Part III - Modular Forms

Lectured by Jack Thorne

Artur Avameri

Michaelmas 2023

Contents

1 Introduction

06 Oct 2022, Lecture 1

Definition 1.1. We define the following groups:

$$\begin{aligned}
\mathfrak{h} &= \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\} \\
GL_2(\mathbb{R})^+ &= \{g \in GL_2(\mathbb{R}) \mid \det(g) > 0\} \\
\Gamma(1) = SL_2(\mathbb{Z}) &= \{g \in M_2(\mathbb{Z}) \mid \det(g) = 1\}.
\end{aligned}$$

Note that $\Gamma(1)$ is a subgroup of $GL_2(\mathbb{R})^+$.

Lemma 1.1. $GL_2(\mathbb{R})^+$ acts transitively on $\mathfrak{h}$ by Möbius transformations.

Proof. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})^+, \tau \in \mathfrak{h}$. Then

$$\mathrm{Im}(g\tau) = \frac{1}{2i}\left(\frac{a\tau + b}{c\tau + d} - \frac{a\overline{\tau} + b}{c\overline{\tau} + d}\right) = \frac{1}{2i}\frac{(ad - bc)(\tau - \overline{\tau})}{|c\tau + d|^2} = \frac{\det(g)\mathrm{Im}(\tau)}{|c\tau + d|^2} > 0,$$

so $g\tau \in \mathfrak{h}$. This action is transitive since

$$x + iy \in \mathfrak{h} \implies \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} i = x + iy,$$

so everything in $\mathfrak{h}$ is conjugate to i. $\square$

Definition 1.2. If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})^+$ and $\tau \in \mathfrak{h}$, then define

$$j(g, \tau) = c\tau + d.$$

This is called a **modular cocycle**. If $k \in \mathbb{Z}$ and $f : \mathfrak{h} \to \mathbb{C}$, then

$$f|_k[g] : \mathfrak{h} \to \mathbb{C}$$

is defined by

$$f|_k[g](\tau) = \det(g)^{k-1} f(g\tau) j(g, \tau)^{-k}.$$

This is the **weight k action of g on f**.

Lemma 1.2. This is a right action of $GL_2(\mathbb{R})^+$: if $g, h \in GL_2(\mathbb{R})^+$, then

$$f|_k[gh] = (f|_k[g])|_k[h].$$

Proof. We compute

$$\begin{aligned}(f|_k[g])|_k[h](\tau) = \det(h)^{k-1} f|_k[g](h\tau) j(h,\tau)^{-k} = \\ \det(h)^{k-1}\det(g)^{k-1} f(gh\tau) j(g,h\tau)^{-k} j(h,\tau)^{-k} \stackrel{?}{=} \\ \det(gh)^{k-1} f(gh\tau) j(gh,\tau)^{-k} = f|_k[gh](\tau).\end{aligned}$$

Hence we need to check that $j(gh,\tau) = j(gh,\tau)j(h,\tau)$. Note that if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then

$$g\begin{pmatrix}\tau \\ 1\end{pmatrix} = \begin{pmatrix} a\tau+b \\ c\tau+d\end{pmatrix} = j(g,\tau)\begin{pmatrix} g\tau \\ 1\end{pmatrix}.$$

We now get

$$j(gh,\tau)\begin{pmatrix} gh\tau \\ 1\end{pmatrix} = gh\begin{pmatrix}\tau \\ 1\end{pmatrix} = g\left(j(h,\tau)\begin{pmatrix} h\tau \\ 1\end{pmatrix}\right) = j(h,\tau)j(g,h\tau)\begin{pmatrix} gh\tau \\ 1\end{pmatrix},$$

which finishes the computation and proof. □

Formulae. For $g \in GL_2(\mathbb{R})^+, \tau \in \mathfrak{h}$, we have

$$\mathrm{Im}(g\tau) = \det(g)\frac{\mathrm{Im}(\tau)}{|j(g,\tau)|^2} \text{ and } j(g,\tau)\begin{pmatrix} g\tau \\ 1\end{pmatrix} = g\begin{pmatrix}\tau \\ 1\end{pmatrix}.$$

Definition 1.3. Let $k \in \mathbb{Z}$ and $\Gamma \leq \Gamma(1)$ of finite index[1]. A **weakly modular function of weight** k **and level** Γ is a meromorphic function $f : \mathfrak{h} \to \mathbb{C}$ which is invariant under the weight k action of Γ, i.e. such that

$$\forall \tau \in \mathfrak{h}, \forall \gamma \in \Gamma, f|_k(\gamma) = f.$$

We will define modular forms next time: they are weakly modular functions which are holomorphic both in $\mathfrak{h}$ and at ∞.

It is a fact that modular forms of fixed weight and level live in finite-dimensional $\mathbb{C}$-vector spaces called $M_k(\Gamma)$. These form the main objects of study in this course.

Motivation. Why study modular forms?

(1) They are related to the theory of elliptic functions. Let $E/\mathbb{C}$ be an elliptic curve and ω a holomorphic non–zero 1–form. Then there exists a unique lattice[2] $\Lambda \in \mathbb{C}$ and isomorphism $\phi : \mathbb{C}/\Lambda \to E$ such that $\phi^*(\omega) = dz$. Then

[1] In other words, Γ is a (finite index) subgroup of $\Gamma(1)$.
[2] i.e. a discrete cocompact subgroup, or an abelian subgroup which is freely generated by two elements that are linearly independent over $\mathbb{R}$.

E is isomorphic to the elliptic curve $y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$ where if $k \in \mathbb{Z}$, then $G_k(\Lambda) = \sum_{\lambda \in \Lambda - \{0\}} \lambda^{-k}$. This converges absolutely for $k > 2$.

If $\tau \in \mathfrak{h}$, then $\Lambda\tau = \mathbb{Z}\tau \oplus \mathbb{Z} \subset \mathbb{C}$ is a lattice and $G_k(\tau) = G_k(\Lambda_\tau)$. This is a modular form of weight k and level $\Gamma(1)$, called an Eisenstein series.

$\mathfrak{h}/SL_2(\mathbb{Z})$ can be identified with the set of (isomorphism classes of) elliptic curves over $\mathbb{C}$.

(2) Modular forms f have Fourier expansions $\sum_{n\in\mathbb{Z}} a_n g^n$, $a_n \in \mathbb{C}$ and they often serve as a generating functions for arithmetically interesting sequences a_n.

For example, take $\theta(\tau) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 \tau}$. If $k \in 2\mathbb{N}$, then θ^k is a modular form with q–expansion $\theta^k = \sum_{n\in\mathbb{Z}} r_k(n) e^{\pi i n \tau}$, where $r_k(n)$ is the number of ways of writing n as a sum of k squares, i.e. $r_k(n) = |\{x \in \mathbb{Z}^k \mid \sum_{i=1}^k x_i^2 = n\}|$. By expressing θ^k in terms of other modular forms, we can prove formulae such as $r_4(n) = 8\sum_{d|n, 4\nmid d} d$.

(3) The Riemann zeta function $\zeta(s)$ is an important object of study. Its pleasant features include:

- The Euler product $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$.
- It has a meromorphic continuation to $\mathbb{C}$ and has a functional equation relating $\zeta(s)$ and $\zeta(1-s)$.

A Dirichlet series $\sum_{n\geq 1} a_n n^{-s}$ which has similar properties (Euler product, meromorphic extension, some nice function equation) is called an L–function. Modular forms can be used to construct interesting examples of L–functions. In practice, we take $M_k(\Gamma)$ and decompose it under Hecke operators to get Hecke eigenforms, the nicest possible modular forms, which have the above properties.

(4) The Langlands program predicts a relation between modular forms and objects in arithmetic geometry. A special case of this is the modularity conjecture, which says that there is a bijective correspondence between elliptic curves $E/\mathbb{C}$ up to isogeny and the set of Hecke eigenforms of weight 2. This implies Fermat's last theorem. Note that this is formulated in the language of Hecke operators and L–functions.

Homework. There is a handout on Moodle called "Reminder on Complex Analysis". Have a look at it before the next lecture.

2 Modular Forms on $\Gamma(1)$

09 Oct 2022, Lecture 2

Reminder. A **meromorphic** function in an open subset $U \subset \mathbb{C}$ is a closed subset $A \subset U$ and a holomorphic function $f : U \setminus A \to \mathbb{C}$ such that $\forall a \in A$, $\exists \delta > 0$ such that $D^*(a, \delta) \subset U \setminus A$ and $\exists n \geq 0$ such that $(z-a)^n f(z)$ extends to a holomorphic function in $D(a, \delta)$.

f then has a Laurent expansion $\sum_{m \in \mathbb{Z}} a_m (z-a)^m$ valid on $D^*(a, \delta)$.

Lemma 2.1. Let f be a weakly modular function of weight k and level $\Gamma(1)$. Then there exists a meromorphic function $\tilde{f}$ in $D^*(0,1)$ (the "q-disk") such that

$$f(\tau) = \tilde{f}(e^{2\pi i \tau}).$$

Proof. f is meromorphic in $\mathfrak{h}$ by assumption. Take $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma(1)$. Then $f|_h[\gamma](\tau) = f(\gamma\tau) = f(\tau)$, as f is invariant under the weight k action of γ. But also $f(\gamma\tau) = f(\tau + 1)$, so f is periodic.

Now map a strip of $\mathfrak{h}$ of width 1 to $D^*(0,1)$ by $\tau \mapsto e^{2\pi i \tau}$. Let $a \in D^*(0,1)$ and $\delta > 0$ be such that $D(a, \delta) \subset D^*(0,1)$. Define $\tilde{f}$ on $D(a, \delta)$ by

$$\tilde{f}(q) = f\left(\frac{1}{2\pi i} \log q\right),$$

for any branch of log defined in $D(a, \delta)$. This is meromorphic and independent of the choice of the branch of log, as f is periodic with period 1. This defines $\tilde{f}$ in $D^*(0,1)$. Finally, $\tilde{f}$ is unique since $\tau \mapsto e^{2\pi i \tau}$ is surjective. $\square$

If $\tilde{f}$ extends to a meromorphic function[3] in $D(0,1)$, then $\exists \delta > 0$ such that $\tilde{f}$ has a Laurent expansion $\tilde{f}(q) = \sum_{n \in \mathbb{Z}} a_n q^n$ valid in $D^*(0, \delta)$.

In the region $\{\tau \in \mathfrak{h} \mid \mathrm{Im}(\tau) > \frac{1}{2\pi} \log \delta\}$, we have

$$f(\tau) = \sum_{n \in \mathbb{Z}} a_n q^n,$$

where $q = e^{2\pi i \tau}$. This is called the q–**expansion** of the weakly modular function f.

Definition 2.1. Let f be a weakly modular function of weight k and level $\Gamma(1)$. We say that f is **meromorphic at** ∞ if $\tilde{f}$ extends to a meromorphic function in $D(0,1)$.

We say f is **holomorphic at** ∞ if $\tilde{f}$ is meromorphic at ∞ and has a

[3] This might not be the case if the set of poles has a limit inside the disk.

removable singularity at $q = 0$. In this case, we define

$$f(\infty) = \tilde{f}(0) = \lim_{\mathrm{Im}(\tau)\to\infty} f(\tau).$$

We say f **vanishes at** ∞ if f is holomorphic at ∞ and $f(\infty) = 0$.

Definition 2.2. A **modular function** (of weight k and level $\Gamma(1)$) is a weakly modular function (of weight k and level $\Gamma(1)$) which is meromorphic at ∞.

A **modular form** is a weakly modular function which is holomorphic in $\mathfrak{h}$ and holomorphic at ∞.

A **cuspidal modular form** is a modular form that vanishes at ∞.

Remark. We let $M_k(\Gamma(1))$ denote the set of modular forms of weight k and level $\Gamma(1)$. We write $S_k(\Gamma(1))$ for the set of cuspidal modular forms of weight k, level $\Gamma(1)$. Note $S_k(\Gamma(1)) \subset M_k(\Gamma(1))$. These are $\mathbb{C}$–vector spaces. If k is odd, then these both only contain the zero function, since taking $\gamma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \Gamma(1)$ gives $f|_k[\gamma](\tau) = f(\tau)(-1)^k = f(\tau)$.

We now consider even weights only. If $k \in \mathbb{Z}$ is even, let

$$G_k(\tau) = \sum_{\lambda\in\Lambda_\tau\setminus 0} \lambda^{-k} = \sum_{(m,n)\in\mathbb{Z}^2\setminus 0} (m\tau + n)^{-k},$$

where $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$ for any $\tau \in \mathfrak{h}$.

If $\gamma \in \Gamma(1)$, then formally we have

$$G_k|_k[\gamma](\tau) = G_k(\gamma\tau)j(\gamma, \tau)^{-k} = \sum_{\lambda\in\Lambda_{\gamma\tau}\setminus 0} \lambda^{-k} j(\gamma, \tau)^{-k},$$

but $\Lambda_{\gamma\tau} = \mathbb{Z}\frac{a\tau+b}{c\tau+d} \oplus \mathbb{Z} = (c\tau + d)^{-1} (\mathbb{Z}(a\tau + b) \oplus \mathbb{Z}(c\tau + d)) = (c\tau + d)^{-1}\Lambda_\tau$. Hence

$$\begin{aligned} G_k|_k[g](\tau) &= \sum_{\lambda\in(c\tau+d)^{-1}\Lambda_\tau\setminus 0} \lambda^{-k}(c\tau + d)^{-k} \\ &= \sum_{\lambda\in\Lambda_\tau\setminus 0} ((c\tau + d)^{-1}\lambda)^{-k}(c\tau + d)^{-k} = G_k(\tau). \end{aligned}$$

This is justified only when the series defining $G_k(\tau)$ converges absolutely. Hence:

Proposition 2.2. Let $k > 2$ be an even integer. Then $G_k(\tau)$ converges absolutely and defines a modular form of weight k and level $\Gamma(1)$ which has

$G_k(\infty) = 2\zeta(k)$. G_k is the **weight k Eisenstein series**.

We will later see that $M_2(\Gamma(1)) = 0$.

Proof. We want to show absolute and locally uniform convergence in $\mathfrak{h}$. This will show that G_k is holomorphic by complex analysis. Let $A \geq 2$ and define $\Omega_A = \{\tau \in \mathfrak{h} \mid \mathrm{Im}(\tau) \geq \frac{1}{A}, \mathrm{Re}(\tau) \in [-A, A]\}$. We show uniform convergence in Ω_A. If $\tau \in \Omega_A, x \in \mathbb{R}$, then $|\tau + x| \geq \begin{cases} \frac{1}{A} & |x| \leq 2A \\ \frac{|x|}{2} & |x| \geq 2A. \end{cases}$ Hence

$$|\tau + x| \overset{(\dagger)}{\geq} \sup\left(\frac{1}{A}, \frac{|x|}{2A^2}\right) \geq \sup\left(\frac{1}{2A^2}, \frac{|x|}{2A^2}\right) = \frac{1}{2A^2}\sup(1, |x|).$$

($\dagger$) follows by drawing a diagram with the lines $y = \frac{1}{A}$ and $y = \frac{x}{2A^2}$ and marking the point $(2A, \frac{1}{A})$ on it, then noticing that out supremum always lies above the supremum of these two lines. If $(m, n) \in \mathbb{Z}^2, m \neq 0$, then

$$|m\tau + n| = |m|\left|\tau + \frac{n}{m}\right| \geq |m|\frac{1}{2A^2}\sup\left(1, \left|\frac{n}{m}\right|\right) = \frac{1}{2A^2}\sup\left(|m|, |n|\right).$$

This is also valid when $m = 0$ by inspection. If $\tau \in \Omega_A$, then

$$\begin{aligned}
&\sum_{(m,n)\in\mathbb{Z}^2\setminus 0} |m\tau + n|^{-k} \\
&\leq \left(\frac{1}{2A^2}\right)^{-k} \sum_{(m,n)\in\mathbb{Z}^2\setminus 0} \sup\left(|m|, |n|\right)^{-k} \\
&= (2A^2)^k \sum_{d\in\mathbb{N}} d^{-k} \cdot \left|\{(m,n) \in \mathbb{Z}^2 \mid \sup\left(|m|, |n|\right) = d\}\right| \\
&= (2A^2)^k \sum_{d\in\mathbb{N}} d^{-k} 8d = 8(2A^2)^k \sum_{d\in\mathbb{N}} d^{1-k} \\
&< \infty
\end{aligned}$$

whenever $k - 1 > 1$, i.e. $k > 2$. This shows absolute convergence, and uniform convergence in Ω_A by the Weierstrass M-test[4]. Hence G_k is holomorphic in $\mathfrak{h}$ and invariant under the weight k action of $\Gamma(1)$. It remains to show that G_k is holomorphic at ∞ with $G_k(\infty) = 2\zeta(k)$. For this, it suffices to check that

$$\lim_{\mathrm{Im}(\tau)\to\infty} G_k(\tau) = 2\zeta(k).$$

[4] If we have a sequence of functions $f_n : \Omega \to \mathbb{C}$ and values $M_n > 0$ with $|f_n(x)| < M_n$ and $\sum M_n < \infty$, then $\sum f_n$ converges absolutely and uniformly on Ω. Here, replace n with d and sum d over $\sum_{(m,n)\in\mathbb{Z}^2\setminus 0, \sup(|m|,|n|)=d} |m\tau + n|^{-k}$.

This follows from uniform convergence in Ω_A: we get

$$\lim_{\mathrm{Im}(\tau)\to\infty} G_k(\tau) = \sum_{(m,n)\in\mathbb{Z}^2\setminus 0} \lim_{\mathrm{Im}(\tau)\to\infty} (m\tau+n)^{-k} = \sum_{n\in\mathbb{Z}\setminus 0} n^{-k} = 2\sum_{n\geq 1} n^{-k} = 2\zeta(k).$$

$\square$

11 Oct 2022, Lecture 3

Recap. We defined what it means for a function $f : \mathfrak{h} \to \mathbb{C}$ to be a modular form of weight k and level $\Gamma(1)$. $M_k(\Gamma(1))$ is the $\mathbb{C}$–vector space of such forms. If $f \in M_k(\Gamma(1))$, then there exists a holomorphic $\tilde{f} : D(0,1) \to \mathbb{C}$ (here we call $D(0,1)$ the q–disk) such that $\forall \tau \in \mathfrak{h}$, $f(\tau) = \tilde{f}(e^{2\pi i\tau})$. The Taylor expansion of $\tilde{f}$ gives the q–expansion

$$f(\tau) = \sum_{n\geq 0} a_n q^n, \ q = e^{2\pi i\tau}.$$

We have $f(\infty) = \tilde{f}(0) = a_0$. If $k > 2$ is even, then $G_k(\tau) = \sum_{\lambda\in\Lambda_\tau\setminus 0} \lambda^{-k}$ converges absolutely and defines an element of $M_k(\Gamma(1))$ with $G_k(\infty) = 2\zeta(k)$.

We define

$$E_k(\tau) = \frac{G_k(\tau)}{2\zeta(k)} = 1 + \sum_{n\geq 1} a_n q^n.$$

We will soon show that we have $a_n \in \mathbb{Q}\ \forall n \geq 1$.

We can construct more modular forms: if $f \in M_k(\Gamma(1))$ and $g \in M_l(\Gamma(1))$, then $fg \in M_{k+l}(\Gamma(1))$. To check this is a modular form, we need to check that:

- fg is holomorphic, which is true as f, g are holomorphic.
- fg is invariant under the weight $k + l$ action of $\Gamma(1)$, which is true as f, g are invariant under the weight k and l actions of $\Gamma(1)$ – this is just a computation.
- fg is holomorphic at ∞. This is true as the q–expansions multiply, so since f, g have no negative terms, the same is true for fg.

Hence we get e.g. $E_4^3, E_6^2 \in M_{12}(\Gamma(1))$ and $\frac{E_4^3 - E_6^2}{1728} \in S_{12}(\Gamma(1))$ (i.e. it is cuspidal since zero at infinity). This difference is Ramanujan's Δ–function. We will show it is nonzero later.

We now want to show that $M_k(\Gamma(1))$ is finite–dimensional. We first study $\Gamma(1)/\mathfrak{h}$. For this, introduce a fundamental set $\mathfrak{f}' \subset \mathfrak{h}$ for the $\Gamma(1)$–action. We define[5] a fundamental set to be a set that intersects each $\Gamma(1)$–orbit in exactly

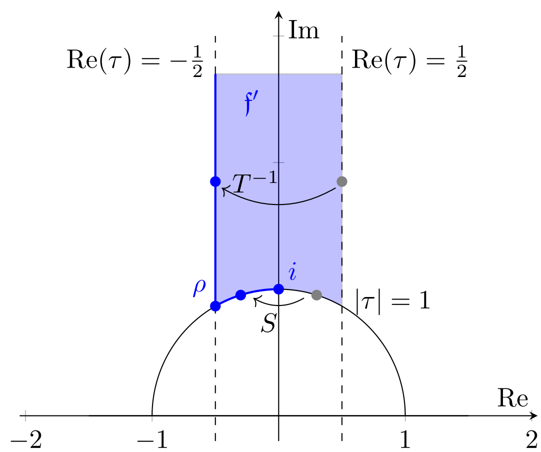
[5] Definitions in literature may vary, so we omit a formal definition.

one element. Define

$$\mathfrak{f} = \left\{ \tau \in \mathfrak{h} \mid \mathrm{Re}(\tau) \in \left[-\frac{1}{2}, \frac{1}{2}\right], |\tau| \geq 1 \right\}.$$

$$\mathfrak{f}' = \left\{ \tau \in \mathfrak{f} \mid \mathrm{Re}(\tau) \in \left[-\frac{1}{2}, \frac{1}{2}\right), |\tau| = 1 \implies \mathrm{Re}(\tau) \in \left[-\frac{1}{2}, 0\right] \right\}.$$

Introduce $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in $\Gamma(1)$. We observe that every element of $\mathfrak{f}$ is conjugate under S or T^{-1} to an element of $\mathfrak{f}'$, which is true since $T(\tau) = \tau + 1$ and $S(\tau) = -\frac{1}{\tau}$.



Proposition 2.3. Let $G = \Gamma(1)/\{\pm I\}$. Then

(i) $\forall \tau \in \mathfrak{h}, \tau$ is $\Gamma(1)$–conjugate to an element of $\mathfrak{f}'$.

(ii) If $\tau, \tau' \in \mathfrak{f}'$ are $\Gamma(1)$–conjugate, then $\tau = \tau'$.

(iii) If $\tau \in \mathfrak{f}'$, then $\mathrm{Stab}_G(\tau)$ is trivial, except in the two cases $\mathrm{Stab}_G(i) = \langle S \rangle$ and $\mathrm{Stab}_G(\rho) = \langle ST \rangle$, where $\rho = e^{2\pi i/3}$.

(iv) $\Gamma(1)$ is generated by S and T.

Proof. Let H be the subgroup of G generated by S and T.

Claim. Every $\tau \in \mathfrak{h}$ is H–conjugate to an element of $\mathfrak{f}'$.

Proof. By our above observation and since $S, T \in H$, it suffices to prove that every $\tau \in \mathfrak{h}$ is H–conjugate to $\mathfrak{f}$. Take $\tau \in \mathfrak{h}$. Recall that if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, then $\mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2}$.

In particular, $\forall R \geq 0$, the intersection $H\tau \cap \{\mathrm{Im}(\tau') > R\}$ is finite, since $\mathrm{Im}(\gamma\tau) > R \iff |c\tau + d|^2 < \frac{\mathrm{Im}(\tau)}{R}$, but $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$ is a lattice, so the set $\{(c,d) \in \mathbb{Z}^2 \mid |c\tau + d| < R'\}$ is finite.

So there exists $h \in H$ such that $\mathrm{Im}(h\tau) \geq \mathrm{Im}(h'\tau)\ \forall h' \in H$. After replacing τ by $h\tau$, we can assume $\mathrm{Im}(\tau) \geq \mathrm{Im}(h\tau)\ \forall h \in H$. Since acting by T does not change $\mathrm{Im}(\tau)$, we can also assume $\mathrm{Re}(\tau) \in \left[-\frac{1}{2}, \frac{1}{2}\right]$. We have $\mathrm{Im}(\tau) \geq \mathrm{Im}(S\tau) = \frac{\mathrm{Im}(\tau)}{|\tau|^2} \implies |\tau| \geq 1$, proving the claim and (i). $\square$

Now take $\tau, \tau' \in \mathfrak{f}'$ and suppose $\gamma\tau = \tau'$ for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$. We want to show that either $\gamma = \pm I$ or $\tau = i, \rho$.

WLOG assume $\mathrm{Im}(\tau') = \mathrm{Im}(\gamma\tau) \geq \mathrm{Im}(\tau)$, i.e. $\mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2} \geq \mathrm{Im}(\tau)$, so $|c\tau + d| \leq 1$. However, if $\tau \in \mathfrak{f}'$, then $\mathrm{Im}(\tau) \geq \frac{\sqrt{3}}{2}$ with equality if and only if $\tau = \rho$. Hence $|c\tau + d| \geq |c|\mathrm{Im}(\tau) \geq |c|\frac{\sqrt{3}}{2} \implies |c| \leq \frac{2}{\sqrt{3}} \implies |c| = 0, 1 \implies c = 0$ or $c = \pm 1$.

- If $c = 0$, then $\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, so $ad = 1 \implies a = d = \pm 1$, so $\gamma = \pm T^m$ for $m \in \mathbb{Z}$. However, T acts on $\mathfrak{f}'$ by shifting the real part, so it can only stay in $\mathfrak{f}'$ if $m = 0$ (as $\mathrm{Re}(\mathfrak{f}') \in \left[-\frac{1}{2}, \frac{1}{2}\right)$), so $\gamma = \pm I$ and $\tau' = \tau$.

- If $c = 1$, then $\gamma = \begin{pmatrix} a & b \\ 1 & d \end{pmatrix}$ and $|\tau + d| \leq 1$. By drawing another picture, we see that the only circles centered at integers of radius 1 which intersect $\mathfrak{f}'$ are centered at $-d = 0, -d = -1$. Hence either $d = 0$, whence $|\tau| = 1$, or $d = 1$, whence $\tau = \rho$.

  - If $c = 1, d = 0, |\tau| = 1$, then $\gamma = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$ since the determinant must be 1. Then $\gamma\tau = \frac{a\tau - 1}{\tau} = a - \frac{1}{\tau} = a - \overline{\tau}$, so $\mathrm{Re}(\gamma\tau) = a - \mathrm{Re}(\tau) \in \mathrm{Re}(\mathfrak{f}' \cap \{|\tau| = 1\}) = \left[-\frac{1}{2}, 0\right]$. However, we also have $\mathrm{Re}(\gamma\tau) \in a - \left[-\frac{1}{2}, 0\right] = a + \left[0, \frac{1}{2}\right]$.

    The intersection $\left[-\frac{1}{2}, 0\right] \cap \left(a + \left[0, \frac{1}{2}\right]\right)$ can be nonempty only if either $a = 0$, whence $\mathrm{Re}(\gamma\tau) = \mathrm{Re}(\tau) = 0$, so $\tau = \gamma\tau = i$, or $a = -1$, whence $\mathrm{Re}(\tau) = \mathrm{Re}(\gamma\tau) = -\frac{1}{2}$, so $\tau = \gamma\tau = \rho$.

    If $a = 0$, then $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -S$, which stabilizes i, and $\langle -S \rangle = \langle S \rangle$.

    If $a = -1$, then $\gamma = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = (ST)^2$, which stabilizes ρ, and $(ST)^3 = I$, so $\langle (ST)^2 \rangle = \langle ST \rangle$.

  - If $c = 1, d = 1, \tau = \rho$, then $\gamma = \begin{pmatrix} a & b \\ 1 & 1 \end{pmatrix}$, so $\rho = \gamma\rho = \frac{a\rho+b}{\rho+1}$. We have $\rho^2 + \rho + 1 = 0$, so $\rho^2 + \rho = -1$, so $a\rho + b = \rho^2 + \rho = -1$. But $a, b \in \mathbb{Z}$ and $1, \rho$ are linearly independent over $\mathbb{R}$, so $a = 0, b = -1$, so $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = -ST$, which stabilizes ρ.

- If $c = -1$, we can reduce this to the case $c = 1$ by replacing γ with $-\gamma$.

We have now shown the first three parts of the proposition. It remains to show the last part, i.e. $\Gamma(1) = \langle S, T \rangle$. Since $S^2 = -I$, it is enough to show that $H = G$. Choose $\tau \in \mathrm{Int}(f)$, so $\mathrm{Stab}_G(\tau) = \{I\}$. Let $g \in G$. By our claim proving (i), $\exists h \in H$ such that $hg\tau \in \mathfrak{f}'$. We must therefore have $hg\tau = \tau$, hence $hg \in \mathrm{Stab}_G(\tau) = \{I\}$, so $g = h^{-1} \in H$. $\square$

13 Oct 2022, Lecture 4

Notation. We write $e_\tau = |\mathrm{Stab}_G(\tau)|$.

Let f be a nonzero modular function of weight k, level $\Gamma(1)$. If $\tau \in \mathfrak{h}$, then $v_\tau(f)$ is the order of f at τ (the unique $n \in \mathbb{Z}$ such that $f(z) = (z-\tau)^n g(z)$ for some meromorphic g that is holomorphic and non–vanishing at τ). We define $v_\infty(f)$ to be the order of f at infinity, i.e. $v_\infty(f) = v_0(\tilde{f})$ for $\tilde{f}$ the meromorphic function in $D(0,1)$ with $f(\tau) = \tilde{f}(e^{2\pi i\tau})$.

Proposition 2.4. Let f be a nonzero modular function of weight k, level $\Gamma(1)$. Then

$$\sum_{\tau \in \Gamma(1)\backslash\mathfrak{h}} \frac{1}{e_\tau} v_\tau(f) + v_\infty(f) = \frac{k}{12}.$$

Proof. We first check that the sum is well–defined:

- If $\tau \in \mathfrak{h}$, then $e_\tau, v_\tau(f)$ only depend on the $\Gamma(1)$–orbit of τ. This is because if $\gamma \in \Gamma(1)$ and $\tau \in \mathfrak{h}$, then $\mathrm{Stab}_{\Gamma(1)}(\tau)$ and $\mathrm{Stab}_{\Gamma(1)}(\gamma\tau)$ are conjugate subgroups of $\Gamma(1)$, so $e_\tau = e_{\gamma\tau}$. On the other hand, $f(\gamma\tau) = f(\tau)j(\gamma,\tau)^k$ and $j(\gamma,\tau)$ is holomorphic and non–vanishing on $\mathfrak{h}$, so $v_{\gamma\tau}(f) = v_\tau(f)$.

- The sum only has a finite number of nonzero terms, since if f is a modular function and $\tilde{f}$ is a meromorphic function on $D(0,1)$, then $\exists\delta > 0$ such that $\tilde{f}$ is holomorphic and non–vanishing in $D^*(0,\delta)$. Thus $\exists R > 0$ such that f is holomorphic and non–vanishing in $\{\tau \in \mathfrak{h} \mid \mathrm{Im}(\tau) > R\}$. Hence to show the sum is finite, it suffices to show that f only has a finite number of zeroes and poles in $\mathfrak{f}$ (as $\mathfrak{f}$ intersects every $\Gamma(1)$–orbit), for which it suffices to show that f has a finite number of zeroes and poles in $\mathfrak{f} \cap \{\tau \in \mathfrak{h} \mid \mathrm{Im}(\tau) \le R\}$, which is true as the set is compact (closed and bounded) and the zeroes and poles of f are discrete.

To prove the identity, we use contour integration. Setup: if $U \subset \mathbb{C}$ is an open subset, $f : U \to \mathbb{C}$ is holomorphic and $\gamma : [0,1] \to U$ is a path, then

$$\int_\gamma f(z)\mathrm{d}z = \int_{t=0}^{1} f(\gamma(t))\gamma'(t)\mathrm{d}t.$$

We have the pullback formula: if $u : U \to V$ is a holomorphic map between open subsets of $\mathbb{C}$, $g : V \to \mathbb{C}$ is holomorphic and γ is a path in U, then

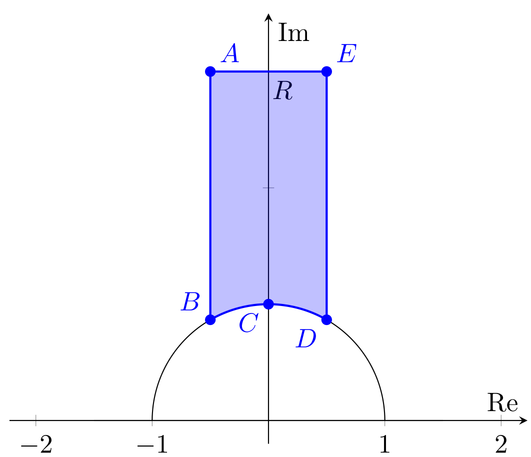
$$\int_{u\circ\gamma} g(z)\mathrm{d}z = \int_\gamma u^*(g(z)\mathrm{d}z) = \int_\gamma g(u(z))u'(z)\mathrm{d}z.$$

A particularly nice case: if $g(z) = h'(z)/h(z)$, then $g(z)\mathrm{d}z = d\log h$, so $\int_{u\circ\gamma} d\log h = \int_\gamma u^*(d\log h) = \int_\gamma d(\log h \circ u) = \int_\gamma \frac{(h\circ u)'(z)}{(h\circ u)(z)}\mathrm{d}z$.

We also have (Cauchy's) argument principle: if $U \subset \mathbb{C}$ is a simply connected open subset, $\gamma \subset U$ is a simple positvely oriented closed path and g is a meromorphic function in U with no zeroes or poles on γ, then

$$\frac{1}{2\pi i}\oint_\gamma d\log g = \frac{1}{2\pi i}\oint_\gamma \frac{g'(z)}{g(z)}\mathrm{d}z = \sum_{a\in\mathrm{Int}(\gamma)} v_a(g).$$

We now apply this to our modular function f. Choose $R > 0$ such that f has no zeroes or poles in $\{\tau \in \mathfrak{h} \mid \mathrm{Im}(\tau) \geq R\}$. We consider $\frac{1}{2\pi i}\oint_\gamma d\log f$, where γ is the contour $ABCDE$.



By choice of R, there are no zeroes or poles of f on AE. We first consider the case where f has no zeroes or poles at all on γ. Then the argument principle gives

$$\frac{1}{2\pi i}\oint_\gamma d\log f = \frac{1}{2\pi i}\int_{AB}+\int_{BC}+\int_{CD}+\int_{DE}+\int_{EA} d\log f = \sum_{\tau\in\Gamma(1)\backslash\mathfrak{h}}\frac{1}{e_\tau}v_\tau(f)$$

(as $v_\tau(f)\neq 0$, $e_\tau = 1$ under our assumptions).

Apply the pullback formula with $u(\tau)=\tau+1$. Then $u(AB)=ED$, $f\circ u = f$, so

$$\int_{u(AB)} d\log f = \int_{AB} d\log f\circ u = \int_{AB} d\log f = \int_{ED} d\log f = -\int_{DE} d\log f.$$

Hence $\int_{AB}+\int_{DE} d\log f = 0$.

Now take $q=e^{2\pi i\tau}$, so $f=\tilde{f}\circ q$ and $q(AE)$ is a positively oriented circle around 0 in $D(0,1)$. So

$$\frac{1}{2\pi i}\int_{q(AE)} d\log\tilde{f} = v_\infty(f) = \frac{1}{2\pi i}\int_{AE} d\log\tilde{f}\circ q = \frac{1}{2\pi i}\int_{AE} d\log f.$$

Now take $v(\tau)=S(\tau)=-\frac{1}{\tau}$. Then $v(BC)=DC$ and we know $f|_k[S](\tau)=f\left(-\frac{1}{\tau}\right)\tau^{-k}=f(\tau)$, so $f\circ v = f(\tau)\tau^k$. Hence

$$\begin{aligned}&\int_{DC} d\log f = \int_{v(BC)} d\log f = \int_{BC} d\log(f\circ v) = \int_{BC} d\log(f(\tau)\tau^k)\\ =&\int_{BC} d\log f + kd\log\tau = \int_{BC} d\log f + k(\log C - \log B)\end{aligned}$$

where here log is any branch of the logarithm defined on BC. But $B=\rho, C=i$, so $\log B = i\frac{2\pi}{3}$ and $\log C = i\frac{\pi}{2}$. Hence

$$\int_{CD} d\log f = -\int_{DC} d\log f + k\left(\frac{2\pi i}{3}-\frac{2\pi i}{4}\right),$$

giving

$$\int_{BC}+\int_{CD} d\log f = 2\pi i k\frac{1}{12}.$$

We have

$$\begin{aligned}\sum_{\Gamma(1)\backslash\mathfrak{h}} \frac{1}{e^\tau} v_\tau(f) =& \frac{1}{2\pi i}\left(\int_{AB} + \int_{BC} + \int_{CD} + \int_{DE} + \int_{EA} d\log f\right)\\ =& \frac{1}{2\pi i}\left(0 + \frac{k}{12} + 0 - v_\infty(f)\right)\\ \implies & \sum_{\tau\in\Gamma(1)\backslash\mathfrak{h}} \frac{1}{e_\tau} v_\tau(f) + v_\infty(f) = \frac{k}{12}.\end{aligned}$$

This finishes the proof in the case where there are no zeroes or poles. If there are zeroes or poles on γ, we need to modify the contour. For example, if there's a zero or a pole at a point P on AB, then consider the contour γ', which is just γ but with a small semicircle around our (discrete) pole, which satisfies the property that f has no zeroes or poles on γ'. The trickiest case is when there is a zero or pole at $B = \rho$ or $C = i$. This is Q3 on example sheet 1. □

16 Oct 2022, Lecture 5

Example 2.1. Take $k = 4$, $f = E_4 \in M_4(\Gamma(1))$. Hence $\forall \tau \in \mathfrak{h}, v_\tau(E_4) \geq 0$ (as it is holomorphic in $\mathfrak{h}$). We know $E_4(\tau) = 1 + \sum_{n\geq 1} a_n q^n$, so $E_4(\infty) \neq 0$ and $v_\infty(E_4) = 0$. Hence our formula gives

$$\sum_{\tau\in\Gamma(1)\backslash\mathfrak{h}} \frac{1}{e_\tau} v(E_4) = \frac{1}{3} v_\rho(E_4) + \frac{1}{2} v_i(E_4) + \sum_{\tau\in\Gamma(1)\backslash\mathfrak{h}, \tau\not\sim\rho,i} v_\tau(E_4) = \frac{1}{3}.$$

So we have $\frac{a}{3} + \frac{b}{2} + c = \frac{1}{3}$, where $a, b, c \in \mathbb{Z}_{\geq 0}$, which gives the only solution $a = 1, b = c = 0$, so $E_4(\rho) = 0$ and $E_4(\tau) \neq 0$ if $\tau \notin \Gamma(1)\rho$.

If $k = 6$, $f = E_6$, then we get

$$\frac{1}{3} v_\rho(E_6) + \frac{1}{2} v_i(E_6) + \sum_{\tau\not\sim\rho,i} v_\tau(E_6) = \frac{6}{12} = \frac{1}{12},$$

so this forces $v_\rho(E_6) = 0$, $v_i(E_6) = 1$, $v_\tau(E_6) \neq 0$ if $\tau \not\sim \rho$ and $\tau \not\sim i$, so $E_6(i) = 0$, $E_6(\tau) \neq 0$ if $\tau \not\sim \rho, i$.

Recall $\Delta = \frac{E_4^3 - E_6^2}{1728} \in S_{12}(\Gamma(1))$. This is nonzero since $\Delta(\rho) = \frac{E_4(\rho)^3 - E_6(\rho)^2}{1728} = -\frac{E_6(\rho)^2}{1728} \neq 0$. We also have $v_\infty(\Delta) \geq 1$ by construction, so plug in Δ to our formula to get

$$\sum_\tau \frac{1}{e_\tau} v_\tau(\Delta) + v_\infty(\Delta) = 1,$$

so $v_\infty(\Delta) = 1$, so Δ has a simple zero at ∞ and Δ is nonvanishing in $\mathfrak{h}$.

Theorem 2.5. Let $k \in 2\mathbb{Z}$. Then:

(1) If $k < 0$ or $k = 2$, then $M_k(\Gamma(1)) = 0$; and $M_0(\Gamma(1)) = \mathbb{C} \cdot 1$.

(2) If $4 \le k \le 10$, then $M_k(\Gamma(1)) = \mathbb{C} \cdot E_k$.

(3) For any k, multiplication by Δ gives an isomorphism $M_k(\Gamma(1)) \xrightarrow{\times\Delta} S_{k+12}(\Gamma(1))$.

Proof. (1) Let $f \in M_k(\Gamma(1))$ be nonzero. Then $\sum \frac{1}{e_\tau} v_\tau(f) + v_\infty(f) = \frac{k}{12}$. Note the LHS is ≥ 0, but for $k < 0$, the RHS is < 0. If $k = 2$, then we get the equation $\frac{a}{3} + \frac{b}{2} + c = \frac{1}{6}$ for $a, b, c \in \mathbb{Z}_{\ge 0}$, which has no solutions.

Suppose $f \in M_0(\Gamma(1)) \setminus \mathbb{C} \cdot 1$. Then $f - f(\infty) \cdot 1 \in S_0(\Gamma(1))$ is a nonzero function (here 1 is the constant function 1). Then $\sum_\tau \frac{1}{e_\tau} v_\tau(f - f(\infty) \cdot 1) + \underbrace{v_\infty(f - f(\infty) \cdot 1)}_{\ge 1} = 0$, a contradiction, so $M_0(\Gamma(1)) = \mathbb{C} \cdot 1$.

(2) Let $4 \le k \le 10$ and $f \in M_k(\Gamma(1))$. Consider $f - f(\infty) \cdot E_k \in S_k(\Gamma(1))$. If this is nonzero, then

$$\sum_\tau \frac{1}{e_\tau} v_\tau(f - f(\infty) \cdot E_k) + \underbrace{v_\infty(f - f(\infty) \cdot E_k)}_{\ge 1} = \frac{k}{12} < 1,$$

a contradiction. So $f = f(\infty) \cdot E_k$.

(3) Our map $\times\Delta : M_k(\Gamma(1)) \to S_{k+12}(\Gamma(1))$ is a well–defined $\mathbb{C}$–linear map. It is injective, since if $\Delta f = 0$, then $f = 0$ (as Δ is nonvanishing in $\mathfrak{h}$). For surjectivity, if $f \in S_{k+12}(\Gamma(1))$, then $\frac{f}{\Delta}$ is holomorphic in $\mathfrak{h}$ and invariant under the weight k action of $\Gamma(1)$.

We need to show $\frac{f}{\Delta}$ is holomorphic at ∞, as then $\frac{f}{\Delta} \in M_k(\Gamma(1))$, so $f = \frac{f}{\Delta} f \in \mathrm{Im}(\times\Delta)$. Hence we need $v_\infty\left(\frac{f}{\Delta}\right) \ge 0$. But $v_\infty\left(\frac{f}{\Delta}\right) = \underbrace{v_\infty(f)}_{\ge 1} - \underbrace{v_\infty(\Delta)}_{=1} \ge 0$, so we're done.

∎

Corollary 2.6. If $k \in 2\mathbb{Z}$, $k \ge 0$, then $M_k(\Gamma(1))$ is finite–dimensional and

$$\dim_{\mathbb{C}} M_k(\Gamma(1)) = \begin{cases} \lfloor \frac{k}{12} \rfloor + 1 & k \not\equiv 2 \pmod{12}. \\ \lfloor \frac{k}{12} \rfloor & k \equiv 2 \pmod{12}. \end{cases}$$

Proof. We proved this for $0 \le k \le 10$. In general, use induction on k: we need to show that for $k \ge 0$, $\dim_{\mathbb{C}} M_{k+12}(\Gamma(1)) = \dim_{\mathbb{C}} M_k(\Gamma(1)) + 1$.

We know $E_{k+12} \in M_{k+12}(\Gamma(1))$, so $M_{k+12}(\Gamma(1)) = \mathbb{C}E_{k+12} \oplus S_{k+12}(\Gamma(1))$. But this equals $\mathbb{C}E_{k+12} \oplus \Delta M_k(\Gamma(1))$, so $\dim_{\mathbb{C}} M_{k+12}(\Gamma(1)) = 1 + \dim_{\mathbb{C}} M_k(\Gamma(1))$.

∎

Example 2.2. We have $E_4^2 \in M_8(\Gamma(1)) = \mathbb{C}E_8$. So there is a relation between E_4^2 and E_8 (in this case, one is a scalar multiple of the other), but we have $E_8(\infty) = 1 = E_4(\infty)^2 \implies E_4^2 = E_8$.

Similarly, $E_4E_6 \in M_{10}(\Gamma(1)) = \mathbb{C}E_{10}$, so we find $E_4E_6 = E_{10}$.

Corollary 2.7. If $k \in 2\mathbb{N}$, then $M_k(\Gamma(1))$ is spanned as a $\mathbb{C}$–vector space by $\{E_4^aE_6^b \mid a, b \in \mathbb{Z}_{\geq 0}, 4a + 6b = k\}$. In other words, if $\mathcal{M} = \oplus_{k\in\mathbb{Z}}M_k(\Gamma(1))$, then $\mathcal{M}$ is a graded $\mathbb{C}$–algebra generated by E_4 and E_6.

Proof. We proved this for $0 \leq k \leq 10$. If $k \geq 12$, then

$$M_k(\Gamma(1)) = \mathbb{C}E_k \oplus \Delta M_{k-12}(\Gamma(1)) = \mathbb{C}f \oplus \Delta M_{k-12}(\Gamma(1))$$

for any $f \in M_k(\Gamma(1))$ such that $f(\infty) \neq 0$ by the same argument. We can always find some $A, B \in \mathbb{Z}_{\geq 0}$ such that $4A+6B = k$, so $E_4^AE_6^B \in M_k(\Gamma(1))$ and $(E_4^AE_6^B)(\infty) \neq 0$. Now by induction, $M_{k-12}(\Gamma(1)) = \langle E_4^aE_6^b \mid 4a+6b = k-12\rangle$, so $\Delta M_{k-12}(\Gamma(1)) = \langle \Delta E_4^aE_6^b \mid 4a + 6b = k - 12\rangle$. But $\Delta \in \langle E_4^3, E_6^2\rangle$, so

$$\Delta M_{k-12}(\Gamma(1)) = \langle E_4^aE_6^b \mid 4a + 6b = k\rangle$$

and $E_4^AE_6^B \in \langle E_4^aE_6^b \mid 4a + 6b = k\rangle$, so $M_k(\Gamma(1)) = \langle E_4^aE_6^b \mid 4a + 6b = k\rangle$. □

Theorem 2.8. Let $j(\tau) = \frac{E_4(\tau)^3}{\Delta}$. Then j is a modular function of weight 0, level $\Gamma(1)$ which is holomorphic on $\mathfrak{h}$ and has a simple pole at ∞. It defines a bijection $\Gamma(1) \setminus \mathfrak{h} \to \mathbb{C}$ given by $\tau \to j(\tau)$. Moreover, every modular function of weight 0, level $\Gamma(1)$ is a rational function of j.[6]

The interpretation of this is that it is possible to define a Riemann surface structure on $\Gamma(1) \setminus \mathfrak{h} \sqcup \{\infty\}$ such that we get a compact Riemann surface whose meromorphic functions are exactly the modular functions of weight 0. So the theorem says that this Riemann surface, called $X(1)$, is isomorphic to the Riemann sphere, and our formula says that if $\mathcal{L}$ is an invertible sheaf on a compact Riemann surface and S is a meromorphic section, then $\sum_a v_a(S) = \deg(\mathcal{L})$. This is useful if we are also taking algebraic geometry.

18 Oct 2022, Lecture 6

Proof. We showed that Δ is nonvanishing in $\mathfrak{h}$ and has a simple zero at ∞. Hence j is holomorphic in $\mathfrak{h}$ and $v_\infty(j) = 3v_\infty(E_4) - v_\infty(\Delta) = -1$. Note that if $\gamma \in \Gamma(1)$, then $j|_0[\gamma](\tau) = j(\gamma\tau) = j(\tau)$ since the map is constant on $\Gamma(1)$–orbits. To show the map is a bijection, we need to show that $\forall z \in \mathbb{C}$, there exists a unique orbit $\Gamma(1)\cdot\tau$ such that $j(\tau) = z$, i.e. $v_\tau(j - z) > 0$.

We know

$$\sum_{\tau\in\Gamma(1)\setminus\mathfrak{h}} \frac{1}{e_\tau} \underbrace{v_\tau(j-z)}_{\geq 0,\text{ as } j-z \text{ is holomorphic in } \mathfrak{h}.} = 1,$$

[6] Remember that $\Gamma(1) \setminus \mathfrak{h}$ is the set of orbits of $\Gamma(1)$ under $\mathfrak{h}$.

(since $v_\infty(j-z) = -1$ and $\frac{k}{12} = 0$) again giving $\frac{a}{3} + \frac{b}{2} + c = 1$ for $a, b, c \in \mathbb{Z}_{\geq 0}$, $a = v_\rho(j-z), b = v_i(j-z), c = \sum_{\tau \not\sim \rho, i} v_\tau(j-z)$. This gives the solutions

- $(a, b, c) = (0, 0, 1)$, so $j - z$ vanishes at a unique $\Gamma(1) \cdot \tau$.
- $(a, b, c) = (0, 2, 0)$, so $j - z$ vanishes at i.
- $(a, b, c) = (3, 0, 0)$, so $j - z$ vanishes at ρ.

Hence our map is bijective. Consider a nonzero modular function f of weight 0. To get rid of all the poles, we can consider a product $f \cdot \prod_{i=0}^{n} (j(\tau) - j(a_i))^{b_i}$ for $a_i \in \mathfrak{h}$, $b_i \in \mathbb{Z}_{\geq 0}$, where the a_i are among the poles of f in $\mathfrak{h}$. Hence to show f is a rational function of j, it is enough to consider the case where f is holomorphic in $\mathfrak{h}$. Then there exists $m \geq 0$ such that $\Delta^m f$ is holomorphic at ∞, so $\Delta^m f$ is holomorphic in $\mathfrak{h}$ and at ∞, so $\Delta^m f \in M_{12m}(\Gamma(1))$. We showed that $M_{12m}(\Gamma(1)) = \langle E_4^a E_6^b \mid 4a + 6b = 12m \rangle$, so f is a linear combination of functions of the form $\frac{E_4^a E_6^b}{\Delta^m}$, where $4a + 6b = 12m$.

Hence it is enough to show that $\frac{E_4^a E_6^b}{\Delta^m}$ is a rational function of j where $4a + 6b = 12m$, $a, b \in \mathbb{Z}_{\geq 0}$. But then $2a + 3b = 6m$, which gives $p, q \in \mathbb{Z}_{\geq 0}$ such that $a = 3p, b = 2q$, so $p + q = m$. Then

$$\frac{E_4^a E_6^b}{\Delta^m} = \left(\frac{E_4^3}{\Delta}\right)^p \left(\frac{E_6^2}{\Delta}\right)^q = j^p \left(\frac{E_6^2}{\Delta}\right)^q.$$

As $E_4^3 - E_6^2 = 1728\Delta$, we get $j = \frac{E_6^2}{\Delta} + 1728$. So this is a rational function of j. ☐

Proposition 2.9. Let $k \geq 4$ be an even integer. Then

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n \geq 1} \sigma_{k-1}(n) q^n$$

where $q = e^{2\pi i \tau}$ and $\sigma_{k-1}(n) = \sum_{d \mid n} d^{k-1}$.

Proof. We start from the identity

$$\pi \cot(\pi\tau) = \frac{1}{\tau} + \sum_{n \geq 1} \left(\frac{1}{\tau + n} + \frac{1}{\tau - n}\right).$$

This is true for $\tau \in \mathfrak{h}$ and it is even locally uniformly convergent in $\mathfrak{h}$. We can write

$$\pi \cot(\pi\tau) = i\pi \frac{e^{\pi i \tau} + e^{-\pi i \tau}}{e^{\pi i \tau} - e^{-\pi i \tau}} = \pi i \frac{q+1}{q-1} = -\pi i (1+q)(1-q)^{-1} = -\pi i \left(1 + 2\sum_{n \geq 1} q^n\right).$$

Differentiate term–by–term $k-1$ times. The RHS of the bottom expression is

$$-2\pi i\left(\frac{\mathrm{d}}{\mathrm{d}\tau}\right)^{k-1}\left(\sum_{n\geq 1} q^n\right) = -(2\pi i)^k\sum_{n\geq 1} n^{k-1}q^n,$$

while the RHS of the top expression is

$$(-1)^{k-1}(k-1)!\left(\tau^{-k}+\sum_{n\geq 1}(\tau+n)^{-k}+(\tau-n)^{-k}\right) = (-1)^{k-1}(k-1)!\sum_{n\in\mathbb{Z}}(\tau+n)^{-k}.$$

Rearranging and using the fact that k is even (to make the sign go away) gives

$$\sum_{n\in\mathbb{Z}}(\tau+n)^{-k} = \frac{(2\pi i)^k}{(k-1)!}\sum_{n\geq 1} n^{k-1}q^n, \tau\in\mathfrak{h}.$$

Then

$$G_k(\tau) = \sum_{(m,n)\in\mathbb{Z}^2\setminus 0}(m\tau+n)^{-k} = 2\zeta(k)+\sum_{\substack{(m,n)\in\mathbb{Z}^2\setminus 0,\\ m\neq 0}}(m\tau+n)^{-k} = 2\zeta(k)+2\sum_{m\geq 1}\sum_{n\in\mathbb{Z}}(m\tau+n)^{-k}.$$

Plug in our identity to get

$$G_k(\tau) = 2\zeta(k)+\sum_{m\geq 1}\frac{(2\pi i)^k}{(k-1)!}\sum_{n\geq 1} n^{k-1}q^{mn} = 2\zeta(k)+\frac{2(2\pi i)^k}{(k-1)!}\sum_{N\geq 1}\underbrace{\left(\sum_{n|N} n^{k-1}\right)}_{=\sigma_{k-1}(N)}q^N.$$

□

Corollary 2.10. $E_k(\tau) = \frac{G_k(\tau)}{2\zeta(k)} = 1+\sum_{n\geq 1} a_n q^n$ has all $a_n\in\mathbb{Q}$. Moreover, if $k=4$ or $k=6$, then $a_n\in\mathbb{Z}$.

Proof. We have

$$E_k(\tau) = 1+\frac{(2\pi i)^k}{\zeta(k)(k-1)!}\sum_{n\geq 1}\sigma_{k-1}(n)q^n.$$

Hence we need to show that $\frac{\zeta(k)}{\pi^k}$ is rational. This is on example sheet 1 (when

k is even). One can show that $\zeta(4) = \frac{\pi^4}{90}$ and $\zeta(6) = \frac{\pi^6}{945}$, so

$$E_4(\tau) = 1 + \frac{2^4\pi^4 \cdot 90}{\pi^4 \cdot 6} \sum_{n \geq 1} \sigma_3(n) q^n = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n$$
$$E_6(\tau) = 1 - \frac{2^6\pi^6 \cdot 3^3 \cdot 5 \cdot 7}{\pi^6 \cdot 5!} \sum_{n \geq 1} \sigma_5(n) q^n = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n.$$

□

Corollary 2.11. If $\Delta(\tau) = \sum_{n \geq 1} \tau(n) q^n$ is the q–expansion of Δ, then $\tau(1) = 1$ and $\tau(n) \in \mathbb{Z}\ \forall n \geq 1$.

Proof. Write $E_4 = 1 + 240U$ and $E_6 = 1 - 504V$ for $U, V = q + \ldots \in \mathbb{Z}[[q]]$. Then

$$\begin{aligned}\Delta &= \frac{E_4^3 - E_6^2}{1728} = \frac{(1+240U)^3 - (1-504V)^2}{1728} \\ &= \frac{3 \cdot 240U + 3 \cdot 240^2 U^2 + 240^3 U^3 + 2 \cdot 504V - 504^2 V^2}{1728} \\ &= \frac{(3 \cdot 240U + 2 \cdot 504V)}{1728} + R,\end{aligned}$$

where we claim $R \in q^2\mathbb{Z}[[q]]$, but for this we just need to check that $1728 \mid 3 \cdot 240^2, 1728 \mid 240^3, 1728 \mid 504^2$, which is true.

We need to check that

$$\frac{(3 \cdot 240U + 2 \cdot 504V)}{1728} = \frac{2^4 \cdot 3^2 \cdot 5 \cdot U + 2^4 \cdot 3^2 \cdot 7 \cdot V}{2^6 \cdot 3^3} \in \mathbb{Z}[[q]].$$

But this equals

$$\frac{5U + 7V}{12} = \frac{5(U-V)}{12} + V.$$

Hence we need to check that

$$\frac{5}{12}(\sigma_3(n) - \sigma_5(n)) \in \mathbb{Z}\ \forall n \geq 1,$$

i.e. we need to check that

$$\sigma_3(n) \equiv \sigma_5(n) \pmod{12}\ \forall n \geq 1.$$

But this is true as $d^3 \equiv d^5 \pmod{12}\ \forall d \in \mathbb{N}$.

Finally, we compute $\tau(1) = \frac{3 \cdot 240 + 2 \cdot 504}{1728} = 1$. □

20 Oct 2022, Lecture 7

Theorem 2.12. Let $k \geq 4$ be even and $N = \dim_{\mathbb{C}} S_k(\Gamma(1))$. Then there exists a unique basis $f_0, \ldots, f_N$ for $M_k(\Gamma(1))$ as a $\mathbb{C}$–vector space such that

(a) $\forall 0 \leq i \leq N$, $f_i = \sum_{n\geq 0} a_n(f_i)q^n$ for $a_n(f_i) \in \mathbb{Z}$ $\forall n \geq 0$.

(b) If $0 \leq i, n \leq N$, then $a_n(f_i) = \delta_{in}$.

So in other words, $f_i = q^i + O(q^{N+1})$. This is important because $M_k(\Gamma(1))$ has a $\mathbb{Z}$–structure, i.e. we can realize it as a tensor product $M_k(\Gamma(1)) = M_k(\Gamma(1), \mathbb{Z}) \oplus \mathbb{C}$, where $M_k(\Gamma(1), \mathbb{Z}) = \{f \in M_k(\Gamma(1)) \mid \forall n \geq 0, a_n(f) \in \mathbb{Z}\}$.

Proof. We first construct $f_0, \ldots, f_N \in M_k(\Gamma(1))$ with properties (a) and (b). Write $k = 12a + d$, for $a, d \in \mathbb{Z}_{\geq 0}$ such that $d = 14$ if $k \equiv 2 \pmod{12}$, or $0 \leq d \leq 10$ if $d \not\equiv 2 \pmod{12}$.

Then

$$\left\lfloor \frac{k}{12} \right\rfloor = \begin{cases} a & k \not\equiv 2 \pmod{12} \\ a+1 & k \equiv 2 \pmod{12} \end{cases} \implies \lfloor a \rfloor = \begin{cases} \lfloor \frac{k}{12} \rfloor & k \not\equiv 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor - 1 & k \equiv 2 \pmod{12}. \end{cases}$$

We have $\dim_{\mathbb{C}} M_k(\Gamma(1)) = N + 1 = \begin{cases} \lfloor \frac{k}{12} \rfloor + 1 & k \not\equiv 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor & k \equiv 2 \pmod{12}, \end{cases}$ so $a = N$, $k = 12N + d$.

Now consider $A, B \in \mathbb{Z}_{\geq 0}$ such that $d = 4A + 6B$. Consider the modular forms

$$g_i = \Delta^i E_4^A E_6^B E_6^{2(N-i)}$$

for $0 \leq i \leq N$. Each g_i has weight $12i + 4A + 6B + 12(N-i) = 12N + d = k$, so $g_i \in M_k(\Gamma(1))$. As E_4, E_6, Δ have q–expansions in $\mathbb{Z}[[q]]$, so does g_i. The leading term of g_i is q^i, so the q–expansions look like

$$\begin{aligned} g_0 &= 1 + a_1(g_0)q + \ldots + a_N(g_0)q^N + O(q^{N+1}) \\ &\vdots \\ g_{N-1} &= 0 + \ldots + q_{N-1} + a_N(g_{N-1})q^N + O(q^{N+1}) \\ g_N &= 0 + \ldots + 0 + q^N + O(q^{N+1}) \end{aligned}$$

We can now carry out row reduction on the g_i to obtain $f_0, \ldots, f_N$ satisfying (a) and (b). For uniqueness, consider the linear functionals

$$\begin{aligned} a_0, \ldots, a_N &: M_k(\Gamma(1)) \to \mathbb{C} \\ f &\mapsto a_i(f),\ f = \sum_{n\geq 0} a_n(f)q^n. \end{aligned}$$

Then $a_i(f_j) = \delta_{ij}$, which forces $a_0, \ldots, a_n$ to be linearly independent. Hence they form a basis of the dual vector space $M_k(\Gamma(1))^*$. So $f_0, \ldots, f_N$ is the dual basis of $M_k(\Gamma(1))$, and they form the unique basis with this property. $\square$

3 Hecke operators

Hecke operators are just symmetries (linear endomorphisms) of spaces of modular forms. They can arise from either representation theory: $\Gamma(1) \leq GL_2(\mathbb{Q})^+$, which acts on $\{f : \mathfrak{h} \to \mathbb{C}\}$ by $f \mapsto f|_k[g]$. But $M_k(\Gamma(1)) \leq \{f : \mathfrak{h} \to \mathbb{C}\}^{\Gamma(1)}$, and a general group theory fact says that under suitable conditions, there's an action by a big class of operators; or from geometry: we can think of modular forms as functions on the set of lattices $\mathcal{L}$ in $\mathbb{C}$. In this course, we will follow the second point of view.

Recall. If V is a finite–dimensional $\mathbb{R}$–vector space, then a lattice Λ in V is a subgroup $\Lambda \subset V$ which is discrete and cocompact (i.e. V/Λ is compact).

Lemma 3.1. A subgroup $\Lambda \leq V$ is a lattice if and only if there exists a basis $e_1, \ldots, e_n$ for V as a $\mathbb{R}$–vector space such that $\Lambda = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_n$.

Proof. This is a question on example sheet 2. $\square$

We study $\mathcal{L} = \{\Lambda \leq \mathbb{C} \text{ a lattice}\}$ with its action by $\mathbb{C}^\times$, i.e. $z\Lambda = \{z\lambda \mid \lambda \in \Lambda\}$ for $z \in \mathbb{C}^\times, \Lambda \in \mathcal{L}$.

Proposition 3.2. The map $\tau \mapsto \Lambda\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$ induces a bijection between

$$\Gamma(1) \setminus \mathfrak{h} \leftrightarrow \mathbb{C}^\times \setminus \mathcal{L}$$

(orbits of $\Gamma(1)$ in $\mathfrak{h}$ and the set of lattices in $\mathbb{C}$ modulo scalar multiplication).

Proof. This map is well–defined, since if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, $\tau \in \mathfrak{h}$, then

$$\Lambda_{\gamma\tau} = \mathbb{Z}\left(\frac{a\tau + b}{c\tau + d}\right) \oplus \mathbb{Z} = (c\tau + d)^{-1}\left(\mathbb{Z}(a\tau + b) \oplus \mathbb{Z}(c\tau + d)\right) = (c\tau + d)^{-1}\Lambda_\tau.$$

For surjectivity, if Λ is a lattice, then $\Lambda = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$ with $\mathrm{Im}\left(\frac{e_1}{e_2}\right) \neq 0$. Swapping e_1, e_2 if necessary, we may assume that $\mathrm{Im}\left(\frac{e_1}{e_2}\right) > 0$. Then $\Lambda = e_2(\mathbb{Z}e_1/e_2 \oplus \mathbb{Z}) = e_1\Lambda_\tau$ for $\tau = \frac{e_1}{e_2}$.

For injectivity, if τ, τ' have the same image, then $\exists z \in \mathbb{C}^\times$ such that $\mathbb{Z}\Lambda_\tau = \Lambda_{\tau'}$, i.e. $\exists \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ such that $\tau' = az\tau + bz, 1 = cz\tau + dz$. Then $\tau' = \frac{az\tau + bz}{cz\tau + dz} = \frac{a\tau + b}{c\tau + d}$. But $\mathrm{Im}(\tau') = \mathrm{Im}(\gamma\tau) = \det(\gamma)\frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}$ and $\mathrm{Im}(\tau) > 0, \mathrm{Im}(\tau') > 0$, hence $\det(\gamma) > 0$, so $\det(\gamma) = 1$ and so $\gamma \in \Gamma(1)$. $\square$

Definition 3.1. If $k \in \mathbb{Z}$, say a function $F : \mathcal{L} \to \mathbb{C}$ is **of weight** k if $\forall z \in \mathbb{C}^\times, \Lambda \in \mathcal{L}$, $F(z\Lambda) = z^{-k}F(\Lambda)$.

Proposition 3.3. Let

$$V_k = \{F : \mathcal{L} \to \mathbb{C} \text{ of weight } k\}.$$
$$W_k = \{f : \mathfrak{h} \to \mathbb{C} \mid \forall \gamma \in \Gamma(1), f|_k[\gamma] = f\}.$$

Then the map $F \mapsto (f : \tau \mapsto F(\Lambda\tau))$ induces a $\mathbb{C}$-vector space isomorphism $V_k \to W_k$.

Proof. We first check that if $F \in V_k$, $f(\tau) = F(\Lambda\tau)$, then $f \in W_k$. If $\gamma \in \Gamma(1)$,

$$f|_k[g](\tau) = f(\gamma\tau)j(\gamma,\tau)^{-k} = F(\lambda\gamma\tau)j(\gamma,\tau)^{-k} = F(j(\gamma,\tau)\Lambda_{\gamma\tau}) = F(\Lambda\tau) = f(\tau),$$

so $j(\gamma,\tau)\Lambda_{\gamma\tau} = \Lambda_\tau$.

To show that the map is an isomorphism, we write down its inverse: define $\alpha : W_k \to V_k$ by $\alpha(f)(\Lambda) = e_2^{-k} f(e_1/e_2)$ if $\Lambda = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$ with $\mathrm{Im}(e_1/e_2) > 0$. This is well–defined, since if e_1', e_2' is another basis with $\mathrm{Im}(e_1'/e_2') > 0$, then $\exists \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ such that $e_1' = ae_1 + be_2, e_2' = ce_1 + de_2$. Then

$$\begin{aligned} e_2'^{-k} f(e_1'/e_2') &= (ce_1 + de_2)^{-k} f\left(\frac{ae_1 + be_2}{ce_1 + de_2}\right) \\ &= e_2^{-k}(ce_1/e_2 + d)^{-k} f\left(\frac{ae_1/e_2 + b}{ce_1/e_2 + d}\right) = e_2^{-k} f\left(\frac{e_1}{e_2}\right). \end{aligned}$$

Exercise: check that the two maps are inverse to each other. □

23 Oct 2022, Lecture 8

Definition 3.2. Let $n \in \mathbb{N}$. The n^{th} Hecke operator $T_n : V_k \to V_k$ is defined by the formula

$$(T_n F)(\Lambda) = n^{k-1} \sum_{\Lambda' \underset{n}{\leq} \Lambda} F(\Lambda').$$

Here $\sum_{\Lambda' \underset{n}{\leq} \Lambda}$ means summing over all subgroups Λ' of Λ of index n.

We also write $T_n : W_k \to W_k$ for the endomorphism arising from the isomorphism $V_k \xrightarrow{\sim} W_k$.

Why is T_n a well–defined endomorphism of V_k? First of all, the sum is finite since there's a bijection

$$\begin{aligned} \{\Lambda' \leq \Lambda\} &\leftrightarrow \{H \leq \Lambda/n\Lambda \text{ of index } n\} \\ \Lambda' &\mapsto \Lambda'/n\Lambda \\ H + n\Lambda &\leftarrow H \end{aligned}$$

This is well–defined, since Lagrange's theorem implies that

$$\Lambda' \underset{n}{\leq} \Lambda \implies n(\Lambda/\Lambda') = 0 \implies n\Lambda \leq \Lambda'.$$

But $\Lambda/n\Lambda \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is finite, so it has finitely many subgroups of index n.

If $\Lambda' \underset{n}{\leq} \Lambda$, then $n\Lambda \leq \Lambda' \leq \Lambda$, so Λ' is also discrete and cocompact in $\mathbb{C}$.

We next check that T_nF is of weight k, i.e. that $(T_nF)(z\Lambda) = z^{-k}(T_nF)(\Lambda)$. We have an isomorphism $\{\Lambda' \underset{n}{\leq} z\Lambda\} \leftrightarrow \{\Lambda' \underset{n}{\leq} \Lambda\}$ given by $\Lambda' \mapsto z^{-1}\Lambda'$, so

$$(T_nF)(z\Lambda) = n^{k-1} \sum_{\Lambda' \underset{n}{\leq} z\Lambda} F(\Lambda') = n^{k-1} \sum_{\Lambda' \underset{n}{\leq} \Lambda} F(z\Lambda') = n^{k-1} \sum_{\Lambda' \underset{n}{\leq} \Lambda} z^{-k} F(\Lambda') = z^{-k}(T_nF)(\Lambda).$$

Proposition 3.4. (1) If $m, n \in \mathbb{N}$ with $(m,n) = 1$, then $T_mT_n = T_{mn}$.

(2) If p is a prime number and $n \in \mathbb{N}$, then $T_{p^n}T_p = T_{p^{n+1}} + p^{k-1}T_{p^{k-1}}$ (acting on V_k).

Proof. Let $m, n \in \mathbb{N}$, not necessarily coprime. Then

$$\begin{aligned}(T_m(T_nF))(\Lambda) &= m^{k-1} \sum_{\Lambda' \underset{m}{\leq} \Lambda} (T_nF)(\Lambda') = (mn)^{k-1} \sum_{\Lambda' \underset{m}{\leq} \Lambda} \sum_{\Lambda'' \underset{n}{\leq} \Lambda'} F(\Lambda'') \\ &= (mn)^{k-1} \sum_{\Lambda'' \underset{mn}{\leq} \Lambda} a(\Lambda, \Lambda'') F(\Lambda''),\end{aligned}$$

where $a(\Lambda, \Lambda'') = |\{\Lambda \underset{m}{\geq} \Lambda' \underset{n}{\geq} \Lambda''\}| = |H \leq \Lambda/\Lambda'' \mid |H| = n|$ is the number of ways to express Λ' as an intermediate subgroup. If $(m,n) = 1$, then $a(\Lambda, \Lambda'') = 1$ for all $\Lambda'' \leq \Lambda$ as any finite abelian group of order mn has a unique subgroup of order n.

(1) In this case, we find

$$T_mT_nF(\Lambda) = (mn)^{k-1} \sum_{\Lambda'' \underset{mn}{\leq} \Lambda} F(\Lambda'') = (T_{mn}F)(\Lambda) \implies T_mT_n = T_{mn}.$$

(2) The same computation gives (for p prime, $n \in \mathbb{N}$)

$$(T_{p^n}(T_pF))(\Lambda) = p^{(n+1)(k-1)} \sum_{\Lambda'' \underset{p^{n+1}}{\leq} \Lambda} a(\Lambda, \Lambda'') F(\Lambda''),$$

where $a(\Lambda, \Lambda') = |\{H \subset \Lambda/\Lambda'' \mid |H| = p\}|$. But if $\Lambda'' \underset{p^{n+1}}{\leq} \Lambda$, then Λ/Λ'' need not have a unique subgroup of order p, as $\Lambda \cong \mathbb{Z}^2$, so Λ/Λ'' is a finite abelian group of order p^{n+1} that can be generated by 2 elements. But any such group is isomorphic to $\mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}/p^b\mathbb{Z}$, where $a \geq b \geq 0$ are integers such that $a + b = n + 1$. We now split into two cases:

- $b = 0$, so $a = n + 1$ and $\Lambda/\Lambda'' \cong \mathbb{Z}/p^{n+1}\mathbb{Z}$. This group is cyclic and has a unique subgroup of order p, so $a(\Lambda, \Lambda'') = 1$.
- $b > 0$, so $\Lambda/\Lambda'' \cong \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}/p^b\mathbb{Z}$. Let $\Lambda/\Lambda''[p] = \{x \in \Lambda/\Lambda'' \mid px = 0\}$. This is a subgroup of Λ/Λ'', and

$$\{H \leq \Lambda/\Lambda'' \mid |H| = p\} = \{H \leq \Lambda/\Lambda''[p] \mid |H| = p\}.$$

  Hence $\Lambda/\Lambda''[p] \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ from our above isomorphism. So in this case, $a(\Lambda, \Lambda'') = |\{H \leq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \mid |H| = p\}|$. In other words,

$$a(\Lambda, \Lambda') = |\mathbb{P}^1(\mathbb{F}_p)| = |\mathbb{A}^1(\mathbb{F}_p) \cup \{\infty\}| = p + 1.$$

How do we distinguish between these two cases? We will show on example sheet 2 that if $\Lambda'' \underset{p^{n+1}}{\leq} \Lambda$, then there exists a $\mathbb{Z}$–basis e_1, e_2 for Λ such that $\Lambda'' = \mathbb{Z}p^a e_1 \oplus \mathbb{Z}p^b e_2$ for the same a, b satisfying $a \geq b \geq 0, a + b = n + 1$ as before (this is a consequence of Smith normal form).

Hence we see that we are in case 2 if and only if $\Lambda'' \leq p\Lambda$. Thus we find

$$(T_{p^n}(T_pF)(\Lambda)) = p^{(n+1)(k-1)} \sum_{\Lambda'' \underset{p^{n+1}}{\leq} \Lambda} F(\Lambda'') + p^{(n+1)(k-1)} \sum_{\substack{\Lambda'' \leq p\Lambda \\ p^{n-1}}} pF(\Lambda'').$$

Here each Λ'' in case 1 goes into the first sum and each Λ'' in case 2 goes once into the first sum and p times into the second sum. We have

$$\begin{aligned} p^{(n+1)(k-1)} \sum_{\Lambda'' \underset{p^{n+1}}{\leq} p\Lambda} pF(\Lambda'') &= p^{(n-1)(k-1)} p^{2(k-1)} \sum_{\Lambda'' \underset{p^{n-1}}{\leq} \Lambda} pF(p\Lambda'') \\ =& p^{(n-1)(k-1)} p^{2(k-1)} p^{1-k} \sum_{\Lambda'' \underset{p^{n-1}}{\leq} \Lambda} F(\Lambda'') = p^{k-1} T_{p^{n+1}} F(\Lambda). \end{aligned}$$

Hence $T_{p^n} T_p F(\Lambda) = T_{p^{n+1}} F(\Lambda) + p^{k-1} T_{p^{n-1}} F(\Lambda)$.

□

Corollary 3.5. $\forall m, n \in \mathbb{N}$, $T_m T_n = T_n T_m$ as endomorphisms of V_k, i.e. all Hecke operators commute.

Proof. If we write $m = \prod_{i=1}^r p_i^{a_i}$ for $a_i \geq 1$, p_i distinct, then $T_m = T_{p_1^{a_1}} \dots T_{p_r^{a_r}}$. We've shown that if p, q are distinct primes, then T_{p^a}, T_{q^b} commute $\forall a, b \geq 1$.

We need to show that if p is a prime and $a, b \in \mathbb{N}$, then T_{p^a} and T_{p^b} commute. But we have a stronger claim that $\forall a \in \mathbb{N}$, T_{p^a} is a polynomial in T_p. We prove this by induction on a, the case $a = 1$ being trivial.

In general, $T_{p^{a+1}} = T_{p^a}T_p - p^{k-1}T_{p^{a-1}}$, which proves the claim. $\square$

25 Oct 2022, Lecture 9

Lemma 3.6. Let $n \in \mathbb{N}$ and $\Lambda = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \leq \mathbb{C}$ a lattice. Then $\{\Lambda' \underset{n}{\leq} \Lambda\} = \{\mathbb{Z}(ae_1 + be_2) \oplus \mathbb{Z}de_2 \mid a, b, d \in \mathbb{Z}_{\geq 0}, ad = n, b < d\}$, where this is isomorphic to the set $\{a, b, d \in \mathbb{Z}_{\geq 0} \mid ad = n, 0 \leq b < d\}$.

Proof. Consider the short exact sequence

$$0 \to \mathbb{Z}e_2/\mathbb{Z}e_2 \cap \Lambda' \to \Lambda/\Lambda' \to \underbrace{\Lambda/\mathbb{Z}e_2 + \Lambda'}_{\cong \mathbb{Z}e_1/\mathbb{Z}e_1 \cap (\mathbb{Z}e_2 + \Lambda)} \to 0.$$

Then $|\Lambda/\Lambda'| = n$. We let $d = |\mathbb{Z}e_2/\mathbb{Z}e_2 \cap \Lambda'| = \inf\{d \geq 1 \mid de_2 \in \Lambda'\}$ and $a = |\Lambda/\mathbb{Z}e_2 + \Lambda'| = \inf\{a \geq 1 \mid \exists b \in \mathbb{Z} \text{ s.t. } ae_1 + be_2 \in \Lambda'\}$. Then $n = ad$ and there exists a unique $0 \leq b < d$ such that $ae_1 + be_2 \in \Lambda'$.

We now claim that $\Lambda' = \mathbb{Z}(ae_1 + be_2) \oplus \mathbb{Z}de_2$. The inclusion $\geq$ is clear. On the other hand, if $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{Z})$, $\alpha\delta - \beta\gamma = N \in \mathbb{Z}$ is nonzero, then $[\Lambda : \mathbb{Z}(\alpha e_1 + \beta e_2) \oplus \mathbb{Z}(\gamma e_1 + \delta e_2)] = |N|$. So $[\Lambda : \mathbb{Z}(\alpha e_1 + \beta e_2) \oplus \mathbb{Z}(\gamma e_1 + \delta e_2)] = \det \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = n = [\Lambda : \Lambda']$, so $[\Lambda' : \mathbb{Z}(ae_1 + be_2) \oplus \mathbb{Z}de_2] = 1$, so they're equal.

We've defined a map $\{\Lambda' \underset{n}{\leq} \Lambda\} \to \{(a, b, d) \in \mathbb{Z}_{\geq 0} \mid ad = n, 0 \leq b < d\}$. This map has an inverse, given by $(a, b, d) \mapsto \mathbb{Z}(ae_1 + be_2) \oplus \mathbb{Z}de_2$, so it's a bijection. $\square$

Lemma 3.7. Let $f \in W_k$. Then we have the two formulas

$$(T_n f)(\tau) = n^{k-1} \sum_{\substack{ad=n \\ 0 \leq b < d}} d^{-k} f\left(\frac{a\tau + b}{d}\right) = \sum_{\substack{ad=n \\ 0 \leq b < d}} f|_k \left[\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right].$$

Proof. $f \leftrightarrow F \in V_k$ with $f(\tau) = F(\Lambda_\tau)$. By definition,

$$(T_n f)(\tau) = (T_n F)(\Lambda_\tau) = n^{k-1} \sum_{\Lambda' \underset{n}{\leq} \Lambda_\tau} F(\Lambda') = n^{k-1} \sum_{\substack{ad=n \\ 0 \leq b < d}} F(\mathbb{Z}(a\tau + b) \oplus \mathbb{Z}d).$$

This equals

$$n^{k-1} \sum_{a,b,d} F(d(\mathbb{Z}(\frac{a\tau + b}{d} \oplus \mathbb{Z}))) = n^{k-1} \sum_{a,b,d} d^{-k} F(\Lambda_{\frac{a\tau+b}{d}}) = n^{k-1} \sum_{a,b,d} d^{-k} f(\frac{a\tau + b}{d}).$$

For the second formula, recall that if $g \in GL_2(\mathbb{R})^+$, then $f|_k[g] = \det(g)^{k-1} f(g\tau) j(g,\tau)^{k-1}$, so

$$f|_k[\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}](\tau) = n^{k-1} f(\frac{a\tau + b}{d}) d^{-k}.$$

Hence $(T_n f)(\tau) = \sum_{a,b,d} f|_k[\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}]$. □

Corollary 3.8. If $f \in W_k$ and f is holomorphic, then $T_n f$ is also holomorphic.

Proof. Look at the formula above: $T_n f$ is a finite sum of holomorphic functions. □

Proposition 3.9. Let $f \in W_k$ be holomorphic in $\mathfrak{h}$ with q–expansion $f(\tau) = \sum_{m \in \mathbb{Z}} b_m q^m$. Then $T_n f$ has q–expansion $T_n f = \sum_{m \in \mathbb{Z}} c_m q^m$, where

$$c_m = \sum_{\substack{a \in \mathbb{N} \\ a|(m,n)}} a^{k-1} b_{(mn/a^2)}.$$

Proof.

$$\begin{aligned} T_n f =& n^{k-1} \sum_{\substack{ad=n \\ 0 \le b < d}} d^{-k} f(\frac{a\tau + b}{d}) = n^{k-1} \sum_{\substack{ad=n \\ 0 \le b < d}} \sum_{m \in \mathbb{Z}} b_m e^{2\pi i m a \tau/d} e^{2\pi i m b \tau/d} \\ =& n^{k-1} \sum_{ad=n} d^{-k} \sum_{m \in \mathbb{Z}} b_m e^{2\pi i m a \tau/d} \left(\sum_{0 \le b < d} e^{2\pi i m b/d} \right). \end{aligned}$$

Note that $\sum_{0 \le b < d} e^{2\pi i m b/d} = \begin{cases} d & d \mid m \\ 0 & \text{otherwise} \end{cases}$. Hence

$$T_n f = n^{k-1} \sum_{ad=n} d^{1-k} \sum_{m \in \mathbb{Z}} b_{dm} e^{2\pi i a m \tau}.$$

This gives

$$T_n f = \sum_{ad=n} \left(\frac{n}{d}\right)^{k-1} \sum_{m \in \mathbb{Z}} b_{dm} q^{am} = \sum_{a|n} a^{k-1} \sum_{m \in \mathbb{Z}} b_{nm/a} q^{am}.$$

This equals $\sum_{N \in \mathbb{Z}} c_N q^N$, where $c_N = \sum_{\substack{a|m \\ a|n}} a^{k-1} b_{nN/a^2}$. □

Theorem 3.10. T_n preserves the subspaces $S_k(\Gamma(1)) \le M_k(\Gamma(1)) \le W_k \forall n \ge 1$. Moreover, if $f \in M_k(\Gamma(1))$, then $a_0(T_n f) = \sigma_{k-1}(n) a_0(f)$ and $a_1(T_n f) = a_n(f)$.

Proof. To show that T_n preserves $M_k(\Gamma(1))$, we need to show that if $f \in M_k(\Gamma(1))$, then $T_n f$ is holomorphic in $\mathfrak{h}$ (then we're done by the previous corollary) and at ∞, i.e. $a_N(T_n f) = 0$ if $N < 0$.

But $a_N(T_n f) = \sum_{a|(m,n)} a^{k-1} a_{Nn/a^2}(f)$. Since $Nn/a^2 < 0$ and f is holomorphic at ∞, all summands are 0, so $T_n f$ is holomorphic at in ∞.

We have $a_0(T_n f) = \sum_{a|(n,0)} a^{k-1} a_{n\cdot 0/a^2}(f) = \sum_{a|n} a^{k-1} a_0(f) = \sigma_{k-1}(n) a_0(f)$.

Also $a_1(T_n f) = \sum_{a|(n,1)} a^{k-1} a_{n\cdot 1/a^2}(f) = a_n(f)$.

Finally, if $f \in S_k(\Gamma(1))$, then $a_0(f) = 0$, and then $T_n f \in M_k(\Gamma(1))$ and $a_0(T_n f) = \sigma_{k-1}(n) a_0(f) = 0 \implies T_n f \in S_k(\Gamma(1))$. □

Our next goal is to study the spectral decomposition of Hecke operators on $M_k(\Gamma(1))$, i.e. the decomposition of $M_k(\Gamma(1))$ as a sum of (simultaneous) generalized eigenspaces for the T_n.

The simplest case is when $M_k(\Gamma(1))$ or $S_k(\Gamma(1))$ is 1–dimensional (as then every nonzero element is an eigenvector). For example, $S_{12}(\Gamma(1))$ is 1–dimensional, spanned by $\Delta(\tau) = \sum_{n\geq 1} \tau(n) q^n$. So Δ is a T_n–eigenvector for all $n \geq 1$. If $T_n \Delta = \alpha_n \Delta$ for some $\alpha_n \in \mathbb{C}$, then $a_1(T_n\Delta) = a_1(\alpha_n \Delta) = \alpha_n a_1(\Delta) = \alpha_n$ (as we proved $a_1(\Delta) = 1$). But we also have $a_1(T_n\Delta) = a_n(\Delta) = \tau(n)$. Hence $\alpha_n =$ Hecke eigenvalue $= \tau(n) =$ coefficient of q^n.

Ramanujan conjectured in 1916 that τ is multiplicative and $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$ for p prime, $n \in \mathbb{N}$. These identities are true for Hecke operators (i.e. $T_{mn} = T_m T_n$ and $T_{p^{n+1}} = T_p T_{p^n} - p^{k-1} T_{p^{n-1}}$), hence also for the eigenvalues α_n, hence for the numbers $\tau(n)$.

27 Oct 2022, Lecture 10

Our goal now is to study the spectral decomposition of $M_k(\Gamma(1))$ and the arithmetic properties of Hecke eigenvalues.

Definition 3.3. If $f \in M_k(\Gamma(1))$, we say f is an **eigenform** is f is a T_n–eigenvector $\forall n \geq 1$.

We say f is a **normalized eigenform** if $a_1(f) = 1$.

Lemma 3.11. Suppose $k > 0$. Then any eigenform $f \in M_k(\Gamma(1))$ is a scalar multiple of a unique normalized eigenform. Moreover, if f is normalized, then $T_n(f) = a_n(f) f$ $\forall n \geq 1$. (In other words, the n^{th} Hecke eigenvalue = the n^{th} q–expansion coefficient).

For example, Δ is a normalized eigenform and $\tau(n)\Delta = T_n\Delta$.

Proof. We know $a_1(T_n f) = a_n(f)$. We need to show that if f is an eigenform, then $a_1(f) \neq 0$ (as then $f/a_1(f)$ is normalized). But if $a_1 = 0$ and α_n is the eigenvalue of T_n on f, then $a_n(f) = a_1(T_n f) = a_1(\alpha_n f) = \alpha_n a_1(f) = 0$ $\forall n \geq 1$.

Then $f = \sum_{n\geq 0} a_n(f)q^n = a_0(f)$, which is a contradiction as constants are not modular forms of weights $k > 0$.

If f is normalized, then $a_n(f) = a_1(T_n f) = a_1(\alpha_n f) = \alpha_n a_1(f) = \alpha_n$. $\square$

Proposition 3.12. Let $k \geq 4$ be even. Then $G_k(\tau)$ is an eigenform.

Proof. We need to show that G_k is a T_n–eigenvector $\forall n \geq 1$. We know T_n is a polynomial in T_p for p ranging over $p \mid n$ for p prime. Hence it is enough to show that G_k is a T_p–eigenvector $\forall p$ prime.

$G_k(\tau) = G_k(\Lambda_\tau)$ for $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$. Then

$$(T_pG_k)(\Lambda) = p^{k-1} \sum_{\Lambda' \underset{p}{\leq} \Lambda} G_k(\Lambda') = p^{k-1} \sum_{\Lambda' \underset{p}{\leq} \Lambda} \sum_{\lambda \in \Lambda' \setminus 0} \lambda^{-k} = p^{k-1} \sum_{\lambda \in \Lambda \setminus 0} a(\Lambda, \lambda)\lambda^{-k}$$

where $a(\Lambda, \lambda) = |\{\Lambda' \underset{p}{\leq} \Lambda \mid \lambda \in \Lambda'\}|$. We know that if $\Lambda' \underset{p}{\leq} \Lambda$, then $p\Lambda \leq \Lambda' \leq \Lambda$ and we have a bijection $\{\Lambda' \underset{p}{\leq} \Lambda\} \leftrightarrow \{H \leq \Lambda/p\Lambda \mid |H| = p\}$.

If $\lambda \in p\Lambda$, then $\{\Lambda' \underset{p}{\leq} \Lambda \mid \lambda \in \Lambda'\} = \{\Lambda' \underset{p}{\leq} \Lambda\}$, so $a(\Lambda, \lambda) = p + 1$.

If $\lambda \notin p\Lambda$, then $\lambda \neq 0$ modulo $p\Lambda$ and there exists a unique subgroup $H \leq \Lambda/p\Lambda$ of order p such that $\lambda \in H$. Hence in this case, $\{\Lambda' \underset{p}{\leq} \Lambda\} = \{\mathbb{Z}\lambda + p\Lambda\}$ and $a(\Lambda, \lambda) = 1$. Hence

$$(T_pG_k)(\Lambda) = p^{k-1} \sum_{\lambda \in \Lambda \setminus 0} \lambda^{-k} + p^{k-1} \sum_{\lambda \in p\Lambda \setminus 0} p\lambda^{-k}.$$

We get

$$(T_pG_k)(\Lambda) = p^{k-1} \sum_{\lambda \in \Lambda \setminus 0} \lambda^{-k} + p^{k-1} \sum_{\lambda \in \Lambda \setminus 0} p(p\lambda)^{-k} = p^{k-1}G_k(\Lambda) + G_k(\Lambda) = \sigma_{k-1}(p)G_k(\Lambda).$$

$\square$

We can compute the T_n–eigenvalues on G_k for all n now using $a_0(T_n f) = \sigma_{k-1}(n)a_0(f)$. So if f is an eigenform and $a_0(f) \neq 0$, then this forces the eigenvalue to be equal to $\sigma_{k-1}(n)$. So $T_nG_k = \sigma_{k-1}(n)G_k$ $\forall n \geq 1$. The q–expansion of G_k is $2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{n\geq 1} \sigma_{k-1}(n)q^n$ and we also defined $E_k(\tau) = 1 + \frac{(2\pi i)^k}{\zeta(k)(k-1)!} \sum_{n\geq 1} \sigma_{k-1}(n)q^n$. Hence $a_0(E_k) = 1$, but E_k is not a normalized eigenform. Hence the associated normalized eigenform is

$$F_k(\tau) = \frac{\zeta(k)(k-1)!}{(2\pi i)^k} + \sum_{n\geq 1} \sigma_{k-1}(n)q^n = \frac{-B_k}{2k} + \sum_{n\geq 1} \sigma_{k-1}(n)q^n = \frac{\zeta(1-k)}{2} + \sum_{n\geq 1} \sigma_{k-1}(n)q^n$$

(here we gave multiple equivalent expressions).

We have a decomposition $M_k(\Gamma(1)) = \mathbb{C}F_k \oplus S_k(\Gamma(1))$ (for $k \geq 4$). Both summands are T_n–invariant, so it's enough to study the action of T_n on S_k.

Remark. T_n do not usually respect multiplication. In particular, the product of eigenforms is not usually an eigenform. For example, $E_4^2 = E_8$, but $E_4^3 \in M_{12}(\Gamma(1)) = \mathbb{C}E_{12} \oplus \mathbb{C}\Delta$ requires both E_{12} and $\mathbb{C}$ to be expressed and hence is not an eigenform.

Proposition 3.13. If $f \in S_k(\Gamma(1))$ is a cuspidal eigenform, then all of the T_n–eigenvalues on f are algebraic integers. If f is normalized, then $\mathbb{Q}(\{a_n(f)\}_{n=1}^{\infty})$ has finite degree over $\mathbb{Q}$ (i.e. it is a number field).

Proof. We will show that for all $n \geq 1$, all eigenvalues of T_n on $S_k(\Gamma(1))$ are algebraic integers. We will do this by showing that the characteristic polynomial of T_n acting on S_k has integer coefficients (and it is of course monic).

We consider the basis $f_1, \ldots, f_N$ for $S_k(SL_2(\mathbb{Z}))$ characterized by:

- $\forall 1 \leq i \leq N$ and $\forall n \geq 1$, $a_n(f_i) \in \mathbb{Z}$.
- $\forall 1 \leq i, n \leq N$, $a_n(f_i) = \delta_{in}$.

Recall that this meant that $f_1, \ldots, f_N$ was the dual basis to the basis of functionals $a_1, \ldots, a_N$ of $S_k(\Gamma(1))^*$. Hence $\forall f \in S_k(\Gamma(1))$, $f = \sum_{i=1}^N a_i(f) f_i$ (this identity holds for any elements of a finite dimensional vector space with its basis and dual basis)

The claim is that if A denotes the matrix of T_n in the basis of $f_1, \ldots, f_N$, then A has integer entries. As the characteristic polynomial of T_n is $\det(X \cdot I - A)$, this will show that the characteristic polynomial has coefficients in $\mathbb{Z}$.

By definition, $T_n(j) = \sum_{i=1}^N A_{ij} f_i$. Then for $1 \leq m \leq N$,

$$a_m(T_n f_j) = \sum_{i=1}^N A_{ij} a_m(f_j) = \sum_{i=1}^N A_{ij} \delta_{im} = A_{mj}.$$

But $a_m(T_n f_j) = \sum_{a|(m,n)} a^{k-1} a_{mn/a^2}(f_j)$ by the formula from the last lecture. Note that each $a_{mn/a^2}(f_j)$ is in $\mathbb{Z}$ by the definition of f_j, so $\forall m, j$, $A_{mj} \in \mathbb{Z}$.

If f is a normalized eigenform, $f = \sum_{i=1}^N a_i(f) f_i$, then $\forall n \geq 1$, $a_n(f) = \sum_{i=1}^N a_i(f) \underbrace{a_n(f_i)}_{\in \mathbb{Z}}$. Hence $\mathbb{Q}(\{a_n(f)\}_{n \geq 1}) = \mathbb{Q}(\{a_n(f)\}_{n=1}^N)$ has finite degree over $\mathbb{Q}$. $\square$

30 Oct 2022, Lecture 11

We can use this argument to compute Hecke eigenvalues.

Example 3.1. Take $k = 24$. We will compute the eigenvalues of T_{24} acting on $S_{24}(\Gamma(1))$. $S_{24}(\Gamma(1))$ has a unique basis f_1, f_2 with $f_1 = q + O(q^3)$ and $f_2 = q^2 +$

$O(q^3)$. For any $f \in S_{24}(\Gamma(1))$, we have $f = a_1(f)f_1 + a_2(f)f_2$. So in particular, $T_2 f_1 = a_1(T_2 f_1)f_1 + a_2(T_2 f_1)f_2$. We know $a_m(T_n f) = \sum_{a|(m,n)} a^{k-1} a_{mn/a^2}(f)$, so

$$T_2 f_1 = a_1(T_2 f_1)f_1 + a_2(T_2 f_1)f_2 = a_2(f_1)f_1 + (a_4(f_1) + 2^{23}a_1(f_2))f_2 = (a_4(f_1) + 2^{23})f_2.$$

Similarly we get

$$T_2 f_2 = a_2(f_2)f_1 + (a_4(f_2) + 2^{23}a_1(f_2))f_2 = f_1 + a_4(f_2)f_2.$$

In fact,

$$\begin{aligned} f_1 &= \Delta E_6^2 + 1032\Delta^2 = q + 195660q^3 + 12080128q^4 + \dots \\ f_2 &= \Delta^2 = q^2 - 48q^3 + 1080q^4 + \dots \end{aligned}$$

So the matrix of f_2 is

$$\begin{pmatrix} 0 & 1 \\ 20468736 & 1080 \end{pmatrix},$$

so the eigenvalues of T_2 on $S_{24}(\Gamma(1))$ are $12(45 \pm \sqrt{144169})$. Hence $S_{24}(\Gamma(1))$ has a basis of normalized eigenforms g_1, g_2 with q–expansion coefficients in $K_{g_i} = \mathbb{Q}(\sqrt{144169})$ (sidenote: this is a prime number).

Definition 3.4. Let $f : \mathfrak{h} \to \mathbb{C}$ be a continuous function that is invariant under the weight 0 action of $\Gamma(1)$, i.e. $f(\gamma\tau) = f(\tau)\ \forall \gamma \in \gamma(1)$. We define

$$\int_{\Gamma(1)\backslash\mathfrak{h}} f(\tau)\frac{\mathrm{d}x\mathrm{d}y}{y^2} = \int_{\mathfrak{f}'} f(\tau)\frac{\mathrm{d}x\mathrm{d}y}{y^2}$$

(where $\tau = x + iy$).

The motivation for this is that the area form $\frac{\mathrm{d}x\wedge\mathrm{d}y}{y^2}$ on $\mathfrak{h}$ is invariant under $GL_2(\mathbb{R})^+$ (i.e. $g^*(\omega) = \omega\ \forall g \in GL_2(\mathbb{R})^+$). We'd like to say that $\Gamma(1) \setminus \mathfrak{h} \cong \mathbb{C}$ is a manifold where $\omega = \frac{\mathrm{d}x\mathrm{d}y}{y^2}$ descends to $\Gamma(1) \setminus \mathfrak{h}$, so we could use integration on manifolds. This has the following problems:

- We don't assume any knowledge of differential geometry. (In general, if we have a manifold (M, ω), then we have a volume form $\int_M \omega$).

- ω does not descend to $\Gamma(1) \setminus \mathfrak{h}$, because $\Gamma(1)/\{\pm I\}$ has fixed points in $\mathfrak{h}$. The solution for this is to choose a finite order subgroup $\Gamma \leq \Gamma(1)$ with no nontrivial elements of finite order. Then ω will descend to ω_Γ on $\Gamma \setminus \mathfrak{h}$ and $\frac{1}{[\Gamma(1):\Gamma]} \int_{\Gamma\setminus\mathfrak{h}} f\omega_\Gamma$ will be independent of the choice of Γ.

Lemma 3.14. Let $f, g \in S_k(\Gamma(1))$. Then the function $f(\tau)\overline{g(\tau)}\mathrm{Im}(\tau)^k$ is invariant under the weight 0 action of $\Gamma(1)$ and the integral

$$\int_{\Gamma(1)\backslash\mathfrak{h}} f(\tau)\overline{\gamma(\tau)}\mathrm{Im}(\tau)^k \frac{\mathrm{d}x\mathrm{d}y}{y^2}$$

converges absolutely.

Proof. If $\gamma \in \Gamma(1)$, $f(\gamma\tau) = f(\tau)j(\gamma,\tau)^k$ and $\mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}(\tau)}{|j(\gamma,\tau)|^2}$. So

$$f(\gamma\tau)\overline{g(\gamma\tau)}\mathrm{Im}(\gamma\tau)^k = f(\tau)\overline{g(\tau)}j(\gamma,\tau)^k\overline{j(\gamma,\tau)}^k\mathrm{Im}(\tau)^k\frac{1}{|j(\gamma,\tau)|^{2k}} = f(\tau)g(\tau)\mathrm{Im}(\tau)^k.$$

If $f(\tau) = \tilde{f}(q)$ for $\tilde{f} : D(0,1) \to \mathbb{C}$ holomorphic and vanishing at 0, then $\tilde{f}(q) = qh(q)$ for $h : D(0,1) \to \mathbb{C}$ holomorphic. Hence $\forall\delta \in (0,1)$, $\exists C_\delta > 0$ such that $|h(q)| \le C_\delta$ if $0 \le |q| \le \delta$. Hence $|\tilde{f}(q)| \le |q|C_\delta$ if $0 \le |q| \le \delta$.

So $\forall R \ge 0$, $\exists C_{f,R} > 0$ such that $\forall\tau \in \mathfrak{h}$ such that $\mathrm{Im}(\tau) \ge R$, $|f(\tau)| \le |q|C_{f,R} = e^{-2\pi\mathrm{Im}(\tau)}C_{f,R}$. So

$$\int_{\Gamma(1)\backslash\mathfrak{h}} \left|f(\tau)\overline{\gamma(\tau)}\mathrm{Im}(\tau)^k\right| \frac{\mathrm{d}x\mathrm{d}y}{y^2} \le \int_{\mathfrak{f}'} C_{f,\frac{\sqrt{3}}{2}}C_{g,\frac{\sqrt{3}}{2}}e^{-2\pi y}e^{-2\pi y}y^k\frac{\mathrm{d}x\mathrm{d}y}{y^2}.$$

Furthermore, $\mathfrak{f}' \subset \left\{x + iy \mid x \in \left[-\frac{1}{2},\frac{1}{2}\right], y \in \left[\frac{\sqrt{3}}{2},\infty\right)\right\}$. Hence our integral is

$$\le \int_{x=-\frac{1}{2}}^{\frac{1}{2}}\int_{y=\frac{\sqrt{3}}{2}}^{\infty} e^{-4\pi y}y^{k-2}\mathrm{d}x\mathrm{d}y = \int_{y=\frac{\sqrt{3}}{2}}^{\infty} e^{-4\pi y}y^{k-2}\mathrm{d}y < \infty.$$

□

Remark. The second part of the lemma does not hold if f, g are not assumed to be cuspidal.

Definition 3.5. The **Peterson inner product** on $S_k(\Gamma(1))$ is given by the formula

$$\langle f, g\rangle = \int_{\Gamma(1)\backslash\mathfrak{h}} f(\tau)\overline{g(\tau)}\mathrm{Im}(\tau)^k\frac{\mathrm{d}x\mathrm{d}y}{y^2}.$$

This is an inner product as $\langle f, f\rangle = \int_{\Gamma(1)\backslash\mathfrak{h}} |f(\tau)|^2\mathrm{Im}(\tau)^k\frac{\mathrm{d}x\mathrm{d}y}{y^2}$. So if $\langle f, f\rangle = 0$, then $|f|^2y^k = 0$, hence $f = 0$.

Theorem 3.15. For all $n \ge 1$, T_n is Hermitian with respect to the Peterson inner product, i.e. $\forall f, g \in S_k(\Gamma(1))$, $\langle T_nf, g\rangle = \langle f, T_ng\rangle$.

We will give a sketch proof of this next time.

Theorem 3.16. For all $k \ge 12$ even, there exists a basis $f_1, \ldots, f_N$ of normalized eigenforms for $S_k(\Gamma(1))$, unique up to reordering, with the following property:

$\forall 1 \leq i \leq N$, $K_{f_i} = \mathbb{Q}(\{a_n(f_i)\}_{n\geq 1})$ is a number field, contained in $\mathbb{R}$, and $\forall n \geq 1$, $a_n(f_i) \in \mathcal{O}_{K_{f_i}}$ (the algebraic integers in K_{f_i}).

Proof. We know from linear algebra that if $(V, (\cdot,\cdot))$ is an inner product space over $\mathbb{C}$, and $T : V \to V$ is a Hermitian endomorphism, then all eigenvalues of T are real and T is diagonalizable. We also know that if $A_1, A_2, A_3, \ldots$ is an infinite family of commuting Hermitian endomorphisms, then they can be diagonalized simultaneously. So in our case, we find a basis $f_1, \ldots, f_N$ of $S_k(\Gamma(1))$ of eigenforms, which we may assume are normalized. We only need to show that this basis is unique up to reordering , i.e. that all simultaneous eigenspaces are 1–dimensional. But if $f, g \in S_k(\Gamma(1))$ are normalized eigenforms with the same T_n–eigenvalues $\forall n \geq 1$, then $a_n(f) = a_n(g)$ $\forall n \geq 1 \implies f = g$. $\square$