that $\mathcal{S}_{2k}^{\mathrm{new}}(N)$ is also stable by the Hecke operators $T_N(n)\,, \gcd(n\,, N) = 1$.

We state without proof the following theorem.

Theorem 4.4.4 (Multiplicity One Theorem)**.** *Let $f \in \mathcal{S}_{2k}^{\mathrm{new}}\big(\Gamma_0(N)\big)$ and $g \in \mathcal{S}_{2k}\big(\Gamma_0(N)\big)$ be some eigenfunctions of all the Hecke operators $T_N(n)$ for $\gcd(n\,, N) = 1$. Write $f = \sum_{n\geq 1} a_n(f)q^n\ , g = \sum_{n\geq 1} a_n(g)q^n$. If $\forall\ n$ such that $\gcd(n\,, N) = 1$, $T(n)f = \lambda_n f\ ; T(n)g = \lambda_n g$, then $g = \lambda f$.*

Theorem 4.4.5. *$\mathcal{S}_{2k}^{\mathrm{new}}\big(\Gamma_0(N)\big)$ admits a basis of eigenfunctions for $\mathcal{R}\big(\Gamma_0(N)\,, \Delta_0(N)\big)$ (i.e, for all the Hecke operators).*

Proof. As $\mathcal{S}_{2k}^{\mathrm{new}}\big(\Gamma_0(N)\big)$ is stable by the $T(n)\,, \gcd(n\,, N) = 1$, there exists a basis of $\mathcal{S}_{2k}^{\mathrm{new}}\big(\Gamma_0(N)\big)$ of eigenfunctions of all the $T_N(n)\,, \gcd(n\,, N) = 1$.

Let $f \in \mathcal{S}_{2k}^{\mathrm{new}}\big(\Gamma_0(N)\big)$ be such an eigenfunction and let $T \in \mathcal{R}\big(\Gamma_0(N)\,, \Delta_0(N)\big)$, then $g = Tf \in \mathcal{S}_{2k}\big(\Gamma_0(N)\big)$. For all n such that $\gcd(n\,, N) = 1$,

$$T_n g = T_n T f = T T_n f = \lambda_n T f\ .$$

Therefore, g is an eigenfunction of all the Hecke operators $T(n)\,, \gcd(n\,, N) = 1$ with the same eigenvalues as f. By theorem.4.4.4, $g = c_\Gamma f = Tf$. Therefore, f is an eigenfunction of T. □

Lemma 4.4.6. *The vector space $\mathcal{S}_{2k}^{\mathrm{old}}\big(\Gamma_0(N)\big)$ can be generated by the*

$$\sum_{M\,|\,N\ ,\ M<N}\ \sum_{\ell\,|\,\frac{N}{M}} \Psi_{M,N,\ell}\big(\mathcal{S}_{2k}^{\mathrm{new}}\big(\Gamma_0(M)\big)\big)\ .$$

Proof. Exercise. □

Theorem 4.4.7. *Let $\mathcal{B}_M^{\text{new}}$ be the basis of $\mathcal{S}_{2k}^{\text{new}}\big(\Gamma_0(N)\big)$ of normalized eigenfunction of $\mathcal{R}\big(\Gamma_0(N)\,,\Delta_0(N)\big)$. Then $\mathcal{S}_{2k}\big(\Gamma_0(N)\big)$ admits the basis*

$$\mathcal{B} = \coprod_{\ell\,|\,\frac{N}{M}} \coprod_{f\in\mathcal{B}_M^{\text{new}}} \{\, f(\ell z)\,\}\,.$$

If $f \in \mathcal{B}_N^{\text{new}}$, $f = \sum_{n\geq 1} a_n(f)q^n = \sum_{n\geq 1} a_n q^n$, then

$$L(f\,,s) = \prod_{p\nmid N} \big(1 - a_p p^{-s} + p^{2k-1-2s}\big)^{-1} \prod_{p\,|\,N} \big(1 - a_p p^{-s}\big)^{-1}\,.$$

Remark 4.6. If $f \in \mathcal{B}^{\text{new}_M}$ and $\ell\,|\,\frac{N}{M}$, $f(z) = \sum_{n\geq 1} a_n e^{2\mathrm{i}\pi nz}$, then

$$f(\ell z) = \sum_{n\geq 1} a_n e^{2\mathrm{i}\pi n\ell z} = \sum_{n\geq 1} c_n e^{2\mathrm{i}\pi nz} \quad \text{with} \begin{cases} c_n = 0 & \text{if } \ell\nmid n \\ c_n = a_{n/\ell} & \text{if } \ell\,|\,n \end{cases}$$

In particular, $c_1 = 0$ if $\ell \neq 1$.

Remark 4.7. It's not hard to prove that $L(f\,,s)$ admits analytic continuation and a functional equation relating $L(f\,,2k-s)$ and $L(f\,,s)$.

Chapter 5

Modular Equation for $X_0(N)$

In this chapter, we would like to construct a natural curve C over $\mathbb{Q}$ (defined by an equation $F(X\,,Y)=0$ for some $\mathbb{Q}[X\,,Y]$) such that $C\otimes_{\mathbb{Q}}\mathbb{C}$ is birational equivalent to $X_0(N)_{\mathbb{C}}\cong\Gamma_0(N)\backslash\mathbb{H}^*$.

5.1 The Modular Equation

5.2 The Curve $X_0(N)$ over $\mathbb{Q}$

Chapter 6

Elliptic Curves

6.1 Review of Algebraic Varieties over a Field K

6.1.1 Algebraic Varieties

6.1.2 The Case of Curves

6.1.3 Differential Forms

6.1.4 Local Ring on a Curve

6.1.5 The Riemann-Roch Theorem

6.2 Elliptic Curves

6.2.1 Weierstrass Equations and Singularities

6.2.2 Isogenies

6.3 Elliptic Curves over Finite Fields

6.3.1 Number of Rational Points

6.3.2 Dual Isogeny

6.4 The Weil Conjectures

6.4.1 The Statement

6.4.2 Tate Module and Weil Paring

6.4.3 Construction of Weil Paring

6.5 Elliptic Curves over Local Fields

Chapter 7

Eichler–Shimura's Theorem and L-functions

7.1 Eichler–Shimura's Theorem

7.2 L-functions of Elliptic Curves and Modular Forms

Appendix A

Final Exam (3 Hours)

Problem 1.

(I-1) Let p be a prime number. Show that the matrices $\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0 & 1\\ -1 & j\end{smallmatrix}\right)$ for j such that $1 \leq j \leq p$ is a system of representatives of $\Gamma_0(p)\backslash\Gamma_0(1)$.

(I-2) Compute the number μ_∞ of cusps of $X_0(p)$ and the ramification indexes of the canonical morphism $X_0(p) \to X_0(1)$ at these cusps.

We recall that the elliptic points of $X_0(1)$ are the images of i and $\rho = \frac{1+i\sqrt{3}}{2}$ in $X_0(1)$ and that

$$\mathrm{Fix}_{\mathrm{SL}_2(\mathbb{Z})}(i) = \pm\langle\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\rangle \quad \text{and} \quad \mathrm{Fix}_{\mathrm{SL}_2(\mathbb{Z})}(\rho) = \pm\langle\begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}\rangle$$

(I-3) Prove that the set of elliptic points of order 2 of $\Gamma_0(p)$ is in bijection with the set of solutions in $\mathbb{Z}/p\mathbb{Z}$ of the equation $X^2 = -1$. Prove that the set of elliptic points of order 3 of $\Gamma_0(p)$ is in bijection with the set of solutions in $\mathbb{Z}/p\mathbb{Z}$ of the equation $X^2 + X + 1 = 0$.

Let μ_i be the number of elliptic points of order i of $\Gamma_0(p)$. For an integer a prime to p we write $\left(\frac{a}{p}\right)$ the integer 1 (resp. -1) if a is (resp. is not) a square modulo p . Show that $\mu_2 = 1 + \left(\frac{-1}{p}\right)$, $\mu_3 = 1 + \left(\frac{-3}{p}\right)$ if $p \neq 3$ and compute μ_3 for $p = 3$.

(I-4) Give the formula for the genus g_p of $X_0(p)$ and determine the set of prime numbers p such that $g_p = 0$.

(II) Let f be a function on the upper half plane $\mathbb{H}$ and $\gamma = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})^+$. For all integer k we define the function $f|_k\gamma(z)$ on $\mathbb{H}$ by the formula

$$f|_k\gamma(z) := \frac{\det(\gamma)^k}{(cz+d)^{2k}} f(\gamma \cdot z) \ .$$

Let A be a ring $F = \sum_{n\geq 0} a_n q^n$ a formal series with coefficients in A . Let $F|_U$ be the formal series

$$F|_U = \sum_{n\geq 0} a_{pn} q^n \ .$$

(II-1) Show that for all $\gamma\,,\gamma'$ in $\mathrm{GL}_2(\mathbb{R})^+$, $(f|_k\gamma)\gamma' = f|_k\gamma\gamma'$.

We suppose from now that f is a weight $2k$ cuspidal modular form for $\Gamma_0(p)$.

(II-2) Let W be the matrix $W = \left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)$. Show that $f|_k W \in \mathcal{M}_{2k}\big(\Gamma_0(p)\big)$.

(II-3) Let $\gamma_1\,,\cdots,\gamma_{p+1}$ be a system of representatives of $\Gamma_0(p)\backslash \mathrm{SL}_2(\mathbb{Z})$ and $f \in \mathcal{M}_{2k}\big(\Gamma_0(p)\big)$. Show that the function

$$\mathrm{Tr}(f) = \sum_{j=1}^{p+1} f|_k\gamma_j$$

is independent of choice of the γ_i and is a weight $2k$ modular form for $\mathrm{SL}_2(\mathbb{Z})$.

(II-4) Let $f = \sum_{n\geq 0} a_n q^n$ and $f|_k W = \sum_{n\geq 0} b_n q^n$ be the Fourier expansions of f and $f|kW$. Show that

$$\mathrm{Tr}(f) = \sum a_n q^n + p^{1-k} \sum b_{pn} q^n = f + p^{1-k}(f|_k W)|_U \ .$$

(II-5) Show that $\mathrm{Tr}(f|_k W) = f|_k W + p^{1-k} f|_U$ and that $f|_U \in \mathcal{M}_{2k}\big(\Gamma_0(p)\big)$.

(II-6) We suppose in this question that $f \in \mathcal{M}_{2k}\big(\Gamma_0(1)\big) \subset \mathcal{M}_{2k}\big(\Gamma_0(p)\big)$. Show that

$$\mathrm{Tr}(f|_k W) = p^{1-k} T_p f \ .$$

(II-7) We assume that $k = 1$. Show that $f|_k W = -f|_U$. We write $T_p.f = f|_U$. Show that for all n not divisible by p and all $f \in \mathcal{M}_{2k}\big(\Gamma_0(p)\big)$, $T_n T_p.f = T_p T_n.f$ and $T_p^2.f = f$. Deduce from this that $\mathcal{M}_{2k}\big(\Gamma_0(p)\big)$ has a basis of eigenforms for T_p and the Hecke operators T_n with n prime to p .

(II-8) Let $\{\lambda_n\}$ be a set of complex numbers indexed by the set of integers n prime to p. Show that the space of weight 2 modular forms for $\Gamma_0(p)$ which are eigenforms for all the T_n with n prime to p with assoicated eigenvalues λ_n is of dimension at most 1. Let $f = \sum_{n\geq 1} a_n q^n$ be such a non zero cuspidal form. Show that $a_1 \neq 0$. We suppose that $a_1 = 1$, show that $a_p = \pm 1$ and that for all $n \in \mathbb{N}$, $a_{pn} = a_p a_n$. Show that the L-function $L(f\,,s) = \sum_{n\geq 1} \frac{a_n}{n^s}$ has an Eulerian product and give an explicit form of this product.

Problem 2.

(0) Recall the definition of a supersingular elliptic curve defined over a field of characteristic $p > 0$. Show that up to isomorphism there are at most finitely many such curves over the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$.

If X is a finite set, the cardinality of X is written as $|X|$. Let $K = \mathbb{F}_q$ be a finite field of characteristic $p > 3$ and

$$\chi \ : \ K^* \longrightarrow \{ \pm 1 \}$$

the unique non trivial character of K^* of order 2. We define $\chi(0)$ by $\chi(0) = 0$. Let E be an elliptic curve over K given by a Weierstrass equation of the form

$$y^2 = x^3 + ax^2 + bx + c = f(x)$$

for a polynomial $f(x)$ without multiple roots.

(1) Show that

$$|E(\mathbb{F}_q)| = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$$

and deduce that

$$\Big| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \Big| \leq 2\sqrt{q} \ .$$

(2) Compute for all $k \in \mathbb{N}$ the sum $\sum_{x \in \mathbb{F}_q} x^k$.

(3) Let A_q be the coefficient of x^{q-1} in $f(x)^{\frac{q-1}{2}}$. Show the following equality between elements of the field $\mathbb{F}_q$:

$$\big|E(\mathbb{F}_q)\big| = 1 - A_q \ .$$

(4) Let ϕ_q be the Frobenius endomorphism of E. Show that

$$\big|E(\mathbb{F}_q)\big| = 1 + q - a \quad \text{with} \quad a = 1 - \deg(1 - \phi_q) + \deg(\phi_q) \ .$$

(5) Show that E is supersingular if and only if $A_q = 0$.

(6) Let A_p be the coefficient of x^{p-1} in $f(x)^{\frac{p-1}{2}}$. Show that E is supersingular if and only if $A_p = 0$.

(7) Let $E_{\mathbb{Q}}$ be the elliptic curve over $\mathbb{Q}$ with equation $y^2 = x^3 + x$. Determine the set of prime numbers $p \geq 5$ such that $E_{\mathbb{Q}}$ has good supersingular reduction.

The End.

Index