M4P58 Modular Forms

Lectured by Dr David Helm
Typed by David Kurniadi Angdinata

Autumn 2019

Syllabus

Contents

0 Introduction

Lecture 1
Friday
04/10/19

The following are textbooks.

- Serre, A course in arithmetic, 1973
- J Shurman and F Diamond, A first course in modular forms, 2005

Let

$$f = q\prod_{n=1}^{\infty}\left(1-q^n\right)^2\left(1-q^{11n}\right)^2 = \sum_{n=1} b_n q^n = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 + \dots,$$

and let a_n be the number of solutions modulo n to the elliptic curve

$$E = \left\{(x,y) \in \mathbb{Z} \mid y^2 + y = x^3 - x^2 - 10x - 20\right\}.$$

- Modulo 2, there are $a_2 = 4$ solutions $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$.
- Modulo 3, there are $a_3 = 4$ solutions $(1,0)$, $(1,-1)$, $(-1,0)$, $(-1,-1)$.
- Modulo 5, there are $a_5 = 4$ solutions $(0,0)$, $(0,-1)$, $(1,0)$, $(-1,-1)$.
- Modulo 7, there are $a_7 = 9$ solutions $(1,3)$, $(2,2)$, $(2,-3)$, $(-1,1)$, $(-1,-2)$, $(-2,1)$, $(-2,-2)$, $(-3,1)$, $(-3,-2)$.

If $p \ne 11$, then

$$a_p - p = -b_p.$$

The following are some questions.

- What is the relationship between E and f?
- Can we find similar relationships for other E?
- How does one prove something like this?

Let

$$\mathbb{H} = \{x + iy \mid x, y \in \mathbb{R},\ y > 0\} \subseteq \mathbb{C}.$$

Then $\mathbb{H}$ has an action of

$$\mathrm{SL}_2(\mathbb{R}) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{R},\ ad - bc = 1\right\}.$$

Modular forms are complex functions on $\mathbb{H}$ with a high degree of symmetry. These functions are symmetric under the action of large discrete subgroups of $\mathrm{SL}_2(\mathbb{R})$, in particular

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{Z},\ ad - bc = 1\right\} \subseteq \mathrm{SL}_2(\mathbb{R}).$$

Why are these interesting to number theorists? Power series expansions often involve expressions of interest to number theorists. For example,

- Bernoulli numbers,
- divisor functions $\sigma_k(n) = \sum_{d \mid n} d^k$,
- number of points on elliptic curves, and
- traces of Galois representations.

1 Modular forms of level one

1.1 Modular forms

1.1.1 Modular actions

Let

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad a, b, c, d \in \mathbb{R}.$$

Then $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{C} \cup \{\infty\}$ by

$$\gamma \cdot z = \begin{cases} \dfrac{az+b}{cz+d} & z \ne -\dfrac{d}{c} \\ \infty & z = -\dfrac{d}{c} \end{cases} \qquad \gamma \cdot \infty = \frac{a}{c}.$$

One checks that this gives a bijection from $\mathbb{C} \cup \{\infty\}$ to $\mathbb{C} \cup \{\infty\}$, where inverse is given by the inverse matrix

$$\gamma^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

and $\gamma \cdot (\gamma' \cdot z) = \gamma\gamma' \cdot z$. One obtains a left action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{C} \cup \{\infty\}$. An observation is

$$\operatorname{Im} \gamma z = \operatorname{Im} \frac{az+b}{cz+d} = \operatorname{Im} \frac{(az+b)(c\overline{z}+d)}{|cz+d|^2} = \frac{\operatorname{Im}(az+b)(c\overline{z}+d)}{|cz+d|^2} = \frac{(ad-bc)\operatorname{Im} z}{|cz+d|^2}.$$

In particular, if $\gamma \in \mathrm{SL}_2(\mathbb{R})$, then Lecture 2 Friday 04/10/19

$$\operatorname{Im} \gamma z = \frac{\operatorname{Im} z}{|cz+d|^2}.$$

So $\mathrm{SL}_2(\mathbb{R})$ preserves $\mathbb{H} \cup \{\infty\}$. More generally, if $\gamma \in \mathrm{GL}_2(\mathbb{R})$, then

$$\operatorname{Im} \gamma z = \frac{\det \gamma \operatorname{Im} z}{|cz+d|^2}.$$

So

$$\mathrm{GL}_2(\mathbb{R})^+ = \{\gamma \in \mathrm{GL}_2(\mathbb{R}) \mid \det \gamma > 0\}$$

preserves $\mathbb{H} \cup \{\infty\}$. Define

$$f|_{k,\gamma} \ : \ \begin{array}{rcl} \mathbb{H} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \det \gamma^{k-1} f(\gamma z)(cz+d)^{-k} \end{array}, \qquad f : \mathbb{H} \to \mathbb{C}, \qquad \gamma \in \mathrm{GL}_2(\mathbb{R})^+, \qquad k \in \mathbb{Z},$$

where $\det \gamma^{k-1}$ is the fudge factor, which is one for $\gamma \in \mathrm{SL}_2(\mathbb{R})$, and $(cz+d)^{-k}$ is the twisted action on functions. Check that

$$f|_{k,\mathrm{id}} = f, \qquad \left(f|_{k,\gamma}\right)\Big|_{k,\gamma'} = f|_{k,\gamma'\gamma}.$$

This gives, for each k, a left action of $\mathrm{GL}_2(\mathbb{R})^+$ on functions $\mathbb{H} \to \mathbb{C}$, a **modular action of weight** k. A modular form of weight k will be a sufficiently nice function $f : \mathbb{H} \to \mathbb{C}$ such that $f|_{k,\gamma} = f$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. That is, for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathbb{H}$,

$$f(\gamma z)(cz+d)^{-k} = f(z), \qquad \implies \qquad f(\gamma z) = f(z)(cz+d)^k,$$

the **modular transformation law of weight** k. The following are some observations.

- Let $k = 0$. Then constant functions satisfy $f(\gamma z) = f(z)$. It will turn out that all functions of weight zero are constant.
- Let k be odd, and $\gamma = -\mathrm{id}$. Then $\gamma z = z$ for all z and $cz + d = -1$, so $f(\gamma z) = f(z)(cz+d)^k$ gives $f(z) = f(z)(-1)^k$, so $f(z) = -f(z)$, so $f(z) = 0$ for all z. So no non-zero functions $f : \mathbb{H} \to \mathbb{C}$ satisfy the modular transformation law of weight k, for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, when k is odd.

1.1.2 Review of complex analysis

Let $f : U \to \mathbb{C}$, for $U \subseteq \mathbb{C}$ open, and let $p \in U$.

Definition 1.1.1. f is **holomorphic** at p if

$$f'(p') = \lim_{\epsilon \to 0,\ \epsilon \in \mathbb{C}} \frac{f(p'+\epsilon) - f(p')}{\epsilon}$$

exists for all p' in a neighbourhood of p.

Proposition 1.1.2. *f is holomorphic at p implies that f is continuous.*

Proposition 1.1.3. *f is holomorphic at p implies that f is infinitely differentiable at p, that is $f^{(n)}(p)$ exists for all $n \ge 0$. Moreover, we have*

$$f(z) = \sum_{n=0}^{\infty} \frac{f^{(n)}(p)}{n!} (z-p)^n = f(p) + f'(p)(z-p) + \frac{f'(p)}{2} (z-p)^2 + \dots,$$

for all z in a neighbourhood of p.

Corollary 1.1.4. *If f is holomorphic and not identically zero on an open set U, then the zeroes of f are isolated on U.*

More generally is the following.

Definition 1.1.5. f is **meromorphic** at p if there exists a neighbourhood U of p and $g, h : U \to \mathbb{C}$ holomorphic on U such that $f = g/h$ on $U \setminus \{p\}$. Such an f has a **Laurent series expansion** at p,

$$f(z) = \sum_{i=-N}^{\infty} c_i (z-p)^i.$$

The smallest i such that $c_i \neq 0$ is denoted by $\mathrm{ord}_p f$, the **order of vanishing** of f at p.

- If $\mathrm{ord}_p f = -n$ for $n > 0$, we say f has a **pole of order** n.
- If $\mathrm{ord}_p f = n$ for $n > 0$, we say f has a **zero of order** n.

Proposition 1.1.6.

- $\mathrm{ord}_p fg = \mathrm{ord}_p f + \mathrm{ord}_p g$.
- $\mathrm{ord}_p (f+g) \ge \min\{\mathrm{ord}_p f, \mathrm{ord}_p g\}$, *with equality if* $\mathrm{ord}_p f \neq \mathrm{ord}_p g$.

If f is holomorphic on $U \setminus \{p\}$ for U a neighbourhood of p, then f may or may not be meromorphic at p.

Example. $f(z) = e^{-1/z^2}$ is holomorphic on $\mathbb{C} \setminus \{0\}$, but not meromorphic at zero.

Theorem 1.1.7. *Let f be holomorphic on $U \setminus \{p\}$, and there exists $n > 0$ such that*

$$\lim_{x \to p} (x-p)^n f(x)$$

exists. Then f is meromorphic on U, and $\mathrm{ord}_p f \ge -n$.

1.1.3 Modular forms

Definition 1.1.8. $f : \mathbb{H} \to \mathbb{C}$ is a **weakly modular function of weight** k if

- f is meromorphic on $\mathbb{H}$, and
- f satisfies the modular transformation law of weight k.

Consider

$$\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

so $\gamma z = z + 1$ and $cz + d = 1$. The modular transformation law gives $f(z+1) = f(z)$. Let

$$\mathrm{D} = \{q \mid |q| < 1\}.$$

Can define a function

$$\begin{array}{rccc} g & : & \mathrm{D} \setminus \{0\} & \longrightarrow & \mathbb{C} \\ & & q & \longmapsto & f\left(\dfrac{\log q}{2\pi i}\right) \end{array},$$

that is $f(z) = g\left(e^{2\pi i z}\right)$ for $z \in \mathbb{H}$, where g is holomorphic or meromorphic on $\{z \mid 0 < |z| < 1\}$ if and only if f is holomorphic or meromorphic on $\mathbb{H}$.

Definition 1.1.9. $f : \mathbb{H} \to \mathbb{C}$ is a **modular form of weight** k if

1. f satisfies the modular transformation law of weight k,
2. f is holomorphic on $\mathbb{H}$, and
3. f is holomorphic at ∞, so the function $g : \mathrm{D} \setminus \{0\} \to \mathbb{C}$, which is holomorphic on $\mathrm{D} \setminus \{0\}$ by 2, extends to a holomorphic function on D.

Then $q \to 0$ in D if and only if $\operatorname{Im} z \to +\infty$. Then 3 means $g(q)$ is bounded as $q \to 0$ so $f(z)$ is bounded as $\operatorname{Im} z \to +\infty$. For f satisfying 3, $g : \mathrm{D} \setminus \{0\} \to \mathbb{C}$ has a series expansion

$$g(q) = \sum_n a_n q^n = a_0 + a_1 q + \dots$$

in $q = e^{2\pi i z}$. We call this the **q-expansion** for f.

Lecture 3 Monday 07/10/19

Definition 1.1.10. $f : \mathbb{H} \to \mathbb{C}$ is a **meromorphic modular form of weight** k if the same conditions 1 to 3 hold, but with holomorphic weakened to meromorphic.

Note. If f is only meromorphic at ∞ then a finite number of negative powers of q can appear.

Example.

- The **modular discriminant**

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \dots$$

  is a modular form of weight 12.

- The j**-invariant**

$$\mathrm{j}(z) = \frac{1}{q} + 744 + 196844q + 21493760q^2 + \dots$$

  is a meromorphic modular form of weight 0.

1.1.4 Lattice functions

How can we construct modular forms?

Definition 1.1.11. A **lattice** in $\mathbb{C}$ is an abelian subgroup of $\mathbb{C}$ of the form $\mathbb{Z}w_1 + \mathbb{Z}w_2$, where $w_1, w_2 \in \mathbb{C}$ are $\mathbb{R}$-linearly independent. More generally if V is an $\mathbb{R}$-vector space, a **lattice** L in V is a discrete abelian subgroup of V that spans V over $\mathbb{R}$. For $L \subseteq \mathbb{C}$ a lattice and $\lambda \in \mathbb{C}^\times$, let

$$\lambda L = \{\lambda x \mid x \in L\} \subseteq \mathbb{C}.$$

We say that L and λL are **homothetic**. For $z \in \mathbb{H}$, let

$$\mathrm{L}_{z,1} = \mathbb{Z} + \mathbb{Z}z = \{az + b \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

A question is when is $\mathrm{L}_{z,1}$ homothetic to $\mathrm{L}_{z',1}$, and what is a homothety factor?

- Suppose $\mathrm{L}_{z,1} = \lambda \mathrm{L}_{z',1}$. Then there exist a, b, c, d such that $\lambda z' = az + b$ and $\lambda = cz + d$, so

$$\begin{pmatrix} \lambda z' \\ \lambda \end{pmatrix} = \gamma \begin{pmatrix} z \\ 1 \end{pmatrix}. \tag{1}$$

  On the other hand there exist a', b', c', d' such that $z = a'\lambda z' + b'\lambda$ and $1 = c'\lambda z' + d'\lambda$, so

$$\gamma' \begin{pmatrix} \lambda z' \\ \lambda \end{pmatrix} = \begin{pmatrix} z \\ 1 \end{pmatrix}. \tag{2}$$

  Then (1) and (2) imply that

$$\gamma'\gamma \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} z \\ 1 \end{pmatrix},$$

  so $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Moreover (1) implies that $z' = (az + b) / (cz + d)$.

- Conversely, if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then $\gamma z = (az + b) / (cz + d)$, so

$$\mathrm{L}_{\gamma z,1} = (cz + d)^{-1} \mathrm{L}_{az+b,cz+d}.$$

  But certainly $\mathrm{L}_{az+b,cz+d} \subseteq \mathrm{L}_{z,1}$. On the other hand if γ' is inverse to γ,

$$\begin{pmatrix} z \\ 1 \end{pmatrix} = \gamma'\gamma \begin{pmatrix} z \\ 1 \end{pmatrix} = \gamma \begin{pmatrix} az + b \\ cz + d \end{pmatrix} = \begin{pmatrix} a'(az + b) + b'(cz + d) \\ c'(az + b) + d'(cz + d) \end{pmatrix},$$

  so $z \in \mathrm{L}_{az+b,cz+d}$ and $1 \in \mathrm{L}_{az+b,cz+d}$. So $\mathrm{L}_{az+b,cz+d} = \mathrm{L}_{z,1}$, so $\mathrm{L}_{\gamma z,1} = (cz + d)^{-1} \mathrm{L}_{z,1}$.

Definition 1.1.12. A **lattice function of weight** k is a function $F : \{\text{lattices in } \mathbb{C}\} \to \mathbb{C}$ such that

$$F(\lambda L) = \lambda^{-k} F(L),$$

for all lattices L. Given such an F, can define

$$\begin{array}{rccc} f & : & \mathbb{H} & \longrightarrow & \mathbb{C} \\ & & z & \longmapsto & F(\mathrm{L}_{z,1}) \end{array}.$$

If F has weight k, then

$$f(\gamma z) = F(\mathrm{L}_{\gamma z,1}) = F\left((cz + d)^{-1} \mathrm{L}_{z,1}\right) = (cz + d)^k F(\mathrm{L}_{z,1}) = (cz + d)^k f(z).$$

1.2 Eisenstein series

1.2.1 Eisenstein series

Lecture 4 Friday 11/10/19

Definition 1.2.1. For $L \in \mathbb{C}$, define the **Eisenstein series**

$$\mathrm{G}_k(L) = \sum_{w \in L,\ w \neq 0} \frac{1}{w^k}, \qquad \mathrm{g}_k(z) = \mathrm{G}_k(\mathrm{L}_{z,1}) = \sum_{\substack{m=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k}.$$

Then

$$\mathrm{G}_k(\lambda L) = \sum_{w' \in \lambda L,\ w' \neq 0} \frac{1}{w'^k} = \sum_{w \in L,\ w \neq 0} \frac{1}{(\lambda w)^k} = \lambda^{-k} \mathrm{G}_k(L).$$

Corollary 1.2.2. g_k *satisfies the modular transformation law of weight* k.

The following are some questions.

- Does G_k, or g_k, converge?
- Is g_k holomorphic or meromorphic on $\mathbb{H}$?
- Is g_k holomorphic at ∞?
- What is the q-expansion of g_k?

1.2.2 Convergence and holomorphy on $\mathbb{H}$

Definition 1.2.3. Let $U \subseteq \mathbb{C}$ be open. A sequence of functions $f_n : U \to \mathbb{C}$ **converges uniformly on compact sets** to f if for all $C \subseteq U$ compact and $\epsilon > 0$, there exists $N \in \mathbb{Z}$ such that for all $n > N$,

$$|f(z) - f_n(z)| < \epsilon, \qquad z \in C.$$

Theorem 1.2.4. *A uniform limit of holomorphic functions is holomorphic. If f_n converges to f uniformly on compact sets and f_n is holomorphic on U, then f is holomorphic on U.*

Theorem 1.2.5. *Let $k \geq 4$. The series $\mathrm{g}_k(z)$ converges absolutely and uniformly on compact subsets of $\mathbb{H}$.*

Proof. Let

$$P_{z,r} = \{az + b \mid a, b \in \mathbb{R},\ \max(|a|, |b|) = r\} \subseteq \mathbb{C},$$

so $P_{z,r} = rP_{z,1}$, and there are $8r$ points on $P_{z,r} \cap \mathrm{L}_{z,1}$. Then

$$\mathrm{g}_k(z) = \sum_{r=1}^{\infty} \sum_{w \in \mathrm{L}_{z,1} \cap P_{z,r}} \frac{1}{w^k}.$$

The function $z \mapsto |z|$ attains a non-zero minimum $\delta(z)$ on $P_{z,1}$, so on $P_{z,1}$, have $|z| > \delta(z)$, so $1/|z|^k < 1/\delta(z)^k$. On $P_{z,r}$, have $|z| > r\delta(z)$, so $1/|z|^k < 1/r^k\delta(z)^k$. Let $C \subseteq \mathbb{H}$ be compact. Then $z \mapsto \delta(z)$ is a continuous function on C and attains a minimum δ_C. For all $z \in C$ and all $w \in P_{z,r}$, get $|w| > r\delta_C$, so

$$\frac{1}{|w|^k} < \frac{1}{r^k \delta_C^k}.$$

Thus for $z \in C$, $\mathrm{g}_k(z)$ is dominated by

$$\sum_{r=1}^{\infty} \frac{8r}{r^k \delta_C^k} = \frac{8}{\delta_C^k} \sum_{r=1}^{\infty} \frac{1}{r^{k-1}},$$

which converges absolutely for $k \geq 4$. ∎

Corollary 1.2.6. $\mathrm{g}_k(z)$ *is holomorphic on* $\mathbb{H}$.

1.2.3 q-expansion and holomorphy at ∞

The idea is to understand series of the form

$$\sum_{n=-\infty}^{\infty} \frac{1}{(z+n)^k}.$$

Theorem 1.2.7. *A bounded holomorphic function on all of $\mathbb{C}$ is constant.*

Lemma 1.2.8.

1.

$$\frac{\pi^2}{\sin^2 \pi z} = \sum_{n=-\infty}^{\infty} \frac{1}{(z-n)^2} = \sum_{n=-\infty}^{\infty} \frac{1}{(z-n)^2}.$$

2.

$$\pi \cot \pi z = \frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z-n} + \frac{1}{z+n} \right) = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2-n^2}.$$

Proof.

1. The right hand side converges absolutely and uniformly on compact subsets of $\mathbb{C} \setminus \mathbb{Z}$, so the right hand side is holomorphic on $\mathbb{C} \setminus \mathbb{Z}$. Locally around $z = n$, the series looks like

$$\sum_{n=-\infty}^{\infty} \frac{1}{(z-n)^2} = \dots + \frac{1}{(z-n+1)^2} + \frac{1}{(z-n)^2} + \frac{1}{(z-n-1)^2} + \dots = \frac{1}{(z-n)^2} + h_1(z),$$

where $h_1(z)$ is holomorphic in a neighbourhood of $z = n$. Similarly, the left hand side is meromorphic on $\mathbb{C}$, and the Laurent series near $z = n$ is

$$\frac{\pi^2}{\sin^2 \pi z} = \pi \left(\frac{1}{\pi^2 (z-n)^2} + \frac{1}{3} + \frac{1}{15} \pi^2 (z-n)^2 + \dots \right) = \frac{1}{(z-n)^2} + h_2(z),$$

where $h_2(z)$ is a holomorphic function. So the difference

$$g(z) = \sum_{n=-\infty}^{\infty} \frac{1}{(z-n)^2} - \frac{\pi^2}{\sin^2 \pi z}$$

is meromorphic on $\mathbb{C}$ and holomorphic on $\mathbb{C} \setminus \mathbb{Z}$, and the Laurent expression around $z = n$ is

$$g(z) = \frac{1}{(z-n)^2} + h_1(z) - \left(\frac{1}{(z-n)^2} + h_2(z) \right) = h_1(z) - h_2(z),$$

so $g(z)$ is holomorphic at $z = n$ for all n. Consider $t \to \pm\infty$ for $z = a + it$. The right hand side is

$$R = \sum_{n=-\infty}^{\infty} \frac{1}{(z-n)^2} = \sum_{n=a-N}^{a+N} \frac{1}{(z-n)^2} + \sum_{n=-\infty}^{a-N-1} \frac{1}{(z-n)^2} + \sum_{n=a+N+1}^{\infty} \frac{1}{(z-n)^2} = R_0 + R_- + R_+,$$

where R_0 has finitely many terms that converge to less than $\epsilon/2$ as $t \to \pm\infty$ and $R_- + R_+ < \epsilon/2$ for $N \gg 0$ independent of t, so $R < \epsilon$ converges to zero. Similarly, the left hand side is

$$\left| \frac{\pi^2}{\sin^2 \pi z} \right| = \left| \frac{2\pi^2}{e^{\pi i z} - e^{-\pi i z}} \right| \to 0,$$

so $\lim_{t\to\infty} g(a+it) = 0$. Moreover, $g(z+1) = g(z)$ for all z. Then

$$S = \{ z \in \mathbb{C} \mid n-1 \le \operatorname{Re} z \le n, \ -N \le \operatorname{Im} z \le N \}, \qquad n \in \mathbb{Z}$$

is compact, so $|g(z)|$ attains a maximum in S, so $g(z)$ is bounded in S. Since $g(z)$ is also bounded in $R_- + R_+$, $g(z)$ is bounded in $\mathbb{C}$, so g is constant. Since $\lim_{t\to\infty} g(a+it) = 0$, $g = 0$.

2. Check that the right hand side converges absolutely and uniformly on compact subsets of $\mathbb{C} \setminus \mathbb{Z}$, so the right hand side is meromorphic on $\mathbb{C} \setminus \mathbb{Z}$. Similarly, the left hand side is also meromorphic on $\mathbb{C} \setminus \mathbb{Z}$. Comparing derivatives, Lecture 5 Friday 11/10/19

$$-\frac{\pi^2}{\sin^2 \pi z} = -\frac{1}{z^2} - \sum_{n=1}^{\infty} \left(\frac{1}{(z-n)^2} + \frac{1}{(z+n)^2} \right),$$

so the difference is constant. Let $z = \frac{1}{2}$. The left hand side is $\pi \cot \pi/2 = 0$ and the right hand side is

$$\frac{2}{1} + \left(-\frac{2}{1} + \frac{2}{3} \right) + \left(-\frac{2}{3} + \frac{2}{5} \right) + \dots \to 0, \qquad n \to \infty,$$

so the difference is zero.

□

Thus

$$\frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z-n} + \frac{1}{z+n} \right) = \pi \cot \pi z = \pi i \frac{e^{\pi i z} + e^{-\pi i z}}{e^{\pi i z} - e^{-\pi i z}} = \pi i \frac{q+1}{q-1} = \pi i - \frac{2\pi i}{1-q} = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n.$$

Take $\frac{\mathrm{d}^{k-1}}{\mathrm{d}z^{k-1}}$. For $k \ge 2$ even, get

$$-(k-1)! \sum_{n=-\infty}^{\infty} \frac{1}{(z+n)^k} = -(2\pi i)^k \sum_{n=1}^{\infty} n^{k-1} q^n,$$

so

$$\sum_{n=-\infty}^{\infty} \frac{1}{(z+n)^k} = \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^n.$$

Collecting powers of q,

$$\begin{aligned} \mathrm{g}_k(z) &= \sum_{\substack{m=-\infty \\ (m,n)\ne(0,0)}}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k} \\ &= 2 \sum_{n=1}^{\infty} \frac{1}{n^k} + 2 \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k} \\ &= 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} n^{k-1} q^{nm} && \zeta(s) = \sum_{n=1}^{\infty} n^{-s} \\ &= 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n && \sigma_{k-1}(n) = \sum_{d \mid n,\ d>0} d^{k-1}. \end{aligned}$$

Corollary 1.2.9. *$\mathrm{g}_k(z)$ is holomorphic at ∞. In particular, g_k is a modular form of weight k.*

1.2.4 Bernoulli numbers

Definition 1.2.10. The **Bernoulli numbers** b_k are defined by

$$\sum_{k=0}^{\infty} \mathrm{b}_k \frac{x^k}{k!} = \frac{x}{e^x - 1},$$

a formal power series with rational coefficients.

Then

$$\mathrm{b}_0 = 1, \quad \mathrm{b}_1 = -\tfrac{1}{2}, \quad \mathrm{b}_2 = \tfrac{1}{6}, \quad \mathrm{b}_3 = 0, \quad \mathrm{b}_4 = -\tfrac{1}{20}, \quad \dots, \quad \mathrm{b}_{2k} \in \mathbb{Q}, \quad \mathrm{b}_{2k+1} = 0, \quad \dots.$$

Proposition 1.2.11. *For all even k,*

$$\zeta(k) = -\mathrm{b}_k \frac{(2\pi i)^k}{2k!}.$$

Proof. On one hand,

$$\pi z \cot \pi z = \pi i z + \frac{2\pi i z}{e^{2\pi i z} - 1} = \pi i z + \sum_{k=0}^{\infty} \mathrm{b}_k \frac{(2\pi i z)^k}{k!}.$$

On the other hand,

$$\begin{aligned} \pi \cot \pi z &= \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2 - n^2} = \frac{1}{z} - \frac{2z}{n^2} \sum_{n=1}^{\infty} \frac{1}{1 - z^2/n^2} \\ &= \frac{1}{z} - \sum_{n=1}^{\infty} \frac{2}{z} \sum_{k=1}^{\infty} \left(\frac{z^2}{n^2}\right)^k = \frac{1}{z} - \frac{2}{z} \sum_{k=1}^{\infty} z^{2k} \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \frac{1}{z} - \frac{2}{z} \sum_{k=1}^{\infty} \zeta(2k) z^{2k}, \end{aligned}$$

so

$$\pi i z + \sum_{k=0}^{\infty} \mathrm{b}_k \frac{(2\pi i z)^k}{k!} = \pi z \cot \pi z = 1 - 2 \sum_{k=1}^{\infty} \zeta(2k) z^{2k}.$$

Comparing,

$$\mathrm{b}_{2k} \frac{(2\pi i)^{2k}}{(2k)!} = -2\zeta(2k),$$

get the desired formula. ☐

So

$$\mathrm{g}_k(z) = \frac{-\mathrm{b}_k (2\pi i)^k}{k!} + \frac{2(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Set the **normalised Eisenstein series**

$$\mathrm{E}_k = \frac{\mathrm{g}_k}{2\zeta(k)} = 1 - \frac{2k}{\mathrm{b}_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Example.

$$\mathrm{E}_4 = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n, \qquad \mathrm{E}_6 = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n,$$

$$\mathrm{E}_8 = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n, \qquad \mathrm{E}_{12} = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n.$$

Lecture 6 Monday 14/10/19

An observation is if f is modular of weight k and g is modular of weight k', then fg is modular of weight $k + k'$, and if $k = k'$, then $f + g$ is modular of weight k.

Example. Important examples.

- The **modular discriminant**

  $$\Delta(z) = \frac{\mathrm{E}_4 - \mathrm{E}_6^2}{1728} = q - 24q^2 + 252q^3 + \dots$$

  is a modular form of weight 12.

- The j**-invariant**

  $$\mathrm{j}(z) = \frac{\mathrm{E}_4^3}{\Delta} = \frac{1}{q} + 744 + 196844q + \dots$$

  is a meromorphic modular form of weight 0.

1.3 Controlling modular forms

1.3.1 The fundamental domain

The idea is to control the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$. If $f : \mathbb{H} \to \mathbb{C}$ satisfies $f(\gamma z) = (cz+d)^k f(z)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, and if $D \subseteq \mathbb{H}$ such that D meets every $\mathrm{SL}_2(\mathbb{Z})$-orbit in $\mathbb{H}$, then f is determined by its values on D.

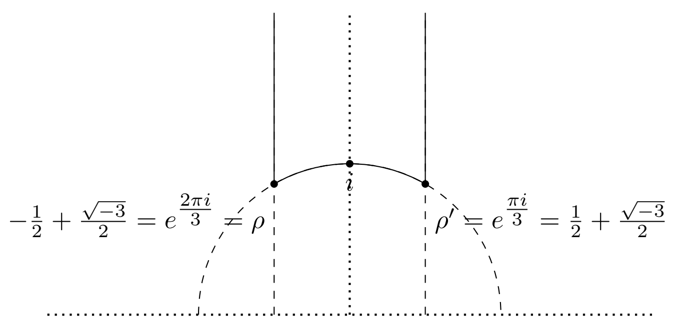
Definition 1.3.1. Let G be a group acting continuously on a complex analytic space X, such as $X = \mathbb{H}$. A subset $D \subseteq X$ is a **fundamental domain** for the action of G if

- D meets every G-orbit in X,
- the subset $\{x \in D \mid \exists g \in G,\ gx \in D,\ gx \neq x\}$ has measure zero, and
- D is closed in X.

Define

$$\mathcal{D} = \left\{z \in \mathbb{H} \;\middle|\; \tfrac{1}{2} \leq \operatorname{Re} z \leq \tfrac{1}{2},\, |z| \geq 1\right\} \subseteq \mathbb{H},$$

so



Let

$$\mathrm{S} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : z \mapsto -\frac{1}{z}, \qquad \mathrm{T} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : z \mapsto z+1,$$

and let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be the subgroup generated by S and T. We will see later that $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Theorem 1.3.2.

1. *For all $z \in \mathbb{H}$, there exists $\gamma \in \Gamma$ such that $\gamma z \in \mathcal{D}$.*
2. *Suppose $z, z' \in \mathcal{D}$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma z = z'$. Then either*
   - $z = z'$,
   - $\operatorname{Re} z = \pm\frac{1}{2}$ *and* $z' = z \mp 1$, *or*
   - $|z| = 1$ *and* $z' = -1/z$.

   In particular, if $z \neq z'$, then z and z' are on the boundary of $\mathcal{D}$.
3. *For $z \in \mathcal{D}$, let I_z be the stabiliser of z in $\mathrm{SL}_2(\mathbb{Z})$, that is*

   $$\mathrm{I}_z = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma z = z\}.$$

   Then $\mathrm{I}_z = \{\pm \mathrm{I}\}$ unless
   - $z = i$, *where* $\mathrm{I}_z = \{\pm\mathrm{I}, \pm\mathrm{S}\}$,
   - $z = \rho$, *where* $\mathrm{I}_z = \left\{\pm\mathrm{I}, \pm(\mathrm{ST}), \pm\left(\mathrm{T}^{-1}\mathrm{S}\right)\right\}$, *or*
   - $z = \rho'$, *where* $\mathrm{I}_z = \left\{\pm\mathrm{I}, \pm(\mathrm{TS}), \pm\left(\mathrm{ST}^{-1}\right)\right\}$.

Corollary 1.3.3. $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Proof. Fix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathring{\mathcal{D}}$ so $\mathrm{SL}_2(\mathbb{Z})\, z \cap \mathcal{D} = \{z\}$ and $\mathrm{I}_z = \{\pm\mathrm{I}\}$. Consider γz. There exists $\gamma' \in \Gamma$ such that $\gamma'\gamma z \in \mathcal{D}$, so $\gamma'\gamma z = z$. So $\gamma'\gamma = \pm\mathrm{I}$, so $\gamma = \pm\gamma'^{-1}$. But $\gamma'^{-1} \in \Gamma$ and $-\mathrm{I} = \mathrm{S}^2 \in \Gamma$, so $\gamma \in \Gamma$. $\square$

Proof of Theorem 1.3.2. Recall $\operatorname{Im}\gamma z = \operatorname{Im} z / |cz+d|^2$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

1. As c and d vary, $\{cz+d\}$ forms a lattice in $\mathbb{C}$, so there exist only finitely many c and d such that $|cz+d| < 1$. So $\operatorname{Im}\gamma z$ attains a maximum as γ varies over Γ, so there exists $\gamma \in \Gamma$ such that $\operatorname{Im}\gamma z$ is maximal. There exists $n \in \mathbb{Z}$ such that $\mathrm{T}^n\gamma z$ has real part between $-\frac{1}{2}$ and $\frac{1}{2}$. Consider $|\mathrm{T}^n\gamma z|$. If this is less than one, then
$$\operatorname{Im} \mathrm{ST}^n\gamma z = \operatorname{Im}\frac{-1}{\mathrm{T}^n\gamma z} > \operatorname{Im}\mathrm{T}^n\gamma z = \operatorname{Im}\gamma z.$$
Since $\mathrm{ST}^n\gamma \in \Gamma$, this contradicts maximality so $|\mathrm{T}^n\gamma z| \geq 1$, so $\mathrm{T}^n\gamma z \in \mathcal{D}$. Lecture 7 Friday 18/10/19

2, 3. Let $z, z' \in \mathcal{D}$ such that $\gamma z = z'$. Without loss of generality $\operatorname{Im} z' \geq \operatorname{Im} z$, so $|cz+d| \leq 1$. Note that $|cz+d| \geq \operatorname{Im}(cz+d) \geq \frac{\sqrt{3}}{2}c$, so $c = -1, 0, 1$. Note that can replace γ with $-\gamma$ if convenient.

   $c = 0$. Then $ad = 1$, so can assume $a = d = 1$, so $\gamma z = z + b$. Since $z, z+b \in \mathcal{D}$, $b = \pm 1$ and $\operatorname{Re} z = \mp\frac{1}{2}$.

   $c = 1$. Have $|z+d| \leq 1$ and $|z| \geq 1$, so $d = -1, 0, 1$.

   - $d = 0$. Then $|z| = 1$, and $\gamma z = (az-1)/z = a - 1/z$. The only possibilities are
     * $a = 0$ and $\gamma = \mathrm{S}$,
     * $a = 1$ and $\gamma = \mathrm{TS}$, so $z = \rho'$, or
     * $a = -1$ and $\gamma = \mathrm{T}^{-1}\mathrm{S}$, so $z = \rho$.
   - $d = 1$. Then $z = \rho$, and $\gamma z = ((b+1)z + b)/(z+1) = b + 1 - 1/(z+1)$, so $b = 0$ or $b = -1$.
   - $d = -1$. Then $z = \rho'$ is similar.

   $c = -1$. Similar.

□

1.3.2 Further review of complex analysis

Recall that on any compact set, a meromorphic function has only finitely many zeroes and poles. If $f(z) = g\left(e^{2\pi i z}\right)$ is meromorphic at infinity and g is meromorphic on $\mathrm{D} = |q| < 1$, zeroes and poles of g are discrete with respect to q, and $\operatorname{Im} z \gg 0$ if and only if $|q| < \epsilon$.

Definition 1.3.4. Let $U \subseteq \mathbb{C}$ be open, and let $f : U \to \mathbb{C}$ be meromorphic on U. If f has a pole at p, can write
$$f(z) = \sum_{n=\operatorname{ord}_p f<0}^{\infty} a_n (z-p)^n.$$
The coefficient a_{-1} is called the **residue** $\operatorname{Res}_p f$ of f at p.

Theorem 1.3.5 (Residue theorem)**.** *Let V be a region in $\mathbb{C}$ whose boundary ∂V is a simple closed curve. Then*
$$\frac{1}{2\pi}\int_{\partial V} f(z)\,\mathrm{d}z = \sum_{p\in V \ \text{pole of } f} \operatorname{Res}_p f.$$

Definition 1.3.6. Let f be meromorphic on $U \subseteq \mathbb{C}$ open. Then the **logarithmic derivative** $\mathrm{d}\log f$ is the function f'/f.

If $f(z) = c_n(z-p)^n + c_{n+1}(z-p)^{n+1} + \dots$, then if $n \neq 0$, then the leading term of f' is $nc_n(z-p)^{n-1}$ and the leading term of f is $c_n(z-p)^n$, so the leading term of f'/f is $n(z-p)^{-1}$. If $n = 0$, then f'/f is holomorphic. So f'/f is meromorphic with simple poles precisely at the points where $\operatorname{ord}_p f \neq 0$, and $\operatorname{Res}_p f'/f$ at such p is $\operatorname{ord}_p f$.

Theorem 1.3.7 (Argument principle)**.**
$$\frac{1}{2\pi i}\int_{\partial V}\frac{f'(z)}{f(z)}\,\mathrm{d}z = \sum_{p\in V}\operatorname{ord}_p f.$$

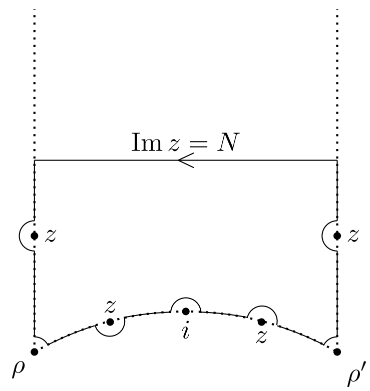
1.3.3 Controlling modular forms

Theorem 1.3.8 ($k/12$-formula)**.** *Let f be a non-zero meromorphic modular form of weight k. Then*

$$\operatorname{ord}_\infty f + \frac{\operatorname{ord}_\rho f}{3} + \frac{\operatorname{ord}_i f}{2} + \sum_{p \in \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H},\ p \nsim \{i,\rho\}} \operatorname{ord}_p f = \frac{k}{12}.$$

Lecture 8 Friday 18/10/19

Proof. Consider the closed curve $C_{N,\epsilon}$,



,

where the z's are zeroes or poles of f, and the circles are of radius ϵ. Consider

$$\frac{1}{2\pi i} \int_{C_{N,\epsilon}} \frac{f'(z)}{f(z)}\, \mathrm{d}z = \sum_{p \in \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H},\ p \nsim \{i,\rho\}} \operatorname{ord}_p f, \qquad \epsilon \to 0.$$

So it suffices to show

$$\lim_{\epsilon \to 0,\ N \to \infty} \frac{1}{2\pi i} \int_{C_{N,\epsilon}} \frac{f'(z)}{f(z)}\, \mathrm{d}z = -\operatorname{ord}_\infty f - \frac{\operatorname{ord}_\rho f}{3} - \frac{\operatorname{ord}_i f}{2} + \frac{k}{12}.$$

The vertical parts of the boundary cancel. The integral over the circular part of $\partial \mathcal{D}$ approaches

$$\frac{1}{2\pi i} \int_\rho^i \frac{f'(z)}{f(z)}\, \mathrm{d}z + \frac{1}{2\pi i} \int_i^{\rho'} \frac{f'(z)}{f(z)}\, \mathrm{d}z = \frac{1}{2\pi i} \left(\int_\rho^i \frac{f'(z)}{f(z)}\, \mathrm{d}z - \int_\rho^i \frac{f'(-1/z)}{f(-1/z)}\, \mathrm{d}z \right)$$

Since $f(-1/z) = z^k f(z)$,

$$\mathrm{d}\left(z^k f(z)\right) = \left(k z^{k-1} f(z) + z^k f'(z)\right) \mathrm{d}z,$$

so

$$\frac{1}{2\pi i} \int_\rho^i \frac{f'(z)}{f(z)}\, \mathrm{d}z + \frac{1}{2\pi i} \int_i^{\rho'} \frac{f'(z)}{f(z)}\, \mathrm{d}z = \frac{1}{2\pi i} \int_\rho^i \frac{f'(z)}{f(z)} - \frac{k z^{k-1} f(z) + z^k f'(z)}{z^k f(z)}\, \mathrm{d}z = -\frac{1}{2\pi i} \int_\rho^i \frac{k}{z}\, \mathrm{d}z = \frac{k}{12}.$$

Since $\mathrm{d}q = 2\pi i q \mathrm{d}z$, the top part is

$$\frac{1}{2\pi i} \int_{\frac{1}{2}+iN}^{\frac{1}{2}-iN} \frac{f'(z)}{f(z)}\, \mathrm{d}z = -\frac{1}{2\pi i} \int_{\text{circle of radius } \epsilon} \frac{g'(q)}{g(q)}\, \mathrm{d}q = -\operatorname{ord}_\infty f.$$

Near i, $f'/f = \operatorname{ord}_i f (z-i)^{-1} + h(z)$, where $h(z)$ is holomorphic and $h(z) \to 0$ as $\epsilon \to 0$. Then the circle $C_{\epsilon,i}$ of radius ϵ centered at i is

$$\lim_{\epsilon \to 0} \frac{1}{2\pi i} \int_{C_{\epsilon,i}} \frac{f'(z)}{f(z)}\, \mathrm{d}z = \lim_{\epsilon \to 0} \frac{1}{2\pi i} \int_{\text{arc of half circle centered at } i} \frac{\operatorname{ord}_i f}{z-i}\, \mathrm{d}z = -\frac{\operatorname{ord}_i f}{2}.$$

Similarly, at ρ and ρ', get that the circles $C_{\epsilon,\rho}$ and $C_{\epsilon,\rho'}$ of radius ϵ centered at ρ and ρ' are

$$\lim_{\epsilon \to 0} \frac{1}{2\pi i} \int_{C_{\epsilon,\rho}} \frac{f'(z)}{f(z)}\, \mathrm{d}z = \lim_{\epsilon \to 0} \frac{1}{2\pi i} \int_{C_{\epsilon,\rho'}} \frac{f'(z)}{f(z)}\, \mathrm{d}z = -\frac{\operatorname{ord}_\rho f}{6},$$

which gives $-\operatorname{ord}_\rho f/3$. $\square$

1.3.4 Holomorphic modular forms

Let
$$\mathrm{M}_k = \{\text{holomorphic modular forms of weight } k\},$$
and let
$$\mathrm{S}_k = \{\text{cusp forms of weight } k\} = \{f \in \mathrm{M}_k \mid \operatorname{ord}_\infty f > 0\} \subseteq \mathrm{M}_k.$$

Corollary 1.3.9.

- $\mathrm{M}_k = 0$ *if* $k < 0$, $k = 2$, *or* k *odd.*
- M_0 *are constants.*
- $\mathrm{M}_4 = \mathbb{C}\mathrm{E}_4$, *where* $\operatorname{ord}_\rho \mathrm{E}_4 = 1$ *and no other zeroes.*
- $\mathrm{M}_6 = \mathbb{C}\mathrm{E}_6$, *where* $\operatorname{ord}_i \mathrm{E}_6 = 1$ *and no other zeroes.*
- $\mathrm{M}_8 = \mathbb{C}\mathrm{E}_8$, *where* $\operatorname{ord}_\rho \mathrm{E}_8 = 2$ *and no other zeroes.*
- $\mathrm{M}_{10} = \mathbb{C}\mathrm{E}_{10}$, *where* $\operatorname{ord}_\rho \mathrm{E}_{10} = \operatorname{ord}_i \mathrm{E}_{10} = 1$ *and no other zeroes.*
- $\mathrm{M}_{12} = \mathbb{C}\mathrm{E}_{12} \oplus \mathbb{C}\Delta$, *where* $\operatorname{ord}_\infty \Delta = 1$ *and no other zeroes.*

Corollary 1.3.10. $\Delta : \mathrm{M}_k \to \mathrm{S}_{k+12}$ *is an isomorphism. On the other hand,*
$$\mathrm{M}_k \cong \mathbb{C}\mathrm{E}_k \oplus \mathrm{S}_k, \qquad k \geq 4 \text{ even},$$
so
$$\mathrm{M}_k \cong \mathbb{C}\mathrm{E}_k \oplus \dots \oplus \mathbb{C}\mathrm{E}_{k-12r}\Delta^r, \qquad k - 12r \in \{0, 4, 6, 8, 10, 14\}.$$
So for $k \geq 4$*, the set*
$$\begin{cases} \mathrm{E}_k, \dots, \mathrm{E}_{k-12\lfloor k/12 \rfloor}\Delta^{\lfloor k/12 \rfloor} & k \not\equiv 2 \mod 12 \\ \mathrm{E}_k, \dots, \mathrm{E}_{14}\Delta^{\lfloor k/12 \rfloor - 1} & k \equiv 2 \mod 12 \end{cases}$$
is a basis for M_k.

Corollary 1.3.11. $\mathrm{E}_4^2 = \mathrm{E}_8$ *and* $\mathrm{E}_4\mathrm{E}_6 = \mathrm{E}_{10}$.

Lecture 9 Monday 21/10/19

A variant is to write $k = 4n + 6m$ with $m = 0, 1$ and $n \geq 0$, for $k \geq 4$. Then $\mathrm{M}_k = \mathbb{C}\mathrm{E}_4^n\mathrm{E}_6^m \oplus \mathrm{S}_k$ gives a basis
$$\mathrm{E}_4^n\mathrm{E}_6^m, \dots, \mathrm{E}_4^{n-3\lfloor n/3 \rfloor}\mathrm{E}_6^m\Delta^{\lfloor n/3 \rfloor}$$
for M_k. Since $\Delta = \left(\mathrm{E}_4^3 - \mathrm{E}_6^2\right)/1728$, we see every modular form of weight k is a polynomial in E_4 and E_6, and
$$\Delta \in q + q^2\mathbb{Z}[[q]], \qquad \mathrm{E}_4^n\mathrm{E}_6^m \in 1 + q\mathbb{Z}[[q]], \qquad \mathrm{E}_4^{n-3}\mathrm{E}_6^m\Delta \in q + q^2\mathbb{Z}[[q]], \qquad \dots$$
have integer coefficients. The upshot is if the q-expansion of f has integer coefficients, then f is an integer combination of
$$\mathrm{E}_4^n\mathrm{E}_6^m, \dots, \mathrm{E}_4^{n-3\lfloor n/3 \rfloor}\mathrm{E}_6^m\Delta^{\lfloor n/3 \rfloor}.$$

Notation. $\mathrm{M}_k(\mathbb{Z}) \subseteq \mathrm{M}_k$ consists of modular forms with integer q-expansions.

Theorem 1.3.12. $\mathrm{M}_k(\mathbb{Z})$ *spans* M_k*, and* $f \in \mathrm{M}_k$ *lies in* $\mathrm{M}_k(\mathbb{Z})$ *if and only if* f *is an integral polynomial in* $\mathrm{E}_4, \mathrm{E}_6, \Delta$.

Definition 1.3.13. A **graded ring** is a ring R, together with a direct sum decomposition, as abelian groups,
$$R = \bigoplus_{i \in \mathbb{Z}} R_i,$$
such that $R_i \cdot R_j \subseteq R_{i+j}$ for all $i, j \in \mathbb{Z}$.

Example.

- $R = \mathbb{C}[X, Y]$, where R_i are polynomials homogeneous of degree i.
- $R = \bigoplus_{k \in \mathbb{Z}} \mathrm{M}_k$.

Let $\mathbb{C}[X,Y]$ be graded with $\deg X = 4$ and $\deg Y = 6$. Have a homomorphism of graded rings

$$\begin{array}{ccc} \mathbb{C}[X,Y] & \longrightarrow & \bigoplus_{k\in\mathbb{Z}} \mathrm{M}_k \\ (X,Y) & \longmapsto & (\mathrm{E}_4, \mathrm{E}_6) \end{array}.$$

Theorem 1.3.14. *This is an isomorphism of graded rings.*

Proof. This map is surjective, since every $f \in \mathrm{M}_k$ is a polynomial in E_4 and E_6. Remains to show this map is injective. Suppose not. There exists $P(X,Y)$, homogeneous of degree k, such that $P(\mathrm{E}_4,\mathrm{E}_6) = 0$. Write $k = 4n + 6m$ with $m = 0,1$. If $P = c_0 X^n Y^n + \dots + c_r X^{n-3r} Y^{m+2r}$ where $r = \lfloor n/3 \rfloor$, then

$$c_0 \mathrm{E}_4^n \mathrm{E}_6^n + \dots + c_r \mathrm{E}_4^{n-3r} \mathrm{E}_6^{m+2r} = 0.$$

Dividing by $\mathrm{E}_4^{n-3r}\mathrm{E}_6^{m+2r}$, get $Q\left(\mathrm{E}_4^3/\mathrm{E}_6^2\right) = 0$ where $Q(X) = c_0 X^r + \dots + c_r$. Since the roots of Q are discrete, and $\mathrm{E}_4^3/\mathrm{E}_6^2$ is non-constant, this is impossible. $\square$

1.3.5 Meromorphic modular forms

Note. The meromorphic modular forms of weight zero form a field. For example, $\mathrm{j}(z) = \mathrm{E}_4^3/\Delta = 1728\mathrm{E}_4^3/\left(\mathrm{E}_4^3 - \mathrm{E}_6^2\right)$ is a non-constant meromorphic modular form, with a pole of order one at infinity, a zero of order three at ρ, and no other zeroes or poles.

Theorem 1.3.15. j *gives a bijection between* $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ *and* $\mathbb{C}$.

Proof. Given $\lambda \in \mathbb{C}$, want $z \in \mathbb{H}$ such that $\mathrm{j}(z) = \lambda$. Consider $g = j - \lambda$. This is meromorphic of weight zero. There is a pole at infinity, and no other poles, and

$$\mathrm{ord}_\infty g + \frac{\mathrm{ord}_\rho g}{3} + \frac{\mathrm{ord}_i g}{2} + \sum_{p \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H},\ p \nsim \{i,\rho\}} \mathrm{ord}_p g = 0.$$

The only possibilities are

- g has a zero at ρ of order three, and no other zeroes,
- g has a zero at i of order two, and no other zeroes, or
- g has a simple zero somewhere else, and no others.

In each case, the zero of g is a unique $\mathrm{SL}_2(\mathbb{Z})$-orbit on which $\mathrm{j}(z) = \lambda$. So j is bijective. $\square$

Lecture 10 Friday 25/10/19

Theorem 1.3.16. *Every meromorphic modular form of weight zero is a rational function in* j*. That is, the field of meromorphic modular forms is* $\mathbb{C}(\mathrm{j})$*.*

Proof. Let g be meromorphic of weight zero. Then g has finitely many $\mathrm{SL}_2(\mathbb{Z})$-orbits worth of poles in $\mathbb{H}$. Saw last time that j is holomorphic in $\mathbb{H}$. If p is a pole of g, then $(\mathrm{j}(z) - \mathrm{j}(p))^{n_p}$ is holomorphic on $\mathbb{H}$ and zero at $z = p$. Doing this for all poles, there exists $P \in \mathbb{C}[X]$ such that $P(\mathrm{j})\, g(z)$ is holomorphic on $\mathbb{H}$. Then for some m, $P(\mathrm{j})\, g(z)\, \Delta^m$ is holomorphic of weight $12m$. So it suffices to show if h is holomorphic of weight $12m$, then h/Δ^m is a rational function in j, since if $P(\mathrm{j})\, g(z)\, \Delta^m = h$ then $P(\mathrm{j})\, g(z) \in \mathbb{C}(\mathrm{j})$, so $g(z) \in \mathbb{C}(\mathrm{j})$. Then h is a sum of terms

$$h = \sum_{a,b} c_{a,b} \mathrm{E}_4^a \mathrm{E}_6^b, \qquad c_{a,b} \in \mathbb{C}, \qquad 4a + 6b = 12m.$$

Considering this equation modulo four and modulo three, find $3 \mid a$ and $2 \mid b$, so

$$\frac{h}{\Delta^m} = \sum_{a,b} c_{a,b} \left(\frac{\mathrm{E}_4^3}{\Delta}\right)^{\frac{a}{3}} \left(\frac{\mathrm{E}_6^2}{\Delta}\right)^{\frac{b}{2}}.$$

So it suffices to show E_4^3/Δ and E_6^2/Δ are rational functions in j. Then $\mathrm{j} = \mathrm{E}_4^3/\Delta$, and

$$\frac{\mathrm{E}_6^2}{\Delta} = \frac{1728\mathrm{E}_6^2}{\mathrm{E}_4^3 - \mathrm{E}_6^2} = \frac{1728\left(\mathrm{E}_6^2 - \mathrm{E}_4^3\right) + 1728\mathrm{E}_4^3}{\mathrm{E}_4^3 - \mathrm{E}_6^2} = -1728 + \frac{1728\mathrm{E}_4^3}{\mathrm{E}_4^3 - \mathrm{E}_6^2} = \mathrm{j} - 1728.$$

$\square$

1.4 Theta series

Let $L \subseteq \mathbb{R}^n$ be a lattice. For $x, y \in L$, $x \cdot y \in \mathbb{R}$. Suppose $x \cdot y \in \mathbb{Z}$ for all $x, y \in L$. A question is for $n \in \mathbb{Z}$, how many $x \in L$ have $x \cdot x = n$? The rough idea is to form the series

$$\sum_{x \in L} q^{x \cdot x} = \sum_{n=0}^{\infty} a_n q^n, \qquad a_n = \# \{x \in L \mid x \cdot x = n\}.$$

We will show, with some slight modifications, and extra hypotheses on L, this generating function turns out to be a modular form.

1.4.1 Quadratic forms

Fix a lattice $L \subseteq \mathbb{R}^n$, so

$$L = \mathbb{Z} \cdot e_1 \oplus \dots \oplus \mathbb{Z} \cdot e_n.$$

Given these e_i, form a matrix A such that $A_{ij} = e_i \cdot e_j$.

Note. $A = B^\intercal B$, where B is the matrix whose columns are the e_i, and $|\det B|$ is the volume of the parallelogram spanned by e_i, so $\det A = (\det B)^2 > 0$.

Definition 1.4.1. The **dual lattice** $L^\vee$ is the set of $y \in \mathbb{R}^n$ such that $y \cdot x \in \mathbb{Z}$ for all $x \in L$.

Let $f_1, \dots, f_n$ be the dual basis to $e_1, \dots, e_n$, that is the unique set of solutions $f_1, \dots, f_n$ such that

$$f_i \cdot e_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

Then $L^\vee$ is spanned by the f_i. Clearly $f_i \in L^\vee$ for all i. Conversely, if $y \in L^\vee$, then $y \cdot e_i = a_i \in \mathbb{Z}$, then $y = \sum_{i=1}^n a_i f_i$.

Proposition 1.4.2. *Let $C = A^{-1}$. Then*

$$f_i = \sum_{j=1}^{n} C_{ij} e_j.$$

Proof.

$$f_i \cdot e_k = \sum_{j=1}^{n} C_{ij} e_j e_k = \sum_{j=1}^{n} C_{ij} A_{jk} = (CA)_{ik} = \begin{cases} 1 & i = k \\ 0 & i \neq k \end{cases}.$$

□

Definition 1.4.3. A lattice L is **self-dual** if $L^\vee = L$ as subsets of $\mathbb{R}^n$.

Proposition 1.4.4. *L is self-dual if and only if the associated matrix A has integer entries and determinant 1.*

Proof. Clearly if $L = L^\vee$, then $e_i \cdot e_j \in \mathbb{Z}$, so A has integer entries. Since $L^\vee \subseteq L$, f_i is an integer combination of the e_j, so $C = A^{-1}$ has integer entries. So $\det A = \pm 1$, but already saw $\det A > 0$. Conversely if A has integer entries and determinant one, $C = A^{-1}$ has integer entries. Then A has integer entries implies that $e_i \cdot e_j \in \mathbb{Z}$ for all i and j, so $e_i \in L^\vee$ for all i, so $L \subseteq L^\vee$. Similarly, C has integer entries implies that $L^\vee \subseteq L$. □

If L is self-dual, get an integer-valued **quadratic form**

$$\begin{array}{rccl} \mathrm{Q}_L : & \mathbb{Z}^n & \longrightarrow & \mathbb{Z} \\ & (a_1, \dots, a_n) & \longmapsto & (a_1 e_1 + \dots + a_n e_n) \cdot (a_1 e_1 + \dots + a_n e_n) = \begin{pmatrix} a_1 & \dots & a_n \end{pmatrix} A \begin{pmatrix} a_1 \\ \dots \\ a_n \end{pmatrix} \end{array}.$$

A question is given m, how often does Q_L represent m?

1.4.2 Fourier analysis

Lecture 11 Friday 25/10/19

Let f be a C^∞ function on $\mathbb{R}^n \to \mathbb{C}$.

Definition 1.4.5. We will say f is **rapidly decreasing** if for all m,

$$\|x|^m \cdot f(x)| \to 0, \qquad |x| \to \infty,$$

where $|x| = (x \cdot x)^{1/2}$. For $f \in \mathrm{C}^\infty$, rapidly decreasing, define

$$\widehat{f}(y) = \int_{\mathbb{R}^n} e^{-2\pi i (x \cdot y)}\, \mathrm{d}x : \mathbb{R}^n \to \mathbb{C}.$$

Fact. If f is smooth and rapidly decreasing, so is $\widehat{f}$.

Fact. If $f(x) = e^{-\pi(x\cdot x)}$, then $\widehat{f}(x) = f(x)$.

Fact. If f is smooth and rapidly decreasing, and $\mathbb{R}^n$ is a lattice with volume V, then

$$\sum_{x \in L} f(x) = \frac{1}{v} \sum_{x \in L^\vee} \widehat{f}(x).$$

1.4.3 Theta series

A crucial assumption is that L is self-dual. An assumption that can be removed is that L is even, so for all $x \in L$, $\mathrm{Q}_L(x) \in 2\mathbb{Z}$.

Definition 1.4.6. The **theta series** Θ_L is defined by

$$\Theta_L(z) = \sum_{x \in L} q^{\frac{1}{2} x \cdot x} = \sum_{m=0}^{\infty} a_m q^m, \qquad a_m = \#\{x \in \mathbb{Z}^n \mid \mathrm{Q}_L(x) = 2m\}.$$

Theorem 1.4.7. *Θ_L is modular of weight $n/2$.*

Example. Let $\Gamma_8 \subseteq \mathbb{R}^8$ be spanned by

$$e_1 = \left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}\right), \qquad e_2 = (1,1,0,0,0,0,0,0),$$

$$e_3 = (1,-1,0,0,0,0,0,0), \qquad e_4 = (0,1,-1,0,0,0,0,0), \qquad e_5 = (0,0,1,-1,0,0,0,0),$$
$$e_6 = (0,0,0,1,-1,0,0,0), \qquad e_7 = (0,0,0,0,1,-1,0,0), \qquad e_8 = (0,0,0,0,0,1,-1,0).$$

Then

$$A = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix},$$

and

$$\mathrm{Q}_L(z_1, \dots, z_8) = 2\left(z_1^2 + \dots + z_8^2 - z_1 z_3 - z_2 z_4 - z_3 z_4 - z_4 z_5 - z_6 z_7 - z_7 z_8\right).$$

If $L \subseteq \mathbb{R}^n$ is even and self-dual, and Θ_L is modular of weight $n/2$, then dimension is ~ 24.

Fact. $L \subseteq \mathbb{R}^n$ even and self-dual implies that $8 \mid n$.

Proof. Serre V.2.1 Corollary 2. □

Proof of Theorem 1.4.7. Know, since L is even, that $\Theta_L(z+1) = \Theta_L(z)$. It suffices to show $\Theta_L(-1/z) = z^{n/2}\Theta_L(z)$. Both sides are holomorphic on $\mathbb{H}$, so it suffices to show

$$\Theta_L\left(-\frac{1}{it}\right) = (it)^{\frac{n}{2}}\,\Theta_L(it).$$

For $t \in \mathbb{R}^\times$, let $L_t = t^{1/2} \cdot L$ and $L_t^\vee = t^{-1/2} \cdot L = L_{t^{-1}}$, so $\operatorname{vol} L_t = t^{n/2}$. By the facts,

$$\sum_{x \in L_t} e^{-\pi(x \cdot x)} = t^{-\frac{n}{2}} \sum_{x \in L_{t^{-1}}} e^{-\pi(x \cdot x)},$$

so

$$\sum_{x \in L} e^{-\pi(x \cdot x)t} = t^{-\frac{n}{2}} \sum_{x \in L} e^{-\frac{\pi(x \cdot x)}{t}}.$$

Now return to Θ_L. The left hand side is

$$\Theta_L\left(-\frac{1}{it}\right) = \sum_{x \in L} e^{\frac{1}{2}\cdot 2\pi i \cdot \left(-\frac{1}{it}\right)\cdot(x \cdot x)} = \sum_{x \in L} e^{-\frac{\pi(x \cdot x)}{t}},$$

and the right hand side is

$$\Theta_L(it) = \sum_{x \in L} e^{\frac{1}{2}\cdot 2\pi i \cdot (it) \cdot (x \cdot x)} = \sum_{x \in L} e^{\pi(x \cdot x)t},$$

so the result follows. ◻

1.4.4 Asymptotic analysis

Let $\Theta_L = \sum_{m=1}^{\infty} a_m q^m$, where a_m is the number of ways Q_L represents $2m$, so $a_0 = 1$. Then

$$\Theta_L = \mathrm{E}_{\frac{n}{2}} + g, \qquad \mathrm{E}_{\frac{n}{2}} \sim \sigma_{\frac{n}{2}-1}(m) \sim m^{\frac{n}{2}-1},$$

where g is a cusp form. Lecture 12 Monday 28/10/19

Lecture 12 is a problem class.

Lecture 13 Friday 01/11/19

Proposition 1.4.8. *Let*

$$\mathrm{E}_k = \sum_{n=0}^{\infty} a_n q^n = 1 + C \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n.$$

Then there exist $A, B \in \mathbb{R}_{>0}$ such that

$$An^{k-1} \le a_n \le Bn^{k-1}.$$

Proof. Set $A = C$. Then

$$\sigma_{k-1}(n) = \sum_{d \mid n} d^{k-1} \ge n^{k-1},$$

so $a_n = C\sigma_{k-1}(n) \ge Cn^{k-1}$. Consider

$$\frac{\sigma_{k-1}(n)}{n^{k-1}} = \sum_{d \mid n} \frac{d^{k-1}}{n^{k-1}} = \sum_{d' \mid n} \frac{1}{d'^{k-1}} \le \sum_{n=1}^{\infty} \frac{1}{n^{k-1}} = \zeta(k-1),$$

so $\sigma_{k-1}(n) \le \zeta(k-1)\, n^{k-1}$. So set $B = C \cdot \zeta(k-1)$, so $a_n \le Bn^{k-1}$. ◻

Theorem 1.4.9 (Hasse)**.** *Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a cusp form of weight k. Then*

$$|a_n| = \mathrm{O}\left(n^{\frac{k}{2}}\right),$$

that is $|a_n|\, n^{-k/2}$ is bounded as $n \to \infty$.

Proof. f/q is holomorphic on $\mathbb{H}$, so $|f/q|$ is bounded as $q \to 0$, so $|f(z)|/e^{-2\pi \operatorname{Im} z}$ is bounded as $\operatorname{Im} z \to \infty$. That is, there exist $M \in \mathbb{R}$ such that $|f(z)| \le Me^{-2\pi \operatorname{Im} z}$. Consider

$$\phi(z) = |f(z)| \operatorname{Im} z^{\frac{k}{2}},$$

so $\lim_{\operatorname{Im} z \to \infty} \phi(z) = 0$. Note that

$$\phi(\gamma z) = |f(\gamma z)| \operatorname{Im} \gamma z^{\frac{k}{2}} = |f(z)||cz+d|^k \frac{\operatorname{Im} z^{\frac{k}{2}}}{|cz+d|^{2\frac{k}{2}}} = |f(z)| \operatorname{Im} z^{\frac{k}{2}} = \phi(z), \qquad \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

Then $\phi(z)$ is determined by its values on the standard fundamental domain, so $\phi(z)$ is bounded on $\mathbb{H}$, so $|f(z)| < M' \operatorname{Im} z^{-k/2}$ for some $M' \in \mathbb{R}$. If $z = x + iy$ for y fixed, then the residue theorem implies that

$$a_m = \frac{1}{2\pi i} \int_C \frac{f(q)}{q^{m+1}} \, \mathrm{d}q = \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{f(x+iy)}{e^{2\pi i(x+iy)m}} \, \mathrm{d}x,$$

so

$$|a_m| \le \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{|f(x+iy)|}{e^{-2\pi ym}} \, \mathrm{d}x \le \frac{|f(x+iy)|}{e^{-2\pi ym}} \le e^{2\pi ym} M' y^{-\frac{k}{2}}.$$

Set $y = 1/m$. Get $|a_n| \le e^{2\pi} M' m^{k/2}$, so $|a_m|/m^{k/2}$ is bounded. ☐

Had

$$\Theta_L = \mathrm{E}_{\frac{n}{2}} + g, \qquad \mathrm{E}_{\frac{n}{2}} \sim m^{\frac{n}{2}-1}, \qquad g = \mathrm{O}\left(m^{\frac{n}{4}}\right).$$

Theorem 1.4.10 (Deligne). *Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a cusp form of weight k. Then*

$$|a_n| = \mathrm{O}\left(n^{\frac{k-1}{2}} \sigma_0(n)\right).$$

Proof. Very rough sketch of argument.

Ramanujan 1910s. Conjectured by Ramanujan for $f = \Delta$.

Weil 1940s. For an algebraic variety V over $\mathbb{F}_q$, what can we say about $\#V(\mathbb{F}_{q^n})$ for various n? Weil associated to V and $\mathbb{F}_q$ a generating function called the **zeta function** $\zeta_{V,q}(t)$ of V over $\mathbb{F}_q$, conjectured several things about $\zeta_{V,q}$, and proved in the case of curves.

- $\zeta_{V,q}$ is a rational function in t.
- $\zeta_{V,q}$ satisfies a certain symmetry under $t \mapsto 1/t$.
- The Riemann hypothesis

$$\zeta_{V,q}(t) = \frac{P_1(t) \dots P_{2d-1}(t)}{P_0(t) \dots P_{2d}(t)}, \qquad \dim V = d,$$

where the roots of $P_i(t)$ have absolute value $q^{i/2}$.

Eichler-Shimura 1950s. Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a nice **congruence subgroup**. Then $X_\Gamma = \Gamma \backslash \mathbb{H}$ has the structure of an algebraic curve over $\mathbb{Q}$, with **good reduction** at primes p not dividing $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$. Eichler, Shimura, and others studied $\zeta_{V,p}$ for $V = X_\Gamma$, and related $\zeta_{V,p}$ to the p-th Fourier coefficients of a basis for forms of weight two and **level** Γ. The Weil conjectures bound a_p in terms of $q^{1/2}$.

Deligne 1960s. Deligne showed that in weight k, there exists a **Kuga-Sato variety**, of dimension $k-1$, whose zeta function has a factor coming from modular forms of weight k and level Γ, and showed that if the Weil conjectures, particularly the Riemann hypothesis, holds, then get the coefficient bound.

Deligne 1970s. Riemann hypothesis in higher dimensions.

☐

1.5 Hecke operators

Lecture 14 Friday 01/11/19

Let $\Delta = \left(\mathrm{E}_4^3 - \mathrm{E}_6^2\right)/1728 = \sum_{n=1}^{\infty} \tau(n) q^n$. Then $\tau(n)$ grows roughly like n^6 or $n^{11/2+\epsilon}$. Mordell proved

- $\tau(mn) = \tau(n)\tau(m)$ if $(m,n)=1$, and
- $\tau\left(p^{n+1}\right) = \tau(p)\tau(p^n) - p^{11}\tau\left(p^{n-1}\right)$.

If $\mathrm{E}_k = 1 + C\sum_n \sigma_{k-1}(n) q^n$, set

$$\mathrm{E}_k' = \frac{1}{C} + \sum_n \sigma_{k-1}(n) q^n.$$

Note.

- If $(m,n)=1$, then

$$\sigma_{k-1}(nm) = \sum_{d \mid n}\sum_{d' \mid m} (dd')^{k-1} = \left(\sum_{d \mid n} d^{k-1}\right)\left(\sum_{d' \mid m} d'^{k-1}\right) = \sigma_{k-1}(n)\sigma_{k-1}(m).$$

- Since $\sigma_{k-1}(p^n) = 1 + \dots + p^{n(k-1)}$,

$$\begin{aligned}\sigma_{k-1}(p)\sigma_{k-1}(p^n) &= \left(1+p^{k+1}\right)\left(1+\dots+p^{n(k-1)}\right) \\ &= 1 + 2p^{k-1} + \dots + 2p^{n(k-1)} + p^{(n+1)(k-1)} \\ &= \sigma_{k-1}\left(p^{n+1}\right) + p^{k-1}\sigma_{k-1}\left(p^{n-1}\right),\end{aligned}$$

  so

$$\sigma_{k-1}\left(p^{n+1}\right) = \sigma_{k-1}(p)\sigma_{k-1}(p^n) - p^{k-1}\sigma_{k-1}\left(p^{n-1}\right).$$

1.5.1 Correspondences

Definition 1.5.1. Let X be a set. The **free abelian group on** X, denoted $\mathbb{Z}X$, is the set of finite formal sums

$$\sum_{i=1}^{r} a_i x_i, \qquad a_i \in \mathbb{Z}, \qquad x_i \in X,$$

where x_i are distinct. Add by combining like terms.

Definition 1.5.2. A **correspondence** on X is a homomorphism $\mathbb{Z}X \to \mathbb{Z}X$. Let

$$\operatorname{Corr} X = \{\text{correspondences on } X\}.$$

Equivalently, a correspondence associates to each $x \in X$, a finite formal sum

$$\sum_{i=1}^{r} a_i y_i, \qquad a_i \in \mathbb{Z}, \qquad y_i \in X.$$

If X is a finite set $X = \{x_1, \dots, x_r\}$, any correspondence T can be represented, in a unique way, by the matrix M_T such that

$$Tx_i = \sum_{j=1}^{r} (M_T)_{ij} x_j,$$

and composition of correspondences is matrix multiplication. Let X be a set, and let

$$\operatorname{Fun}_{\mathbb{C}} X = \{\text{functions } X \to \mathbb{C}\}.$$

Then $T \in \operatorname{Corr} X$ acts on $\operatorname{Fun}_{\mathbb{C}} X$ as follows. If $Tx = \sum_i a_i x_i$ then $(Tf)x = \sum_i a_i f(x_i)$. Check $(T \circ T')f = T(T'f)$, etc. Let

$$\mathcal{L} = \{\text{lattices in } \mathbb{C}\}.$$

Example. The following are correspondences in $\mathcal{L}$.

- For $\lambda \in \mathbb{C}^\times$, have
$$\begin{array}{rccc} \mathrm{R}_\lambda & : & \mathbb{Z}\mathcal{L} & \longrightarrow & \mathbb{Z}\mathcal{L} \\ & & L & \longmapsto & \lambda L \end{array}.$$
- For $n \in \mathbb{Z}_{>0}$, have
$$\begin{array}{rccc} \mathrm{T}_n & : & \mathbb{Z}\mathcal{L} & \longrightarrow & \mathbb{Z}\mathcal{L} \\ & & L & \longmapsto & \sum_{L' \subseteq_n L} L' \end{array},$$
the n **Hecke operators**. Note that there are only finitely many $L' \subseteq L$ of index n, since if L' has index n in L, then L' contains $\mathrm{R}_n L$. Then $L/\mathrm{R}_n L \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. The image of L' in $L/\mathrm{R}_n L$ is a subgroup H of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ of order n. The preimage of H in L is L'. Thus there is a bijection
$$\left\{ \text{ subgroups of } L/\mathrm{R}_n L \text{ of order } n \right\} \qquad \leftrightsquigarrow \qquad \left\{ \text{ sublattices of index } n \right\}.$$

Proposition 1.5.3.

1. $\mathrm{R}_\lambda \mathrm{R}_\mu = \mathrm{R}_{\lambda\mu}$.
2. $\mathrm{R}_\lambda \mathrm{T}_n = \mathrm{T}_n \mathrm{R}_\lambda$.
3. $\mathrm{T}_n \mathrm{T}_m = \mathrm{T}_{nm}$ *if* $(m, n) = 1$.
4. $\mathrm{T}_p \mathrm{T}_{p^n} = \mathrm{T}_{p^{n+1}} + p\mathrm{T}_{p^{n+1}} \mathrm{R}_p$.

Lecture 15 Monday 04/11/19

Corollary 1.5.4. T_p *commute with each other for p prime, also with* R_λ*, and every* T_n *is a polynomial in* T_p *and* R_p *for* $p \mid n$*, so all* T_n *and* R_λ *commute.*

Proposition 1.5.5. *If A is an abelian group of order nm, with $(n, m) = 1$, then A factors uniquely as $B \times C$, where B has order n and C has order m. In particular B is the unique subgroup of A of order n.*

Proof. Write $1 = an + bm$ for $a, b \in \mathbb{Z}$. Have a map
$$\begin{array}{rcl} A & \longleftrightarrow & mA \times nA \\ x & \longmapsto & (mbx, nax) \\ x + y & \longleftarrow & (x, y) \end{array}.$$
Then mA has order n and nA has order m. Clearly inverses on one side, so counting implies isomorphism. $\square$

Proof of Proposition 1.5.3.

1. Easy.
2. If $L \in \mathcal{L}$, then
$$\mathrm{R}_\lambda \mathrm{T}_n L = \mathrm{R}_\lambda \sum_{L' \subseteq_n L} L' = \sum_{L' \subseteq_n L} \mathrm{R}_\lambda L' = \sum_{L' \subseteq_n \mathrm{R}_\lambda L} L' = \mathrm{T}_n \mathrm{R}_\lambda L.$$
3. If $L \in \mathcal{L}$, then
$$\mathrm{T}_n \mathrm{T}_m L = \mathrm{T}_n \sum_{L' \subseteq_m L} L' = \sum_{L' \subseteq_m L} \mathrm{T}_n L' = \sum_{L' \subseteq_m L} \sum_{L'' \subseteq_n L'} L''.$$
An observation is $L'' \subseteq_n L' \subseteq_m L$, so L'' has index nm in L. Let
$$\mathrm{T}_n \mathrm{T}_m L = \sum_{L'' \subseteq_{nm} L} c_{n,m}(L'', L) L'', \qquad c_{n,m}(L'', L) = \#\left\{L' \in \mathcal{L} \mid L'' \subseteq_n L' \subseteq_m L\right\}.$$
An observation is that there is a bijection
$$\begin{array}{rcl} \{\text{lattices } L' \mid L'' \subseteq_n L' \subseteq_m L\} & \longleftrightarrow & \{\text{subgroups } H \text{ of } L/L'' \text{ of order } n\} \\ L' & \longmapsto & L'/L'' \subseteq L/L'' \\ \text{preimage of } H \text{ under } L \to L/L'' & \longleftarrow & H \end{array}.$$
Have $(n, m) = 1$, so $c_{n,m}(L'', L) = 1$ so
$$\mathrm{T}_n \mathrm{T}_m L = \sum_{L'' \subseteq_{nm} L} c_{n,m}(L'', L) L'' = \sum_{L'' \subseteq_{nm} L} L'' = \mathrm{T}_{nm} L.$$

4. If $L \in \mathcal{L}$, then
$$\mathrm{T}_p \mathrm{T}_{p^r} L = \sum_{L'' \subseteq_{p^{r+1}} L} c_{p,p^r}(L'', L) L'', \qquad c_{p,p^r}(L'', L) = \# \{L' \in \mathcal{L} \mid L'' \subseteq_p L' \subseteq_{p^r} L\}.$$
What is
$$c_{p,p^r}(L'', L) = \# \{\text{subgroups of order } p \text{ in } L/L''\}?$$
L/L'' is abelian of order p^{r+1} and generated by two elements. The classification of finite abelian groups implies that every finite abelian group can be written uniquely as $\mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_r\mathbb{Z}$ where $a_1 \mid \dots \mid a_r$, up to isomorphism, and r is the minimal number of generators for such a group. So
$$L/L'' \cong \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}/p^b\mathbb{Z}, \qquad a, b \ge 0, \qquad a + b = r + 1.$$
Case 1. $L/L'' \cong \mathbb{Z}/p^{r+1}\mathbb{Z}$ is cyclic. In this case $c_{p,p^r}(L'', L) = 1$.

Case 2. $L/L'' \cong \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}/p^b\mathbb{Z}$ with $a, b > 0$. Any subgroup of order p is contained in the subgroup killed by p,
$$p^{a-1}\mathbb{Z}/p^a\mathbb{Z} \times p^{n-1}\mathbb{Z}/p^b\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^2.$$
The $p^2 - 1$ elements of $(\mathbb{Z}/p\mathbb{Z})^2 \setminus \{0\}$ each spans a subgroup of order p, and two elements span the same group if and only if they differ by a scalar in $(\mathbb{Z}/p\mathbb{Z})^\times$, so there are $(p^2-1)/(p-1) = p + 1$ subgroups of order p in $(\mathbb{Z}/p\mathbb{Z})^2$. In this case $c_{p,p^r}(L'', L) = p + 1$.

The latter case occurs if and only if L/L'' maps surjectively to $(\mathbb{Z}/p\mathbb{Z})^2 \cong L/\mathrm{R}_p L$, if and only if $\mathrm{R}_p L \supseteq L''$. Thus
$$\begin{aligned} \mathrm{T}_p \mathrm{T}_{p^r} L &= \sum_{L'' \subseteq_{p^{r+1}} L} c_{p,p^r}(L'', L) L'' = \sum_{L'' \subseteq_{p^{r+1}} L \text{ cyclic}} L'' + \sum_{L'' \subseteq_{p^{r+1}} L \text{ not cyclic}} (p+1) L'' \\ &= \mathrm{T}_{p^{r+1}} L + p \sum_{L'' \subseteq_{p^{r+1}} L \text{ not cyclic}} L'' = \mathrm{T}_{p^{r+1}} L + p \sum_{L'' \subseteq_{p^{r-1}} \mathrm{R}_p L} L'' = \mathrm{T}_{p^{r+1}} L + p \mathrm{T}_{p^{r-1}} \mathrm{R}_p L. \end{aligned}$$

□

1.5.2 Hecke operators

Lecture 16 Friday 08/11/19

If $F : \mathcal{L} \to \mathbb{C}$, then
$$\mathrm{T}_n F(L) = \sum_{L' \subseteq_n L} F(L'), \qquad \mathrm{R}_\lambda F(L) = F(\mathrm{R}_\lambda L).$$
Recall that F has weight k if $F(\mathrm{R}_\lambda L) = \lambda^{-k} F(L)$ for all $\lambda \in \mathbb{C}^\times$, if and only if $\mathrm{R}_\lambda F = \lambda^{-k} F$ for all $\lambda \in \mathbb{C}^\times$, so
$$\mathrm{R}_\lambda \mathrm{T}_n F = \mathrm{T}_n \mathrm{R}_\lambda F = \mathrm{T}_n \lambda^{-k} F = \lambda^{-k} \mathrm{T}_n F.$$
So the T_n and R_λ preserve lattice functions of weight k. Have a bijection
$$\begin{array}{ccc} \left\{ f : \mathbb{H} \to \mathbb{C} \;\middle|\; f(\gamma z) = (cz + d)^k f(z) \right\} & \longrightarrow & \{\text{lattice functions } F \text{ of weight } k\} \\ f(z) & \longmapsto & F(\mathrm{L}_{z,1}) \end{array}.$$
On lattice functions of weight k, have
$$\mathrm{T}_p \mathrm{T}_{p^r} = \mathrm{T}_{p^{r+1}} + p^{1-k} \mathrm{T}_{p^{r-1}}.$$
Definition 1.5.6. For $f : \mathbb{H} \to \mathbb{C}$ corresponding to $F : \mathcal{L} \to \mathbb{C}$ of weight k, define $\mathrm{T}_n f$ by
$$(\mathrm{T}_n f)(z) = n^{k-1} (\mathrm{T}_n F)(\mathrm{L}_{z,1}) = n^{k-1} \sum_{L' \subseteq_n \mathrm{L}_{z,1}} F(L').$$
On $f : \mathbb{H} \to \mathbb{C}$, T_n satisfy
$$\mathrm{T}_p \mathrm{T}_{p^r} = \mathrm{T}_{p^{r+1}} + p^{k-1} \mathrm{T}_{p^{r-1}}.$$

Need to rewrite $\sum_{L' \subseteq_n \mathrm{L}_{z,1}} F(L')$ in terms of f. Let

$$\mathrm{S}_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{Mat}_{2 \times 2}(\mathbb{Z}) \;\middle|\; ad = n,\ a, d > 0,\ 0 \le b < d \right\}, \qquad s_n = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{S}_n.$$

Lemma 1.5.7. *The map*

$$\begin{array}{rcl} \mathrm{S}_n & \longrightarrow & \{\text{sublattices of } \mathrm{L}_{z,1} \text{ of index } n\} \\ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} & \longmapsto & \mathrm{L}_{az+b,d} \end{array}$$

is a bijection.

Proof. For surjectivity, let $L \subseteq_n \mathrm{L}_{z,1}$. Then $\mathrm{L}_{z,1}/L$ is a group of order n. Can consider $1 + L \in \mathrm{L}_{z,1}/L$. Let d be the order of $1 + L$, that is d is the smallest positive integer such that $d \in L$. Then $d \mid n$, so set $a = n/d$. Let $L' = \mathbb{Z} + L$ be the lattice generated by 1 and L. Then $L \subseteq_d L'$ and $L \subseteq_n \mathrm{L}_{z,1}$, so $L' \subseteq_a \mathrm{L}_{z,1}$, so $az \in L'$, so there exists $b \in \mathbb{Z}$ such that $az + b \in L$. Since $d \in L$, without loss of generality can arrange $0 \le b < d$. Now $d \in L$ and $az + b \in L$, so $L \subseteq_n \mathrm{L}_{z,1}$ and $\mathrm{L}_{az+b,d} \subseteq_n \mathrm{L}_{z,1}$, so $L = \mathrm{L}_{az+b,d}$. Thus surjective, and for injectivity, can recover a, b, d from $\mathrm{L}_{az+b,d} \subseteq \mathrm{L}_{z,1}$. ☐

Thus

$$\begin{aligned} \mathrm{T}_n f &= n^{k-1} \sum_{L' \subseteq_n \mathrm{L}_{z,1}} F(L') = n^{k-1} \sum_{s_n \in \mathrm{S}_n} F(\mathrm{L}_{az+b,d}) \\ &= n^{k-1} \sum_{s_n \in \mathrm{S}_n} d^{-k} F\left(\mathrm{L}_{\frac{az+b}{d},1}\right) = n^{k-1} \sum_{s_n \in \mathrm{S}_n} d^{-k} f\left(\frac{az+b}{d}\right). \end{aligned}$$

Theorem 1.5.8. *If $f = \sum_{m=0}^{\infty} c(m) q^m$ is modular of weight k, then*

$$\mathrm{T}_n f = \sum_{m=0}^{\infty} \gamma(m) q^m, \qquad \gamma(m) = \sum_{a \mid (m,n),\ a \ge 1} a^{k-1} c\left(\frac{mn}{a^2}\right).$$

Proof.

$$\begin{aligned} \mathrm{T}_n f &= n^{k-1} \sum_{s_n \in \mathrm{S}_n} d^{-k} f\left(\frac{az+b}{d}\right) = n^{k-1} \sum_{s_n \in \mathrm{S}_n} \sum_{m=0}^{\infty} d^{-k} c(m) e^{2\pi i m\left(\frac{az+b}{d}\right)} \\ &= n^{k-1} \sum_{ad=n,\ a>0} \sum_{b=0}^{d-1} \sum_{m=0}^{\infty} d^{-k} c(m) q^{\frac{ma}{d}} e^{\frac{2\pi i m b}{d}} = n^{k-1} \sum_{m=0}^{\infty} \sum_{ad=n,\ a>0} d^{-k} c(m) q^{\frac{ma}{d}} \sum_{b=0}^{d-1} e^{\frac{2\pi i m b}{d}}. \end{aligned}$$

Then

$$\sum_{b=0}^{d-1} e^{\frac{2\pi i m b}{d}} = \begin{cases} d & d \mid m \\ 0 & d \nmid m \end{cases},$$

so

$$\mathrm{T}_n f = n^{k-1} \sum_{m=0,\ d \mid m}^{\infty} \sum_{ad=n,\ a>0} d^{1-k} c(m) q^{\frac{ma}{d}} = \sum_{a \mid n,\ a>0} \sum_{m'=0}^{\infty} a^{k-1} c\left(\frac{m'n}{a}\right) q^{m'a}.$$

Which m' and a give q^m? Need $a \mid (m,n)$ for $a > 0$ and $m'a = m$, so the coefficient is $a^{k-1} c\left(mn/a^2\right)$. The sum of these is $\gamma(m)$. ☐

Corollary 1.5.9. *T_n preserves M_k and S_k.*

In the case $n = p$,

$$\mathrm{T}_p f = \sum_{m=0}^{\infty} \gamma(m) q^m, \qquad \gamma(m) = \begin{cases} c(mp) + p^{k-1} c\left(\dfrac{m}{p}\right) & p \mid m \\ c(mp) & p \nmid m \end{cases}.$$

1.5.3 Eigenforms

An observation is that the dimensions of $\mathrm{M}_4, \mathrm{M}_6, \mathrm{M}_8, \mathrm{M}_{10}, \mathrm{S}_{12}$ are one, so $\mathrm{E}_4, \mathrm{E}_6, \mathrm{E}_8, \mathrm{E}_{10}, \Delta$ are eigenvectors for T_n for all n.

Definition 1.5.10. A function $f \in \mathrm{M}_k$ is an **eigenform** if there exists $\lambda_n \in \mathbb{C}^\times$ such that $\mathrm{T}_n f = \lambda_n f$ for all $n \in \mathbb{Z}_{>0}$.

Lecture 17 Friday 08/11/19

Proposition 1.5.11. *Let $f \in \mathrm{M}_k$ be an eigenform, with $k > 0$, so $\mathrm{T}_n f = \lambda_n f$ for all n. Then if $f = \sum_m c_m q^m$, we have $c_1 \neq 0$ and $\lambda_n c_1 = c_n$ for all $n \geq 1$. In particular, if $c_1 = 1$, then $c_n = \lambda_n$ for all n.*

Proof.

$$\sum_{m=0}^\infty \lambda_n c_m q^m = \lambda_n f = \mathrm{T}_n f = \sum_{m=0}^\infty \gamma(m) q^m, \qquad \gamma(1) = \sum_{a \mid (1,n)} a^{k-1} c(n) = c(n),$$

so $\lambda_n c_1 = c_n$. Suppose $c_1 = 0$. Then $c_n = 0$ for all $n \geq 1$, so f is constant. Since $k \neq 0$, this does not happen. ∎

Corollary 1.5.12. *Recall $\Delta(z) = \sum_n \tau(n) q^n$. Then*

- $\tau(mn) = \tau(n) \tau(m)$ *if* $(m,n) = 1$, *and*
- $\tau\left(p^{r+1}\right) = \tau(p) \tau(p^r) - p^{11} \tau\left(p^{r-1}\right)$.

Proof. $\Delta \in \mathrm{S}_{12}$ is one-dimensional, so there exists λ_n such that $\mathrm{T}_n \Delta = \lambda_n \Delta$. Proposition 1.5.11 implies that $\lambda_n = \tau(n)$ for all n. Thus

- $\tau(mn) \Delta = \lambda_{mn} \Delta = \mathrm{T}_{mn} \Delta = \mathrm{T}_m \mathrm{T}_n \Delta = \lambda_m \lambda_n \Delta = \tau(m) \tau(n) \Delta$, and
- $\tau\left(p^{r+1}\right) \Delta = \mathrm{T}_{p^{r+1}} \Delta = \mathrm{T}_p \mathrm{T}_{p^r} \Delta - p^{11} \mathrm{T}_{p^{r-1}} \Delta = \left(\tau(p) \tau(p^r) - p^{11} \tau\left(p^{r-1}\right)\right) \Delta$.

∎

In fact, the same argument shows if $f \in \mathrm{M}_k$ for $k > 0$ is an eigenform, with q-coefficient one, a **normalised eigenform**, and $f = \sum_{n=0}^\infty c_n q^n$, then

- $c_{nm} = c_n c_m$ if $(n,m) = 1$, and
- $c_{p^{r+1}} = c_p c_{p^r} - p^{k-1} c_{p^{r-1}}$.

Proposition 1.5.13. E_k *is an eigenform for all* k.

Proof. It suffices to show $\mathrm{T}_p \mathrm{E}_k = \lambda_p \mathrm{E}_k$ for all primes p. Recall E_k is a constant multiple of G_k, where $\mathrm{G}_k(L) = \sum_{w \in L, \ w \neq 0} 1/w^k$. Now

$$(\mathrm{T}_p f)(L) = \sum_{L' \subseteq_p L} \sum_{w \in L', \ w \neq 0} \frac{1}{w^k} = \sum_{w \in L, \ w \neq 0} c_w \frac{1}{w_k}, \qquad c_w = \#\left\{L' \subseteq_p L \mid w \in L'\right\}.$$

Note that $pL \subseteq L' \subseteq L$. If $w \in pL$, then $w \in L'$ for all $L' \subseteq_p L$, and there are $p+1$ of these. If $w \notin pL$, then $pL \subseteq_{p^2} L$ and $pL \subsetneq pL + \mathbb{Z}w \subsetneq L$, so $pL \subsetneq_p pL + \mathbb{Z}w$ and $pL + \mathbb{Z}w \subsetneq_p L$. In this case there exists a unique lattice of index p containing w. Thus

$$\begin{aligned} \mathrm{T}_p \mathrm{G}_k(L) &= \sum_{w \in L \setminus pL} \frac{1}{w^k} + \sum_{w \in pL, \ w \neq 0} (p+1) \frac{1}{w^k} = \sum_{w \in L, \ w \neq 0} \frac{1}{w^k} + p \sum_{w \in pL, \ w \neq 0} \frac{1}{w^k} \\ &= \mathrm{G}_k(L) + p \sum_{w \in L, \ w \neq 0} \frac{1}{(pw)^k} = \mathrm{G}_k(L) + p^{1-k} \sum_{w \in L} \frac{1}{w^k} = \left(1 + p^{1-k}\right) \mathrm{G}_k(L), \end{aligned}$$

so $\mathrm{T}_p \mathrm{E}_k = \left(1 + p^{k-1}\right) \mathrm{E}_k$. ∎

A question is does M_k have a basis of eigenforms for all k? By linear algebra, there exist nice classes of operators that are guaranteed to admit bases of eigenvectors, such as self-adjoint, or more generally, normal operators.

1.5.4 Hermitian pairings

Let V be a $\mathbb{C}$-vector space and $\langle -, - \rangle : V \times V \to \mathbb{C}$ a **Hermitian pairing**. That is,

- $\langle \lambda v + w, x \rangle = \lambda \langle v, x \rangle + \langle w, x \rangle$,
- $\langle x, y \rangle = \overline{\langle y, x \rangle}$, and
- $\langle x, x \rangle > 0$ for all $x \neq 0$.

Example. The standard pairing

$$\begin{array}{ccc} \mathbb{C}^n \times \mathbb{C}^n & \longrightarrow & \mathbb{C} \\ \langle z, w \rangle & \longmapsto & \sum_{i=1}^n z_i \overline{w_i} \end{array}.$$

Definition 1.5.14. Let $A : V \to V$ be $\mathbb{C}$-linear, and $\langle -, - \rangle : V \times V \to \mathbb{C}$ Hermitian. Then the **adjoint** $A^* : V \to V$ is the unique linear map $V \to V$ such that

$$\langle Av, w \rangle = \langle v, A^* w \rangle .$$

We say A is **self-adjoint** if $A^* = A$, and **normal** if A^* commutes with A.

Theorem 1.5.15. *If A is normal, then A has a basis of eigenvectors.*

Lecture 18 Monday 11/11/19

Lemma 1.5.16. $A^{**} = A$.

Proof. For all $v, w \in V$,

$$\langle v, A^{**} w \rangle = \langle A^* v, w \rangle = \overline{\langle w, A^* v \rangle} = \overline{\langle Aw, v \rangle} = \langle v, Aw \rangle ,$$

so $A^{**} w = Aw$ for all $w \in V$. ☐

Definition 1.5.17. If $W \subseteq V$, let

$$W^\perp = \{ v \in V \mid \forall w \in W, \ \langle v, w \rangle = 0 \} .$$

Proposition 1.5.18. $\mathrm{Im}\, A^* = (\mathrm{Ker}\, A)^\perp$.

Proof. $\langle v, A^* w \rangle = \langle Av, w \rangle = 0$ if $v \in \mathrm{Ker}\, A$. So $\mathrm{Im}\, A^* \subseteq (\mathrm{Ker}\, A)^\perp$, so $\mathrm{rk}\, A^* \leq \mathrm{rk}\, A$. The same argument with A^* in place of A implies that $\mathrm{rk}\, A = \mathrm{rk}\, A^{**} \leq \mathrm{rk}\, A^*$. So $\mathrm{rk}\, A^* = \mathrm{rk}\, A$, so $\mathrm{Im}\, A^* = (\mathrm{Ker}\, A)^\perp$. ☐

In particular, $\mathrm{Im}\, A^* \cap \mathrm{Ker}\, A = \{0\}$ and $\dim \mathrm{Im}\, A^* + \dim \mathrm{Ker}\, A = \mathrm{rk}\, A^* + n - \mathrm{rk}\, A = n$. So $V = \mathrm{Im}\, A^* \oplus \mathrm{Ker}\, A$.

Theorem 1.5.19 (Spectral theorem for normal operators)**.** *If A and A^* commute, then A^* is diagonalisable.*

Proof. Induction on $\dim V$. Then $\dim V = 1$ is clear. Let λ be an eigenvalue of A, and let $A' = A - \lambda \mathrm{I}_V$, so $V = \mathrm{Ker}\, A' \oplus \mathrm{Im}\, A'^*$, where $\dim \mathrm{Ker}\, A' > 0$. Then A commutes with A', and $A'^* = A^* - \overline{\lambda} \mathrm{I}_V$, so A commutes with A'^*. So $AA'^* v = A'^* A v$, so A preserves the image of A'^*. The restriction of $\langle -, - \rangle$ to $\mathrm{Im}\, A'^*$ is still Hermitian on $\mathrm{Im}\, A'^*$ and the restriction of A to $\mathrm{Im}\, A'^*$ is still normal, since its adjoint is the restriction of A^* to $\mathrm{Im}\, A'^*$. By induction A is diagonalisable on $\mathrm{Im}\, A'^*$ and scalar on $\mathrm{Ker}\, A'$, so diagonalisable. ☐

Also the need the folllowing observation.

Proposition 1.5.20. *If $A : V \to V$ and $B : V \to V$ commute, and $V_\lambda = \mathrm{Ker}\, (A - \lambda \mathrm{I}_V)$, then $BV_\lambda = V_\lambda$.*

Proof. If $v \in V_\lambda$, then $ABv = BAv = B\lambda v = \lambda Bv$, so $Bv \in V_\lambda$. ☐

1.5.5 The Petersson inner product

To apply this to modular forms, we need a bilinear pairing on M_k or S_k. The idea is to show that there exists a pairing $\langle -, - \rangle_k : \mathrm{S}_k \times \mathrm{S}_k \to \mathbb{C}$ such that $\langle \mathrm{T}_n f, g \rangle = \langle f, \mathrm{T}_n g \rangle$ for all n, so T_n are self-adjoint, hence diagonalisable.

Definition 1.5.21. Let $f, g \in \mathrm{S}_k$. The **Petersson inner product** $\langle f, g \rangle_k$ is

$$\langle f, g \rangle_k = \iint_{\mathcal{D}} f(z) \overline{g(z)} \frac{(\mathrm{Im}\, z)^k}{(\mathrm{Im}\, z)^2} \, \mathrm{d}x \, \mathrm{d}y = \frac{i}{2} \iint_{\mathcal{D}} f(z) \overline{g(z)} \frac{(\mathrm{Im}\, z)^k}{(\mathrm{Im}\, z)^2} \, \mathrm{d}z \, \mathrm{d}\overline{z}.$$

Here $z = x + iy$ and $\overline{z} = x - iy$, so $\mathrm{d}z \mathrm{d}\overline{z} = (\mathrm{d}x + i \mathrm{d}y) \wedge (\mathrm{d}x - i \mathrm{d}y) = -2i (\mathrm{d}x \wedge \mathrm{d}y)$.

Then

$$f(\gamma z)\overline{g(\gamma z)}(\operatorname{Im}\gamma z)^k = f(z)(cz+d)^k\overline{g(z)(cz+d)^k}\frac{\operatorname{Im} z}{|cz+d|^{2k}} = f(z)\overline{g(z)}(\operatorname{Im} z)^k,$$

and

$$\frac{1}{(\operatorname{Im}\gamma z)^2}\mathrm{d}(\gamma z)(\gamma\overline{z}) = \frac{1}{(\operatorname{Im}\gamma z)^2|cz+d|^4}\mathrm{d}z\mathrm{d}\overline{z} = \frac{1}{(\operatorname{Im} z)^2}\mathrm{d}z\mathrm{d}\overline{z},$$

so for all $U \subseteq \mathbb{H}$,

$$\iint_{\gamma(U)} f(z)\overline{g(z)}\frac{(\operatorname{Im} z)^k}{(\operatorname{Im} z)^2}\ \mathrm{d}z\ \mathrm{d}\overline{z} = \iint_U f(z)\overline{g(z)}\frac{(\operatorname{Im} z)^k}{(\operatorname{Im} z)^2}\ \mathrm{d}z\ \mathrm{d}\overline{z}.$$

Note. This converges for $f, g \in \mathrm{S}_k$, since $f(a+it)$ goes like e^{-t} as $t \to \pm\infty$, and the same for g. If $\langle f, f\rangle = 0$, the integrand vanishes identically, since it lives in $\mathbb{R}_{\geq 0}$. So $f = 0$ on $\mathcal{D}$, hence everywhere. Then

$$\langle \lambda f, g\rangle_k = \lambda\langle f, g\rangle_k, \qquad \langle f, \lambda g\rangle_k = \overline{\lambda}\langle f, g\rangle_k, \qquad \langle f, g\rangle_k = \overline{\langle g, f\rangle_k}.$$

So $\langle -, -\rangle_k$ is Hermitian.

Theorem 1.5.22. $\langle \mathrm{T}_n f, g\rangle_k = \langle f, \mathrm{T}_n g\rangle_k$ *for all* $f, g \in \mathrm{S}_k$ *and* $n \in \mathbb{Z}_{\geq 1}$.

Corollary 1.5.23. *Each* T_n *is diagonalisable on* S_k. *Since* T_n *and* T_m *commute for all* n *and* m, T_m *preserves eigenspaces of* T_n *for all* m. *By induction,* T_m *preserves the simultaneous eigenspaces of* T_n *for all* $n < m$.

Proposition 1.5.24. *Let* $n > \lfloor k/12\rfloor + 1$. *Fix* $\lambda_2, \dots, \lambda_n \in \mathbb{C}$. *The subspace* V *of* S_k *on which* $\mathrm{T}_i = \lambda_i$ *for* $i = 2, \dots, n$ *is zero or one-dimensional.*

Proof. Let $f \in V$, so $f = c_1 q + c_2 q^2 + \dots$. Seen if $\mathrm{T}_i f = \lambda_i f$, then $c_i = \lambda_i c_1$. Also seen that if the first n Fourier coefficients of f vanishes, then $f = 0$, by the $k/12$-formula. So $c_1 \neq 0$ unless $f = 0$. Now if $f, g \in V \setminus \{0\}$, there exists $\lambda \in \mathbb{C}$ such that f and λg have the same q-coefficient, and thus the same first n Fourier coefficients. But then $f - \lambda g = 0$. ☐

Corollary 1.5.25. S_k *admits a basis of eigenforms for all* k.

Proof. Let $n \geq \lfloor k/12\rfloor + 1$. Can diagonalise S_k with respect to the first n Hecke operators. Any simultaneous eigenspace for these is at most one-dimensional, and preserved by all T_n. So each of these is actually an eigenspace for all T_n. ☐

Lecture 19 Friday 15/11/19

Note. If f and g are eigenforms, and f is not a scalar multiple of g, there exists T_n such that $\mathrm{T}_n f = \lambda_n f$ and $\mathrm{T}_n g = \mu_n g$ with $\lambda_n \neq \mu_n$. Then

$$\langle \mathrm{T}_n f, g\rangle_k = \langle \lambda_n f, g\rangle_k = \lambda_n\langle f, g\rangle_k, \qquad \langle f, \mathrm{T}_n g\rangle_k = \langle f, \mu_n g\rangle_k = \overline{\mu_n}\langle f, g\rangle_k,$$

$$\lambda_n\langle f, f\rangle_k = \langle \mathrm{T}_n f, f\rangle_k = \langle f, \mathrm{T}_n f\rangle_k = \overline{\langle \mathrm{T}_n f, f\rangle_k} = \overline{\lambda_n}\langle f, f\rangle_k.$$

So $\lambda_n = \overline{\lambda_n}$ and $\mu_n = \overline{\mu_n}$. Then $(\lambda_n - \mu_n)\langle f, g\rangle_k = 0$, so $\langle f, g\rangle_k = 0$.

The formula for T_n on q-expansions implies that T_n takes a q-expansion with $\mathbb{Z}$ coefficients to another such. Saw that the space of modular forms with integral q-expansions is spanned by

$$\mathrm{E}_4^n\mathrm{E}_6^m, \dots, \mathrm{E}_4^{n-3\lfloor n/3\rfloor}\mathrm{E}_6^m\Delta^{\lfloor n/3\rfloor}, \qquad k = 4n + 6m, \qquad n, m > 0,$$

where $m \in \{0, 1\}$ is minimal, so the matrix of T_n with respect to this basis has integer entries. Thus the characteristic polynomial of T_n on S_k has integer coefficients, so the eigenvalues of T_n are algebraic integers.

Example. Can ask when modular forms are congruent modulo p. In fact $\mathrm{E}_{12} \equiv \Delta \mod 691$.

Ribet 1970s proved that when an Eisenstein series of suitable weight is congruent modulo p to a cusp form, can use the Galois representation attached to that cusp form to construct elements of ideal class groups of cyclotomic fields.

1.6 L-functions

1.6.1 Dirichlet L-functions

Definition 1.6.1. Let $\{a_n\}_{n\geq 1}$ be a sequence of complex numbers, usually algebraic integers. The **Dirichlet series** attached to a_n is the formal series $\sum_{n=1}^{\infty} a_n n^{-s}$, thought of as a function of $s \in \mathbb{C}$.

Example. $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$.

In general, if $|a_n| \leq Cn^k$, then the corresponding series converges absolutely for $\operatorname{Re} s > k+1$.

Example. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a **primitive character**, that is does not factor through $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ for $m \mid N$ such that $m \neq N$. Set

$$a_n = \begin{cases} \chi(n) & (n,N) = 1 \\ 0 & (n,N) \neq 1 \end{cases}.$$

Then

$$\mathrm{L}(s,\chi) = \sum_n a_n n^{-s}$$

is the **Dirichlet L-function** attached to χ.

In both these examples, and many others,

- these series have meromorphic, and often analytic, continuations to all of $\mathbb{C}$,
- there is a **functional equation** relating values at s and $k-s$ for some k, and
- there is an **Euler product**.

Example.

$$\zeta(s) = 2^s \pi^{s-1} \sin\tfrac{\pi s}{2} \Gamma(1-s) \zeta(1-s), \qquad \zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}, \qquad \mathrm{L}(s,\chi) = \prod_{p\nmid N} \frac{1}{1-\chi(p) p^{-s}}.$$

1.6.2 Hecke L-functions

Let $f = \sum_{n=0}^{\infty} a_n q^n \in \mathrm{M}_k$. Define

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

Example. Let $f = \mathrm{E}_k' = (-1)^{k/2} \mathrm{b}_k/2k + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$. Then

$$\mathrm{L}(s,f) = \sum_{n=1}^{\infty} \sigma_{k-1}(n) n^{-s} = \prod_{p \text{ prime}} \frac{1}{1-\sigma_{k-1}(p) p^{-s}} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}} \cdot \frac{1}{1-p^{k-1}p^{-s}} = \zeta(s) \zeta(s-k+1),$$

since $\sigma_{k-1}(mn) = \sigma_{k-1}(m) \sigma_{k-1}(n)$ for $(m,n) = 1$ and $\sigma_{k-1}(p^r) = 1 + \dots + p^{r(k-1)}$.

Lecture 20 Friday 15/11/19

Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a cusp form. Recall that Hasse implies that $|a_n| \leq Cn^{k/2}$, so gives absolute convergence of $\mathrm{L}(s,f)$ for $\operatorname{Re} s > k/2 + 1$.

Theorem 1.6.2.

1. *$\mathrm{L}(s,f)$ extends to a holomorphic function on all of $\mathbb{C}$.*
2. *Set $\mathrm{R}(s,f) = (2\pi)^{-s} \Gamma(s) \mathrm{L}(s,f)$. Then*

$$\mathrm{R}(s,f) = (-1)^{\frac{k}{2}} \mathrm{R}(k-s,f).$$

3. *If f is a normalised eigenform, then*

$$\mathrm{L}(s,f) = \prod_{p \text{ prime}} \frac{1}{1-a_p p^{-s} + p^{k-1} p^{-2s}}.$$

Definition 1.6.3. The infinite product $\prod_{n=1}^{\infty}(1+c_n)$ **converges** if $\lim_{N\to\infty}\prod_{n=1}^{N}(1+c_n)$ converges to a non-zero number, if and only if $\sum_{n=1}^{\infty}\log(1+c_n)$ converges. Then $\prod_{n=1}^{\infty}(1+c_n)$ **converges absolutely** if $\prod_{n=1}^{\infty}(1+|c_n|)$ converges.

Lemma 1.6.4. *$\prod_{n=1}^{\infty}(1+c_n)$ converges absolutely if and only if $\sum_{n=1}^{\infty}|c_n|$ converges.*

Proof.

$$\sum_{n=1}^{N}|c_n| \le \prod_{n=1}^{N}(1+|c_n|) \le \prod_{n=1}^{N} e^{|c_n|} \le e^{\sum_{n=1}^{\infty}|c_n|}.$$

$\square$

Proof of Theorem 1.6.2. Recall that $\Gamma(s)=\int_0^{\infty} t^{s-1}e^{-t}\,\mathrm{d}t$ is meromorphic on $\mathbb{H}$, with poles at $\mathbb{Z}_{\le 0}$ and never zero, and satisfies $\Gamma(s+1)=s\Gamma(s)$ so $\Gamma(n)=(n-1)!$. Substituting $t\mapsto 2\pi nt$ in $\Gamma(s)$,

$$\Gamma(s)=\int_0^{\infty}(2\pi nt)^{s-1}e^{-2\pi nt}(2\pi n)\,\mathrm{d}t=(2\pi n)^s\int_0^{\infty}t^{s-1}e^{-2\pi nt}\,\mathrm{d}t,$$

so

$$\mathrm{L}(s,f)=\sum_{n=1}^{\infty}a_n n^{-s}=\sum_{n=1}^{\infty}a_n\frac{(2\pi)^s}{\Gamma(s)}\int_0^{\infty}t^{s-1}e^{-2\pi nt}\,\mathrm{d}t.$$

Then

$$\begin{aligned}
\mathrm{R}(s,f)=\frac{\Gamma(s)}{(2\pi)^s}\mathrm{L}(s,f)&=\sum_{n=1}^{\infty}a_n\int_0^{\infty}t^{s-1}e^{-2\pi nt}\,\mathrm{d}t=\int_0^{\infty}t^{s-1}\sum_{n=1}^{\infty}a_ne^{-2\pi nt}\,\mathrm{d}t=\int_0^{\infty}t^{s-1}f(it)\,\mathrm{d}t\\
&=\int_0^1 t^{s-1}f(it)\,\mathrm{d}t+\int_1^{\infty}t^{s-1}f(it)\,\mathrm{d}t=\int_1^{\infty}\left(\frac{1}{t}\right)^{s-1}f\left(\frac{i}{t}\right)\mathrm{d}\left(\frac{1}{t}\right)+\int_1^{\infty}t^{s-1}f(it)\,\mathrm{d}t\\
&=\int_1^{\infty}\left(t^{-s-1}(it)^k f(it)+t^{s-1}f(it)\right)\mathrm{d}t=\int_1^{\infty}f(it)\left((-1)^{\frac{k}{2}}t^{k-s-1}+t^{s-1}\right)\mathrm{d}t,
\end{aligned}$$

1. $\mathrm{R}(s,f)$ converges independently of s uniformly for s in a compact subset of $\mathbb{C}$, so it is holomorphic in s, and extends to a holomorphic function on $\mathbb{C}$. Then $\mathrm{L}(s,f)=(2\pi)^s\Gamma(s)^{-1}\mathrm{R}(s,f)$, so $\mathrm{L}(s,f)$ is holomorphic since $\Gamma(s)$ is non-vanishing.

2. $\mathrm{R}(s,f)$ is symmetric up to a sign under $s\mapsto k-s$, so $\mathrm{R}(s,f)=(-1)^{k/2}\mathrm{R}(k-s,f)$.

3. Now assume f is a normalised eigenform, so $f=\sum_{n=1}^{\infty}a_nq^n$ with $a_1=1$ and $\mathrm{T}_nf=a_nf$. Then $a_{nm}=a_na_m$ if $(n,m)=1$, so

$$\mathrm{L}(s,f)=\sum_n a_nn^{-s}=\prod_{p\text{ prime}}\sum_{k=0}^{\infty}a_{p^k}p^{-ks},$$

a power series in p^{-s}. Fix p, and consider

$$\left(1-a_pp^{-s}+p^{k-1}p^{-2s}\right)\sum_{k=0}^{\infty}a_{p^k}p^{-ks}.$$

The p^0 coefficient is $a_1=1$, the p^1 coefficient is $a_pp^{-s}-a_pp^{-s}=0$, and the p^{r+1} coefficient is

$$a_{p^{r+1}}p^{-(r+1)s}-a_pa_{p^r}p^{-(r+1)s}+p^{k-1}a_{p^{r-1}}p^{-(r+1)s}=\left(a_{p^{r+1}}-a_pa_{p^r}+p^{k-1}a_{p^{r-1}}\right)p^{-(r+1)s}=0,$$

since $a_{p^{r+1}}=a_pa_{p^r}-p^{k-1}a_{p^{r-1}}$. So

$$\mathrm{L}(s,f)=\prod_{p\text{ prime}}\sum_{k=0}^{\infty}a_{p^k}p^{-ks}=\prod_{p\text{ prime}}\frac{1}{1-a_pp^{-s}+p^{k-1}p^{-2s}}.$$

$\square$

Lecture 21 is a problem class. Lecture 21 Monday 18/11/19