MODULAR FORMS

Frits Beukers

November 30, 2011

Contents

1 The modular group

1.1 Definition

Consider the upper half plane

$$\mathcal{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}.$$

Let $\mathrm{SL}(2,\mathbb{R})$ be the group of real 2×2-matrices with determinant 1. The group $\mathrm{SL}(2,\mathbb{R})$ acts on $\mathcal{H}$ via

$$\phi_{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} : \tau \mapsto \frac{a\tau+b}{c\tau+d}.$$

Lemma 1.1.1 *Suppose $\tau = x+iy \in \mathcal{H}$. Then, for any $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$ we have*

$$\mathrm{Im}\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{y}{|c\tau+d|^2}.$$

In particular, $\phi_M(\tau) \in \mathcal{H}$.

Proof. Notice that

$$\begin{aligned}
\mathrm{Im}\left(\frac{a\tau+b}{c\tau+d}\right) &= \mathrm{Im}\frac{(a\tau+b)(c\overline{\tau}+d)}{|c\tau+d|^2} \\
&= \mathrm{Im}\frac{ac\tau\overline{\tau}+bd+ad\tau+bc\overline{\tau}}{|c\tau+d|^2} \\
&= \mathrm{Im}\frac{ad(x+iy)+bc(x-iy)}{|c\tau+d|^2} \\
&= \mathrm{Im}\frac{(ad-bc)iy}{|c\tau+d|^2} = \frac{y}{|c\tau+d|^2} > 0.
\end{aligned}$$

□

One easily checks that $\phi_M \circ \phi_{M'} = \phi_{MM'}$ and $\phi_M = \mathrm{Id} \iff M = \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. From now on we say that $M \in \mathrm{SL}(2,\mathbb{R})$ acts on $\mathcal{H}$ when we mean ϕ_M. Also note that it is actually the group $\mathrm{SL}(2,\mathbb{R})/\{\pm 1\}$ which acts on $\mathcal{H}$.
We now compute the *fixpoints* of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. That is, we determine $\tau_0 \in \mathcal{H}$ such that

$$\tau_0 = \frac{a\tau_0+b}{c\tau_0+d}.$$

It immediately follows that $c\tau_0^2 + (d-a)\tau_0 - b$. Hence, when $c \neq 0$,

$$\tau_0 = \frac{a-d+\sqrt{(a-d)^2+4bc}}{2c}.$$

The discriminant equals $(a-d)^2+4bc = (a+d)^2 - 4(ad-bc) = (a+d)^2 - 4$. So we can distinguish the following cases

$|a+d| > 2$. There are two real fixpoints and we call the transformation *hyperbolic.*

$|a+d| < 2$. There are two complex fixpoints, one in the upper half plane. We call the transfomation *elliptic.*

$|a+d| = 2$. There is precisely one real fixpoint and we call the transformation *parabolic*.

When $c = 0$ we have the transformation $\tau \mapsto \frac{a\tau+b}{d}$. In that case we call $i\infty$ (the point at infinity) a fixpoint. When $a \neq d$ we get the extra fixpoint $\tau_0 = b/(d-a)$. In the first case we have that $ad = 1$ and $a = d = \pm 1$. Hence $|a + d| = 2$ and we call our transformation again parabolic. When $a \neq d$ it follows from $ad = 1$ that $|a+d| > 2$ and we call our transformation again hyperbolic.

1.2 SL(2, ℤ)

We define

$$\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}.$$

We distinguish two special elements of $\mathrm{SL}(2,\mathbb{Z})$ namely

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

corresponding to

$$T : \tau \mapsto \tau + 1 \qquad S : \tau \mapsto \frac{-1}{\tau}.$$

Theorem 1.2.1 *The group* $\mathrm{SL}(2,\mathbb{Z})$ *is generated by* S *and* T*.*

Proof. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ and apply the following algorithm.

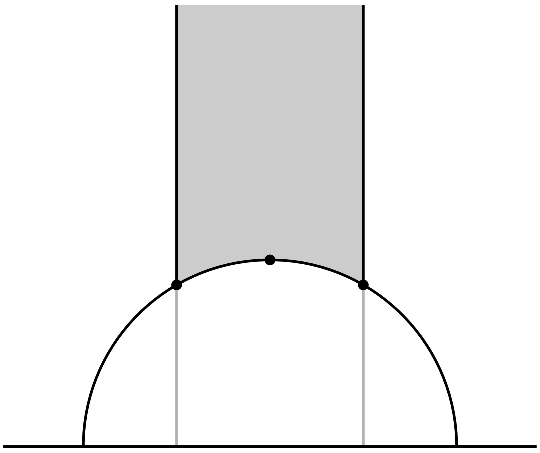
1. If $c = 0$, then terminate.
2. Choose $n \in \mathbb{Z}$ such that $|a + nc| \leq |c|/2$.
3. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} := \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}$.
4. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ -a & -b \end{pmatrix}$.
5. Goto step (1).

After step (4) the new value of $|c|$ is at most $1/2$ times the original value of $|c|$. Hence after a finite number of loops we obtain $c = 0$ and we are left with a matrix of the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$. Since $ad = 1$ and $a, d \in \mathbb{Z}$ we have either $a = d = 1$ or $a = d = -1$. In the first case we verify that our matrix equals T^b, in the second case S^2T^{-b}, since $S^2 = -\mathrm{Id}$. □

In $\mathcal{H}$ we consider the so-called *fundamental domain* of $\mathrm{SL}(2,\mathbb{Z})/\pm 1$. Define

$$F = \{\tau \in \mathcal{H} \mid |\mathrm{Re}\tau| \leq 1/2, |\tau| \geq 1\}.$$

We say that $\tau, \tau' \in \mathcal{H}$ are $\mathrm{SL}(2,\mathbb{Z})$-equivalent if there exists $M \in \mathrm{SL}(2,\mathbb{Z})$ such that $\tau' = M\tau$. The equivalence relation is indicated by $\sim$.



Theorem 1.2.2 *1. To every $\tau_0 \in \mathcal{H}$ there exists $\tau_1 \in F$ which is $\mathrm{SL}(2,\mathbb{Z})$-equivalent to τ_0.*

2. Let $\tau_0, \tau_1 \in F$ be distinct and suppose that $\tau_1 \sim \tau_0$. Then $\tau_1, \tau_0 \in \partial F$ and we have either $\tau_1 = \tau_0 \pm 1$ or $\tau_1 = -1/\tau_0$, or both (when $\tau_0 = e^{2\pi i/3}$ or $e^{\pi i/3}$).

Proof. For part (1) we perform the following algorithm

1. Choose $n \in \mathbb{Z}$ such that $|\mathrm{Re}\tau_0 + n| \le 1/2$ and put $\tau_0 := \tau_0 + n$.
2. If $|\tau_0| \ge 1$ we are done. If $|\tau_0| < 1$ we put $\tau_0 := -1/\tau_0$ and go to the previous step.

We assert that this process terminates after a finite number of steps. Notice that $\mathrm{Im}(-1/\tau_0) = \tau_0/|\tau_0|^2$. So every time we enter step (2) with $|\tau_0|^2 \le 1/2$, the new value of τ_0 will have imaginary part at least twice as large as the original one. So after a finite number of steps we reach a situation where $|\tau_0|^2 > 1/2$. When $|\tau_0| \ge 1$ we are done, but when $1/2 < |\tau_0|^2 < 1$ we easily verify that $-1/\tau_0 \in F \cup T(F) \cup T^{-1}(F)$. So at most one more translation is required to end in F.
Now suppose that $\tau_1 \sim \tau_0$ and $\tau_0, \tau_1 \in F$. Suppose $\tau_1 = \frac{a\tau_0+b}{c\tau_0+d}$. Then

$$\mathrm{Im}\tau_1 = \frac{\mathrm{Im}\tau_0}{|c\tau_0 + d|^2} = \frac{\mathrm{Im}\tau_0}{c^2|\tau_0|^2 + 2cd\mathrm{Re}\tau_0 + d^2} \tag{1}$$

Using $|\tau_0| \ge 1$ and $2|\mathrm{Re}\tau_0| \le 1$ we derive

$$c^2|\tau_0|^2 + 2cd\mathrm{Re}\tau_0 + d^2 \ge c^2 - |cd| + d^2 \ge 1.$$

Since c, d are integers that cannot be both zero. Hence $\mathrm{Im}\tau_1 \le \mathrm{Im}\tau_0$. Similarly we see that $\mathrm{Im}\tau_0 \le \mathrm{Im}\tau_1$. Hence $\mathrm{Im}\tau_1 = \mathrm{Im}\tau_0$. From (1) we now deduce that

$$1 = c^2|\tau_0|^2 + 2cd\mathrm{Re}\tau_0 + d^2 \ge c^2 - |cd| + d^2 \ge 1$$

and hence all inequalities are equalities. In particular when $c = 0$ we find $d = \pm 1$ and $\tau_1 = \tau_0 + b/d$. Hence τ_1, τ_0 are on the vertical lines $\mathrm{Re}\tau = 1/2$. When $c \ne 0$ we deduce that $c^2|\tau_0|^2 = 1$, hence $|c| = 1, |\tau_0| = 1$. If $d = 0$ then $\tau_1 = -1/\tau_0$. If $d \ne 0$ we derive in addition that $2|\mathrm{Re}\tau_0| = 1$. This is the situation where $\tau_0 = e^{2\pi i/3}$ or $e^{\pi i/3}$.

□

2 First examples of modular forms

2.1 The Poisson summation formula

The simplest examples of modular forms are theta-series and Eisenstein series. To derive their special modular properties we need the following useful theorem.

Theorem 2.1.1 (Poisson summation formula) *Let $f : \mathbb{R} \to \mathbb{C}$ be a function which is twice continuously differentiable and suppose that*

1. $\int_{-\infty}^{\infty} |f(x)|dx$ *converges.*
2. $\int_{-\infty}^{\infty} |\hat{f}(y)|dy$ *converges, where*

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{-2\pi ixy} f(x)dx$$

   is the Fourier transform of f.

3. *The infinite series* $\sum_{n\in\mathbb{Z}} |f(n+x)|$ *converges uniformly for x in any compact interval.*
4. *The infinite series* $\sum_{m\in\mathbb{Z}} |\hat{f}(n+y)|dy$ *converges uniformly for y in any compact interval.*

Then ,for any $x \in \mathbb{R}$,

$$\sum_{n\in\mathbb{Z}} f(n+x) = \sum_{m\in\mathbb{Z}} \hat{f}(m)e^{2\pi imx}.$$

In particular,

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{m\in\mathbb{Z}} \hat{f}(m).$$

Proof (sketch). The function $F(x) := \sum_{n\in\mathbb{Z}} f(n+x)$ is periodic with period 1. So it has a Fourier expansion

$$F(x) = \sum_{m\in\mathbb{Z}} F_m e^{2\pi imx}$$

where

$$F_m = \int_0^1 F(x)e^{-2\pi imx}dx.$$

Note that the latter integral can be rewritten as

$$\begin{aligned} F_m &= \int_0^1 \sum_{n\in\mathbb{Z}} f(n+x)e^{-2\pi imx}dx \\ &= \int_{-\infty}^{\infty} f(x)e^{-2\pi imx}dx = \hat{f}(m) \end{aligned}$$

Hence

$$\sum_{n\in\mathbb{Z}} f(n+x) = \sum_{m\in\mathbb{Z}} \hat{f}(m)e^{2\pi imx}.$$

□

2.2 The theta-series

The following function is classical since it occurs standard in the solution of the socalled heat equation. Consider the function

$$\theta(\tau) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 \tau}$$

which converges for every $\tau \in \mathcal{H}$.

Theorem 2.2.1 *We have for every $\tau \in \mathcal{H}$,*

1. $\theta(\tau + 2) = \theta(\tau)$
2. $\theta(-1/\tau) = \sqrt{\tau/i}\ \theta(\tau)$

Here $\sqrt{\tau/i}$ is chosen with positive real part.

Proof. We apply the Poisson summation formula to $f(x) = e^{\pi i x^2 \tau}$. Then

$$\begin{aligned} \hat{f}(y) &= \int_{-\infty}^{\infty} \exp(\pi i x^2 \tau - 2\pi i x y) dx \\ &= \int_{-\infty}^{\infty} \exp(\pi i \tau (x - y/\tau)^2 - \pi i y^2/\tau) dx \\ &= \exp(-\pi i y^2/\tau) \int_{-\infty}^{\infty} \exp(\pi i \tau x^2) dx \end{aligned}$$

The last integral is standard and equals $\sqrt{i/\tau}$. Hence

$$\sum_{n\in\mathbb{Z}} e^{\pi i n^2 \tau} = \sqrt{\frac{i}{\tau}} \sum_{m\in\mathbb{Z}} e^{-\pi i m^2/\tau}.$$

□

2.3 Eisenstein series

For every $k \in \mathbb{Z}_{k\ge 3}$ we define

$$G_k(\tau) = \frac{(k-1)!}{2(2\pi i)^k} \sum_{m,n}{}' \frac{1}{(m\tau + n)^k}$$

as function of $\tau \in \mathcal{H}$. The $'$ in the summation means that we skip the term with $m = n = 0$. When $k \ge 3$ the double series is absolutely convergent. Notice also that $G_k(\tau) \equiv 0$ when k is odd. This follows from the antisymmetry in the defining summation.

Theorem 2.3.1 *Let B_k be the k-th Bernoulli number and denote $q = e^{2\pi i \tau}$. Let σ_r be the sum of divisors function given by $\sigma_r(n) = \sum_{d|n} d^r$. Then, for all $\tau \in \mathcal{H}$,*

$$G_k(\tau) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Recall that

$$\frac{z}{e^z - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} z^k.$$

For the proof of Theorem 2.3.1 we need the following Lemmas.

Lemma 2.3.2 (Euler) *For any even $k \in \mathbb{Z}_{\geq 2}$ we have*

$$\zeta(k) := \sum_{n=1}^{\infty} \frac{1}{n^k} = -\frac{(2\pi i)^k}{(k-1)!} \frac{B_k}{2k}.$$

Lemma 2.3.3 *Let $k \in \mathbb{Z}_{\geq 2}$. Then, for any $z \in \mathcal{H}$ we have*

$$\sum_{n \in \mathbb{Z}} \frac{1}{(n-z)^k} = \frac{(2\pi i)^k}{(k-1)!} \sum_{r=1}^{\infty} r^{k-1} e^{2\pi i r z}.$$

Proof. We apply the Poisson summation formula to $f(x) = 1/(x-z)^k$. Notice that

$$\hat{f}(r) = \int_{-\infty}^{\infty} \frac{e^{2\pi i r x}}{(x-z)^k}\, dx.$$

When $r \geq 0$ we integrate over a closed loop Γ_R consisting of the interval $[-R, R]$ and the half circle $Re^{i\phi}$ with $0 \leq \phi \leq \pi$. Then we let $R \to \infty$. The integral over the half circle goes to 0, the integral over the segment to $\hat{f}(r)$. On the other hand, according to Cauchy's residue theorem, for $R > |z|$ the integral over Γ_R equals $2\pi i$ times the residue of $e^{2\pi i r x}/(x-z)^k$ at the pole $x = z$. This equals $(2\pi i r)^k e^{2\pi i r z}/(k-1)!$. Hence, when $m \geq 0$,

$$\hat{f}(r) = \frac{(2\pi i)^k}{(k-1)!} r^{k-1}.$$

When $r < 0$ we can use the alternative contour consisting of $[-R, R]$ and the half circle in the lower half plane. Since this alternative contour has no zeros in its interior, Cauchy's theorem gives us $\hat{f}(r) = 0$ when $r < 0$. Poisson summation now gives us the desired formula.

□

Notice that the series in $e^{2\pi i z}$ in Lemma 2.3.3 is the $k-11$-st derivative of $\frac{-\pi}{(k-1)!}(1/2 + \sum_{r=1}^{\infty} e^{2\pi i r z}$ which equals $\frac{-\pi}{(k-1)!} \cot \pi z$. Conversely, Lemma 2.3.3 could also have been derived by differentiation of *Euler's identity*

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

which holds for all $z \notin \mathbb{Z}$.

Proof of Theorem 2.3.1. Recall that when $k \in \mathbb{Z}_{\geq 2}$ is even,

$$\begin{aligned} G_k(\tau) &= \frac{(k-1)!}{2(2\pi i)^k} \sum_{m,n}{}' \frac{1}{(m\tau + n)^k} \\ &= \frac{(k-1)!}{2(2\pi i)^k} \left(\sum_{n}{}' \frac{1}{n^k} + 2 \sum_{m=1}^{\infty} \sum_{n \in \mathbb{Z}} \frac{1}{(-m\tau + n)^k} \right) \end{aligned}$$

The first term reads $2(k-1)!\zeta(k)/2(2\pi i)^k$ which is equal to $-B_k/2k$ according to Euler's lemma. We use Lemma 2.3.3 with $z = m\tau$ to compute the second term. We obtain

$$G_k(\tau) = -\frac{B_k}{2k} + \sum_{m=1}^{\infty} \sum_{r=1}^{\infty} r^{k-1} e^{2\pi i r m \tau}. \tag{2}$$

Put $q = e^{2\pi i \tau}$ and group the terms to a power series in q. We get

$$G_k(\tau) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

□

Examples,

$$\begin{aligned} G_4(\tau) &= \frac{1}{240} + q + 9q^2 + 28q^3 + 73q^4 + \cdots \\ G_6(\tau) &= -\frac{1}{504} + q + 33q^2 + 244q^3 + 1057q^4 + \cdots \\ G_8(\tau) &= \frac{1}{480} + q + 129q^2 + 2188q^3 + \cdots \end{aligned}$$

When we carry out the summation over m in (2) we get

$$G_k(\tau) = -\frac{B_k}{2k} + \sum_{r=1}^{\infty} \frac{r^{k-1}q^r}{1-q^r}.$$

This is the socalled *Lambert series* expansion for G_k.
By their definition, the Eisenstein series have a remarkable set of functional equation. For any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ notice that

$$\begin{aligned} G_k\left(\frac{a\tau+b}{c\tau+d}\right) &= {\sum_{m,n}}' \frac{(c\tau+d)^k}{(m(a\tau+b)+n(c\tau+d))^k} \\ &= (c\tau+d)^k {\sum_{m,n}}' \frac{1}{((ma+nc)\tau+bm+nd)^k} \end{aligned}$$

Because the pair $(ma+nc, bm+nd)$ runs over $\mathbb{Z}^2$ when (m,n) does, the latter summation equals $G_k(\tau)$. Thus we find that

$$G_k\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k G_k(\tau).$$

2.4 Modular forms

Motivated by the examples we define modular functions with respect to $\mathrm{SL}(2,\mathbb{Z})$.

Definition 2.4.1 *Let k be a positive even integer. A holomorphic function f on $\mathcal{H}$ is called a modular form of weight k with respect to* $\mathrm{SL}(2,\mathbb{Z})$ *if the following two conditions hold.*

1. $$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau)$$
   for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ *and all $\tau \in \mathcal{H}$.*

2. *f can be written as a power series in $q = e^{2\pi i\tau}$, convergent for all $|q| < 1$.*

Remarks:

1. Notice that the Eisenstein series we defined satisfy the conditions above.

2. It does not make sense to define modular forms with respect to $\mathrm{SL}(2,\mathbb{Z})$ of odd weight k. For such a form we would have $f(-1/\tau) = \tau^k f(\tau)$ but also $f(1/(-\tau)) = (-\tau)^k f(\tau)$, which is exactly the opposite of $\tau^k f(\tau)$. However when we consider modular forms with respect to subgroups of $\mathrm{SL}(2,\mathbb{Z})$, modular forms of odd weight do make sense.

3. The theta-function is not a modular form with respect to $\mathrm{SL}(2,\mathbb{Z})$ for many reasons. To start with, it seems to have weight 1/2. It is not invariant under $\tau \to \tau+1$ and it is not a power series in q. However, it will turn out to be a modular form with respect to subgroups of $\mathrm{SL}(2,\mathbb{Z})$.

The second condition of our definition comes down to the following. Let f be a modular form. Through the functional equation $f(\tau+1) = f(\tau)$ and the fact that f is holomorphic in $\mathcal{H}$ we deduce that $F(q) := f\left(\frac{\log q}{2\pi i}\right)$, as a function of q, is holomorphic for all q with $0 < |q| < 1$. Hence $q = 0$ is an isolated singularity of $F(q)$. Condition (2) on modular forms simply says that $F(q)$ can be extended holomorphically to $q = 0$. Since $q = 0$ corresponds to $\tau = i\infty$ we say that f is holomorphic at $\tau = i\infty$. In particular a modular form has an expansion as a power series in q which converges for all q with $|q| < 1$. Moreover, if the constant term of the q-expansion of f is zero, we say that f has a zero at $\tau = i\infty$.

2.5 The pseudoform G_2

After having seen $G_4, G_6, \ldots$ it is very tempting to define

$$G_2(\tau) = -\frac{1}{24} + \sum_{r=1}^{\infty} \frac{rq^r}{1-q^r}, \quad q = e^{2\pi i \tau}$$

and hope that it is modular. It turns out to be almost modular.

Theorem 2.5.1 *Let $G_2^*(\tau) = G_2(\tau) + \frac{1}{8\pi \mathrm{Im}(\tau)}$. Then, for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ we have*

$$G_2^*\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 G_2^*(\tau).$$

In particular, this implies that

$$G_2\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 G_2(\tau) - \frac{c(c\tau+d)}{4\pi i}.$$

Proof (sketch) We cannot define G_2 through a series of the form

$$\sum_{m,n}{}' \frac{1}{(m\tau+n)^2}$$

since it does not converge. However, for any $s > 0$ the series

$$\sum_{m,n}{}' \frac{1}{(m\tau+n)^2 |m\tau+n|^s}$$

does converge. It also turns out that the limit as $s \downarrow 0$ exists. For a proof see the appendix to this section. Call this limit $G_2^*(\tau)$. This is known as *Hecke's trick* named after E.Hecke (1925), one of the founders of the classical theory of modular forms. Of course this limit has the desired modular behaviour. Moreover, Hecke showed that $G_2^*(\tau) = G_2(\tau) + 1/8\pi\mathrm{Im}(\tau)$. For a proof of this fact we refer again to the appendix of this section.

□

2.6 The discriminant function

Consider the function

$$\Delta(\tau) = q \prod_{r=1}^{\infty} (1-q^n)^{24}, \quad q = e^{2\pi i \tau}.$$

We will show that it is a modular forms of weight 12. Notice that

$$\begin{aligned} \frac{\Delta'(\tau)}{\Delta(\tau)} &= \frac{d}{d\tau}\left(2\pi i\tau + 24\sum_{r=1}^{\infty}\log(1-q^r)\right) \\ &= 2\pi i\left(1 - 24\sum_{r=1}^{\infty}\frac{rq^r}{1-q^r}\right) \\ &= -48\pi i G_2(\tau) \end{aligned}$$

Using the transformation property of G_2 we find that

$$\frac{\Delta'(-1/\tau)}{\Delta(-1/\tau)} = \tau^2\frac{\Delta'(\tau)}{\Delta(\tau)} + \frac{12}{\tau}.$$

Hence

$$\frac{d}{d\tau}(\log\Delta(-1/\tau)) = \frac{d}{d\tau}(\log(\tau^{12}\Delta(\tau))).$$

After integration and exponentiation we find that there exists $c \neq 0$ such that

$$\Delta(-1/\tau) = c\tau^{12}\Delta(\tau).$$

Substitution of $\tau = i$ and the fact that $\Delta(i) \neq 0$ shows that $c = 1$. Moreover, we have trivially that $\Delta(\tau+1) = \Delta(\tau)$. Since $\tau \to \tau+1$ and $\tau \to -1/\tau$ generate $\mathrm{SL}(2,\mathbb{Z})$ we coinclude that $\Delta(\tau)$ is a modular form of weight 12.
Since the product expansion for $\Delta(\tau)$ converges for all q with $|q| < 1$ we see that $\Delta(\tau)$ is non-zero throughout $\mathcal{H}$ and it has a zero at $i\infty$.
We denote the coefficients of the q-series expansion of $\Delta(\tau)$ by $\tau(n)$. In other words,

$$\begin{aligned} \Delta(\tau) &= \sum_{n=1}^{\infty}\tau(n)q^n \\ &= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + 8405q^7 + \cdots \end{aligned}$$

It was discovered by Ramanujan that $\tau(n)$ is a multiplicative function of n. A proof was given by Mordell around 1916. It was also conjectured by Ramanujan that $|\tau(p)| < 2p^{11/2}$ for all primes p. This is a very special case of the so-called Riemann hypothesis in positive characteristic which was only proved by Deligne around 1973. Another conjecture, which is still unproven yet, is that $\tau(n) \neq 0$ for all n.

2.7 Appendix

In this section we elaborate on Hecke's trick relating G_2 and G_2^*. We start with the function

$$G_2(s,\tau) = \frac{-1}{8\pi^2}\sum_{m,n}{}' \frac{1}{(m\tau+n)^2|m\tau+n|^s}$$

for $\tau \in \mathcal{H}$ and $s > 0$. We rewrite the summation as

$$G_2(s,\tau) = \frac{-1}{8\pi^2}\left(\sum_{n=1}^{\infty}\frac{2}{n^{2+s}} + \sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{2}{(n-m\tau)^2|n-m\tau|^s}\right).$$

For each m we compute the summation over $n\in\mathbb{Z}$ using Poisson summation applied to the function $f_m(x)=\frac{1}{(x-m\tau)^2|x-m\tau|^s}$. Notice

$$\hat{f}_m(r)=\int_{-\infty}^{\infty}\frac{e^{2\pi i r x}}{(x-m\tau)^2|x-m\tau|^s}\,dx.$$

Replace x by mx to obtain

$$\hat{f}_m(r)=\frac{1}{m^{1+s}}\int_{-\infty}^{\infty}\frac{e^{2\pi i r m x}}{(x-\tau)^2|x-\tau|^s}\,dx.$$

By a twofold partial integration it we see that for all $r\ne 0$ we have $|\hat{f}_m(r)|=O(\frac{1}{m^{3+s}r^2})$ where the O-symbol does not depend on s. So we get

$$G_2(s,\tau)=\frac{-1}{4\pi^2}\left(\sum_{n=1}^{\infty}\frac{1}{n^{2+s}}+\sum_{m=1}^{\infty}\sum_{r\ne 0}\hat{f}_m(r)+\sum_{m=1}^{\infty}\hat{f}_m(0)\right). \tag{3}$$

When $s\downarrow 0$ the first summation tends to $-\zeta(2)/4\pi^2=-1/24$. Because of the estimate (independent of s) for $|\hat{f}_m(r)|$ we see that the double summation with $r\ne 0$ converges to the sum

$$\frac{-1}{4\pi^2}\sum_{m=1}^{\infty}\frac{1}{m}\sum_{r\ne 0}\int_{-\infty}^{\infty}\frac{e^{2\pi i r m x}}{(x-\tau)^2}\,dx$$

as $s\downarrow 0$. By residue calculus as in the proof of Lemma 2.3.3 we show that the terms with $r<0$ are zero and the terms with $r>0$ equal $e^{2\pi i m r\tau}$. So the double sum equals

$$\sum_{m=1}^{\infty}\sum_{r=1}^{\infty}re^{2\pi i r m\tau}.$$

Together with the constant term $-1/24$ this adds up to $G_2(\tau)$. It remains to show that the third summation in (3) converges to $1/8\pi\mathrm{Im}(\tau)$ as $s\downarrow 0$. Notice

$$\hat{f}_m(0)=\frac{1}{m^{1+s}}\int_{-\infty}^{\infty}\frac{1}{(x-\tau)^2|x-\tau|^s}\,dx.$$

The latter integral equals

$$\frac{1}{m^{1+s}}\int_{-\infty}^{\infty}\frac{1}{(x-i\mathrm{Im}\tau)^2|x-i\mathrm{Im}\tau|^s}\,dx=\frac{1}{(m\ \mathrm{Im}\tau)^{1+s}}\int_{-\infty}^{\infty}\frac{1}{(x-i)^2|x-i|^s}\,dx.$$

If we replace $(x-i)^2|x-i|^s$ by $(x-i)^{2+s/2}(x+i)^{s/2}$ in the last integral and perform a partial integration we get

$$\int_{-\infty}^{\infty}\frac{1}{(x-i)^2|x-i|^s}\,dx=-\frac{s}{2+s}\int_{-\infty}^{\infty}\frac{1}{(x^2+1)^{1+s/2}}\,dx.$$

Putting everything together we get

$$\sum_{m=1}^{\infty}\hat{f}_m(0)=\frac{s\zeta(1+s)}{2+s}\frac{1}{\mathrm{Im}\tau}^{1+s}\int_{-\infty}^{\infty}\frac{1}{(x^2+1)^{1+s/2}}\,dx.$$

Now we let $s\downarrow 0$. Then $s\zeta(1+s)$ tends to 1 and the integral to π. Hence the sum $\sum_m\hat{f}(0)$ tends to $-\pi/2\mathrm{Im}\tau$. Hence $-(4\pi^2)^{-1}\sum_{m=1}^{\infty}\hat{f}_m(0)$ tends to $\pi/8\mathrm{Im}\tau$, as desired.

3 Elementary properties of modular forms

3.1 Classification

Using the discriminantfunction $\Delta(\tau)$ it is very easy to give a characterisation of all modular forms with respect to $\mathrm{SL}(2,\mathbb{Z})$. First let us repeat that the weight of such a modular form is an even integer.

Theorem 3.1.1 *The only modular forms of weight* 0 *are the constant functions. There are no non-trivial modular forms of weight* 2 *or negative weight.*

Proof. Suppose f is a modular form of weight 0. Hence it is invariant under $\mathrm{SL}(2,\mathbb{Z})$ and its range is determined by the range of values $f(\tau), \tau \in F$, hence the range on $\mathrm{Im}(\tau) \geq \sqrt{3}/2$. In terms of its q-expansion, the range of f coincides with the range for $|q| \leq e^{-\pi\sqrt{3}}$. But this is a compact set and thus we see that $|f|$ attains a local maximum. This is only possible when f is constant.
Now suppose that f has negative weight $k < 0$. Then $g = \Delta^{|k|} f^{12}$ has weight 0 and must be constant. Since Δ has a zero at $i\infty$, the same holds for g. Hence $g \equiv 0$, which implies $f \equiv 0$.
Suppose that f is a modular forms of weight 2. Let $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$ be its q-expansion and $F(\tau) = a_0\tau + \sum_{n=1}^{\infty} a_n q^n/(2\pi i n)$ its integrated form. More explicitly $F'(\tau) = f(\tau)$. From $f(-1/\tau) = \tau^2 f(\tau)$ it follows that

$$\frac{1}{\tau^2} F'\left(-\frac{1}{\tau}\right) = F'(\tau).$$

Integration yields the existence of a constant C such thar $F(-1/\tau) = F(\tau) + C$ for every $\tau \in \mathcal{H}$. In particular $\tau = i$. Hence $F(i) = F(i) + C$ and we conclude that $C = 0$. Also note that $F(-1/(\tau+1)) = F(\tau+1) = F(\tau) + a_0$. This holds for all τ, in particular $\tau = e^{2\pi i/3}$. We find $F(e^{2\pi i/3}) = F(e^{2\pi i/3}) + a_0$ and hence $a_0 = 0$. Thus F is a modular form of weight zero with constant term of its q-expansion equal to zero. We conclude that $F \equiv 0$, hence $f \equiv 0$.

□

Clearly, modular forms of weight k form a $\mathbb{C}$-linear vector space which we denote by M_k. The subspace of forms that vanish in $i\infty$ is called the space of *cusp forms* and is denoted by S_k.
We have seen above that M_k is trivial if $k = 2$ or a negative integer. For all other values of k the space M_k is non-trivial because of the existence of $1 \in M_0$ and $G_k \in M_k$ for $k = 4, 6, \ldots$. Letting $k \geq 4$ and $f \in M_k$ we can choose a constant such that $f - cG_k \in S_k$. Hence $M_k = \mathbb{C}G_k \oplus S_k$. Furthermore, when we have a cusp form $f \in S_k$ then f/Δ is again a modular form, but of weight $k - 12$. Conversely, given any $g \in M_{k-12}$, the form $g\Delta$ is a cusp form of weight k. From these considerations we deduce the following Theorem.

Theorem 3.1.2 *Let* k *be a non-negative even integer. Then*

1. $$\dim(M_k) = \begin{cases} [k/12] \text{ if } k \equiv 2 \pmod{12} \\ [k/12] + 1 \text{ otherwise} \end{cases}$$
2. $12^3\Delta = (240G_4)^3 - (-504G_6)^2$.
3. M_k *is spanned by all* $G_4^a G_6^b$ *with* $4a + 6b = k$.
4. $G_6(i) = 0$ *and* $G_4(\omega) = 0$ *where* $\omega = e^{2\pi i/3}$.
5. G_4 *and* G_6 *are algebraically independent over* $\mathbb{C}$

Proof. When $k < 12$ there cannot be any cusp forms, since S_k is isomorphic to $M_{k-12} = \{0\}$. Hence $\dim(M_k) = 1$ if $k = 0, 4, 6, 8, 10$. We know that M_2 is trivial.
Since $M_k = \mathbb{C}G_k \oplus S_k$ we have $\dim(M_k) = 1 + \dim(S_k) = 1 + \dim(M_{k-12})$. Assertion (1) now follows by induction on k.
To show part (2) we notice that $(240G_4)^3 - (-504G_6)^3$ is a cusp form of weight 12. Dividing it by Δ gives us a modular of weight 0, hence a constant. A straightforward computation gives us

$$(240G_4)^3 - (-504G_6)^2 = 1728q - 41472q^2 + \cdots$$

We see that the constant should be $1728 = 12^3$.
Part (3) follows again by induction and fact (2).
To prove (4) notice that $G_6(-1/\tau) = \tau^6 G_6(\tau)$. We substitute $\tau = i$ to get $G_6(i) = -G_6(i)$, from which our assertion follows. Similarly $G_4(-1/(\tau+1)) = \tau^4 G_4(\tau)$ where we can substitute $\tau = \omega$. We find $G_4(\omega) = \omega G_4(\omega)$ and our assertion follows.
To prove (5) suppose we have a non-trivial polynomial $P \in \mathbb{C}[X,Y]$ such that $P(G_4, G_6) \equiv 0$. We can assume P is not divisible by Y and write $P(X,Y) = \alpha X^m + YQ(X,Y)$ with $\alpha \neq 0$. So, $\alpha G_4^m + G_6 Q(G_4, G_6) \equiv 0$. Substitute $\tau = i$ and we get $\alpha G_4(i)^m = 0$. Hence $G_4(i) = 0$, which is easily contradicted by the fact that $G_4(i) = 0.006065\ldots$.

□

3.2 Consequences

The small values of $\dim(M_k)$ give us many possibilities to create polynomial relations between the G_k and Δ. In the previous setion we have already seen that $(240G_4)^3 - (504G_6)^2 = 12^3\Delta$. Also note that G_8 and G_4^2 are in M_8. But $\dim(M_8) = 1$ so there exists a constant such that $G_8 = cG_4^2$. We easily calculate $G_8 = 120G_4^2$. Comparison of the coefficients yields the identity

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{r=1}^{n-1} \sigma_3(r)\sigma_3(k-r),$$

something that would be quite hard to prove directly.
Another application is the following. The forms G_6^2, G_{12}, Δ all have weight 12. Since $\dim(M_{12}) = 2$ there is a linear relation of the form $G_{12} = \alpha\Delta + \beta G_6^2$. Since

$$\begin{aligned} 24 \cdot 2730 \cdot G_{12} &= 691 + 24 \cdot 2730(q + \cdots) \\ 504^2 G_6^2 &= 1 - 1008q + \cdots \\ \Delta &= q - \cdots \end{aligned}$$

we deduce that

$$24 \cdot 2730 \cdot G_{12} = 691 \cdot 504^2 G_6^2 + (24 \cdot 2730 + 1008 \cdot 691)\Delta.$$

On both sides we have power series expansions with integer coefficients. Consider everything modulo 691. We obtain

$$G_{12} \equiv \Delta \pmod{691}$$

hence

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}$$

for all $n \in \mathbb{N}$.
One may ask what happens if we differentiate a modular form. The result will in general not be a modular form. Let $f \in M_k$. Then, for any $\gamma \in \mathrm{SL}(2,\mathbb{Z})$ it follows by differentation of $f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$ that

$$f'(\gamma(\tau)) \frac{1}{(c\tau + d)^2} = ck(c\tau + d)^{k-1} f(\tau) + (c\tau + d)^k f'(\tau).$$

Hence $f'(\gamma(\tau)) = ck(c\tau+d)^{k+1}f(\tau) + (c\tau+d)^{k+2}f'(\tau)$. Using the identity $G_2(\gamma(\tau)) = (c\tau+d)^2G_2(\tau) - c(c\tau+d)/4\pi i$ we find that $f'(\tau) + 4\pi ikG_2(\tau)f(\tau)$ is a modular form of weight $k+2$. It is now straightforward to derive the following identities

$$\begin{aligned}\frac{1}{2\pi i}G_4'(\tau) &= \frac{7}{10}G_6(\tau) - 8G_2(\tau)G_4(\tau)\\ \frac{1}{2\pi i}G_6'(\tau) &= \frac{10}{21}G_8(\tau) - 12G_2(\tau)G_6(\tau)\end{aligned}$$

A similar, but slightly more involved calculation gives us

$$\frac{1}{2\pi i}G_2'(\tau) = \frac{5}{6}G_4(\tau) - 2G_2(\tau)^2.$$

From these identities we see that the ring $\mathbb{C}[G_2, G_4, G_6]$ is closed under differentiation, a fact first discovered by Ramanujan.

3.3 Modular functions

There are no modular forms of weight zero except the constant ones. However, if we allow for poles we have more possibilities. Let us define

$$j(\tau) = \frac{(240G_2(\tau))^3}{\Delta(\tau)}.$$

This function has no poles in $\mathcal{H}$, however, it does have a pole at $\tau = i\infty$ as can be seen from the Laurent series expansion

$$j(\tau) = \frac{1}{q} + 744 + 196884q^2 + 21493760q^3 + \cdots, q = e^{2\pi i\tau}.$$

Note that this Laurent expansion converges for all $|q| < 1$.

Definition 3.3.1 *A meromorphic function f on $\mathcal{H}$ is called a modular function if*

1. $f\left(\frac{a\tau+b}{c\tau+d}\right) = f(\tau)$ *for all* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$.
2. *There exists $n \in \mathbb{Z}_{\geq 0}$ such that $e^{2\pi in\tau}f(\tau)$ is bounded as $\tau \to i\infty$, i.e f has at worst a pole in $i\infty$. When n is chosen minimal we say that f has a pole of order n at $i\infty$.*

Notice that a modular function f has a Laurent series expansion in $q = e^{2\pi i\tau}$,

$$f(\tau) = c_{-n}q^{-n} + \cdots + c_1q^{-1} + c_0 + c_1q + c_2q^2 + \cdots \tag{4}$$

Definition 3.3.2 *Every modular function with respect to* $\mathrm{SL}(2,\mathbb{Z})$ *can be written as rational function in $j(\tau)$. In other words, the field of modular functions i generated over $\mathbb{C}$ by $j(\tau)$.*

Proof. Let $f(\tau)$ be a modular function. Suppose that it has no poles in $\mathcal{H}$ and that it has a pole of order n at $i\infty$. If $n = 0$ we know that f is constant and we are done. Suppose f has a Laurent expansion given by (4). Then $f - c_nj^n$ is a modular function with a pole of order at most $n-1$. We repeat this argument as many times as necessary and we find that f is polynomial in j.
Now suppose that f has poles $\tau_1, \ldots, \tau_k$ of orders $n_1, \ldots, n_k$. Then $G(\tau) := f(\tau)\prod_{r=1}^{k}(j(\tau) - j(\tau_r))^{n_r}$ is a modular functions without poles in $\mathcal{H}$. According to our previous argument $g(\tau)$ should be a polynomial in j. Hence f itself is rational function of j.

□

The j-invariant has the beautiful property that its function values are in 1-1-correspondence with $SL(2,\mathbb{Z})$-equivalence classes of point in $\mathcal{H}$.

Theorem 3.3.3 *The function $j(\tau)$ has the following properties:*

1. $j(i) = 12^3 = 1728$ *and* $j(\omega) = 0$ *where* $\omega = e^{2\pi i/3}$.
2. $j(\tau)$ *assumes real values on the lines* $\mathrm{Re}\tau = 0, \pm 1/2$ *and on the unit circle* $|\tau| = 1$.
3. *For any* $\tau_1, \tau_2 \in \mathcal{H}$ *we have*
$$j(\tau_1) = j(\tau_2) \iff \tau_1 \sim \tau_2.$$
4. *The map* $j : \mathcal{H} \to \mathbb{C}$ *is surjective.*

Proof. We have seen in Theorem 3.1.2 that $G_4(\omega) = 0$ and $G_6(i) = 0$. Via the relation $j = (240G_4)^3/\Delta = 12^3(240G_4)^3/(240G_4)^3 - (504G_6)^2$ the first assertion follows.
Notice that the complex conjugate of $q = e^{2\pi i\tau}$ is given by $\overline{q} = e^{-2\pi i\overline{\tau}}$. Hence, using the q-expansion of j, which has real coefficients, we get that $\overline{j(\tau)} = j(-\overline{\tau}$. Suppose that τ_0 is purely imaginary. Then $-\overline{\tau_0} = \tau_0$. Hence $\overline{j(\tau_0)} = j(\tau_0)$ and we see that $j(\tau_0)$ is real. Suppose that $\mathrm{Re}\tau_0 = 1/2$. Then $-\overline{\tau_0} = \tau_0 - 1$. Hence $\overline{j(\tau_0)} = j(\tau_0 - 1) = j(\tau_0)$ and we see again that $j(\tau_0)$ is real. Finally suppose that $|\tau_0| = 1$. Then $-\overline{\tau_0} = -1/\tau$. Hence $\overline{j(\tau_0)} = j(-1/\tau_0) = j(\tau_0)$ and so again $j(\tau_0)$ is real.
Let F^o be the part of F (the fundamental domain of $SL(2,\mathbb{Z})$) where we have deleted the boundary points with negative real part. Then every $\tau \in \mathcal{H}$ is $SL(2,\mathbb{Z})$-equivalent to a unique point in F^o. Without loss of generality we can assume that $\tau_1, \tau_2 \in F^o$. Choose $c \in \mathbb{C}$. Let N_c be the number of points $\tau_0 \in F^o$ such that $j(\tau_0) = c$. Suppose first that $cnot \in \mathbb{R}$. In particular, $j(\tau) - c$ has no zeros on the boundary of F. We will show that $N_c = 1$. Notice that
$$N_c = \frac{1}{2\pi i}\int_\Gamma \frac{j'(\tau)}{j(\tau) - c}\, d\tau,$$
where Γ is the closed contour given by the following picture,

We assume that T is chosen sufficiently large so that $|j(\tau)| > |c|$ for all τ with $\mathrm{Im}\tau > T$. Notice that the differential form $j'd\tau/j - c$ is invariant under $SL(2,\mathbb{Z})$. The vertical parts of Γ are related by the relation $\tau \mapsto \tau + 1$. They are traveresed in opposite directions by Γ, hence the two contributions cancel. The part of Γ on the unit circle consists of two parts that are related by $\tau \mapsto -1/\tau$. The integrals over these two parts also cancel. Hence our integral consists simply of an integration over the segment $[-1/2 + iT, 1/2 + iT]$ from right to left. The q-expansion of $j'/(j - c)$ is easily seen to be $-2\pi i+$ positive powers of $q = e^{2\pi i\tau}$. Integration of q^n over our segment yields 0 if $n > 0$ and -1 if $n = 0$. Hence integration of $j'(j - c)$ over the segment yields $2\pi i$. As a result we obtain that $N_c = 1$.
Now suppose $c \in \mathbb{R}$ and suppose that there are two non-equivalent points τ_1, τ_2 such that $j(\tau_1) = j(\tau_2) = c$. Let U_1, U_2 be two disjoint open neighbourhoods of τ_1, τ_2 which do not contain $SL(2,\mathbb{Z})$-equivalent points. Then $j(U_1)$ and $j(U_2)$ are two open neighbourhoods of c, which have a non-real point c' in common. This contradicts our earlier assertion than $N_{c'} = 1$ for non-real c'.

□

We now quote some remarkable properties of the j-invariant. Let us write
$$j(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n)q^n.$$
Then the coefficients $c(n)$ satisfy
$$c(5n) \equiv 0 \pmod 5 \quad c(7n) \equiv 0 \pmod 7 \quad c(11n) \equiv 0 \pmod{11}$$

for all positive integers n.
The largest sporadic simple group has order

$$2^{46}\cdot 3^{20}\cdot 5^9\cdot 7^6\cdot 11^2\cdot 13^3\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71,$$

the Fischer-Griess monster. The dimensions of its lowest dimensional irreducible representations are $1, 196883, 2126876, \ldots$. Notice that

$$c(1) = 1 + 196883, \quad c(2) = 1 + 196883 + 2126876$$

It turns out that the numbers $c(n)$ are simple linear combinations of the dimensions of irreducible representations of the Monster group. This phenomenon, known as 'monstrous moonshine', was conjectured by Conway and Norton in the late 1970's. It was proved by Richard Borcherds, who received the Fields medal for this work.
A third remarkable property of the j-invariant is that j assumes algebraic values at imaginary quadratic arguments. A very special case is when d is a positive integer which is 3 modulo 4 and such that $\mathbb{Q}(\sqrt{-d})$ has class number 1. Then $j\left(\frac{1+\sqrt{-d}}{2}\right) \in \mathbb{Z}$. The most spectacular case is

$$j\left(\frac{1+\sqrt{-163}}{2}\right) = -262537412640768000 = -640320^3.$$

4 Hecke operators

4.1 Determinant n matrices

Consider for every $n \in \mathbb{Z}_{n>0}$ the set

$$\mathcal{M}_n = \{\begin{pmatrix} A & B \\ C & D \end{pmatrix} \mid A, B, C, D \in \mathbb{Z},\ AD - BC = n\}.$$

Two matrices $M_1, M_2 \in \mathcal{M}_n$ are called equivalent if there exists $\alpha \in \mathrm{SL}(2,\mathbb{Z})$ such that $M_1 = \alpha M_2$. We first show that there is finite set of classes and display a full set of representatives.

Lemma 4.1.1 *Every equivalence class contains and element with $C = 0$ and $D > 0$.*

Proof. To any element $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathcal{M}_n$ we choose integers c, d such that $\gcd(c, d) = 1$ and $cA + dC = 0$ and $cB + dD > 0$. Choose $a, b \in \mathbb{Z}$ such that $ad - bc = 1$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A' & B' \\ 0 & D' \end{pmatrix}$$

where $D' = cB + dD > 0$, as desired.

□

Lemma 4.1.2 *Two matrices $M_i = \begin{pmatrix} A_i & B_i \\ C_i & D_i \end{pmatrix} \in \mathcal{M}_n$ $(i = 1, 2)$ with $D_i > 0$ are equivalent if and only if $A_1 = A_2, D_1 = D_2$ and $B_1 \equiv B_2 \pmod{D_1}$.*

Proof. Suppose that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} M_1 = M_2$. Then clearly, $c = 0$. Hence $a = d = \pm 1$. Since $dD_1 = D_2$ and $D_1, D_2 > 0$ we conclude that $a = d = 1$. Finally, $B_2 = B_1 + bD_1$, from which $B_2 \equiv B_1 \pmod{D_1}$ follows.
Suppose conversely that the conditions are met. So $A_2 = A_1, D_2 = D_1$ and there exists $b \in \mathbb{Z}$ such that $B_2 = B_1 + bD_1$. Then,

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} A_1 & B_1 \\ 0 & D_1 \end{pmatrix} = \begin{pmatrix} A_1 & B_1 + bD_1 \\ 0 & D_1 \end{pmatrix} = \begin{pmatrix} A_2 & B_2 \\ 0 & D_2 \end{pmatrix}.$$

Hence M_1 and M_2 are equivalent.

□

The following is now an immediate consequence.

Theorem 4.1.3 *A full system of representatives of equivalence classes in $\mathcal{M}_n$ is given by*

$$M_h = \begin{pmatrix} A_h & B_h \\ 0 & C_h \end{pmatrix}, \quad A_h D_h = n,\ D_h > 0,\ B_h = 0, 1, \ldots, D_h - 1.$$

Here is an important observation. Suppose that $M_1 \sim M_2$ then, for any $\beta \in SL(2,\mathbb{Z})$ we have $M_1\beta \sim M_2\beta$. In other words, the right action of $SL(2,\mathbb{Z})$ permutes the equivalence classes in $\mathcal{M}_n$.

4.2 Definition

Theorem 4.2.1 *Let* $M_h = \begin{pmatrix} A_h & B_h \\ 0 & D_h \end{pmatrix}$, $h = 1, 2, \ldots, r$ *be a full system of representatives of the classes in* $\mathcal{M}_n$. *Let* f *be a modular form of weight* k *with respect to* $\mathrm{SL}(2, \mathbb{Z})$. *Then*

$$T_n(f) := n^{k-1} \sum_{h=1}^{r} (C_h\tau + D_h)^{-k} f\left(\frac{A_h\tau + B_h}{C_h\tau + D_h}\right)$$

is a modular form of weight k.

Proof. We introduce the formal power $d\tau^{k/2}$ of the differential form $d\tau$ and use the property that

$$d\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{ad - bc}{(c\tau + d)^2} d\tau$$

for any $a, b, c, d \in \mathbb{R}$. This implies in particular that $f(\beta\tau)d(\beta\tau)^{k/2} = f(\tau)d\tau^{k/2}$ for any $\beta \in \mathrm{SL}(2, \mathbb{Z})$. Suppose $\alpha \in \mathrm{SL}(2, \mathbb{Z})$ This α permutes the equivalence classes as follows

$$M_h\alpha = \beta_h M_{\sigma(h)} \; h = 1, 2, \ldots, r$$

for some $\sigma \in S_r$ and $\beta_h \in \mathrm{SL}(2, \mathbb{Z})$ $(h = 1, \ldots, r)$.
Observe that the defining relation for $T_n(f)$ can be rewritten as

$$T_n(f)(\tau)d\tau^{k/2} = n^{k/2-1} \sum_{h=1}^{r} f(M_h\tau)(dM_h\tau)^{k/2}.$$

Replace τ by $\alpha\tau$ with $\alpha \in \mathrm{SL}(2, \mathbb{Z})$. We obtain

$$\begin{aligned} T_n(f)(\alpha\tau)(d\alpha\tau)^{k/2} &= n^{k/2-1} \sum_{h=1}^{r} f(M_h\tau)(dM_h\alpha\tau)^{k/2} \\ &= n^{k/2-1} \sum_{h=1}^{r} f(\beta_h M_{\sigma(h)}\tau)(d\beta_h M_{\sigma(h)}\tau)^{k/2} \\ &= n^{k/2-1} \sum_{h=1}^{r} f(M_{\sigma(h)}\tau)(dM_{\sigma(h)}\tau)^{k/2} \\ &= n^{k/2-1} \sum_{h=1}^{r} f(M_h\tau)(dM_h\tau)^{k/2} = T_n(f)(d\tau)^{k/2} \end{aligned}$$

The boundedness of $T_n(f)$ when $\mathrm{Im}\tau \to \infty$ becomes apparent from the explicit formula (5). □

Using the explicit system of representatives we find that

$$T_n(f) = n^{k-1} \sum_{AD=n,\ B>0,\ B \pmod{D}} D^{-k} f\left(\frac{A\tau + B}{D}\right) \tag{5}$$

In particular, when $n = p$ is prime,

$$T_p(f) = p^{k-1} f(p\tau) + p^{-1} \sum_{b=0}^{p-1} f\left(\frac{\tau + b}{p}\right).$$

Theorem 4.2.2 *Let $f(\tau)$ be a modular form of weight k with q-expansion $\sum_{l=0}^{\infty} a(l)q^l$, $q = e^{2\pi i\tau}$. Then*

$$T_n f(\tau) = \sum_{l=0}^{\infty} \left(\sum_{d|\gcd(n,l)} d^{k-1} a(nl/d^2) \right) q^l.$$

In the particular case when $\gcd(l,n) = 1$ the l-th Fourier coefficient of $T_n f$ equals $a(ln)$. Furthermore, when f is a cusp form, then so is $T_n f$. Consider T_n as a linear map from M_k to itself. Then,

i) For any m, n,

$$T_m T_n = \sum_{d|\gcd(n,m)} d^{k-1} T_{nm/d^2}.$$

ii) For all m, n we have $T_m T_n = T_n T_m$ and when $\gcd(m,n) = 1$, $T_m T_n = T_{mn}$.

iii) For any prime p and any $r > 0$,

$$T_p T_{p^r} = T_{p^{r+1}} + p^{k-1} T_{p^{r-1}}.$$

Proof. Notice

$$\begin{aligned} (T_n f)(\tau) &= n^{k-1} \sum_{AD=n} \sum_{B=0}^{D-1} D^{-k} f\left(\frac{A\tau + B}{D}\right) \\ &= n^{k-1} \sum_{AD=n} \sum_{B=0}^{D-1} D^{-k} \sum_{l=0}^{\infty} a(l) q^{Al/D} e^{2\pi i l B/D}. \end{aligned}$$

Notice that

$$\sum_{B=0}^{D-1} e^{2\pi i l B/D} = \begin{cases} D & \text{when D—l} \\ 0 & \text{when D does not divide l} \end{cases}.$$

We assume that $D|l$ and replace l by lD to obtain

$$T_n(f)(\tau) = n^{k-1} \sum_{AD=n} D^{1-k} \sum_{l=0}^{\infty} a(lD) q^{Al}.$$

Put $A = d, D = n/d$ and sum over all $d|n$,

$$T_n f(\tau) = \sum_{d|n} \sum_{l=0}^{|infty} d^{k-1} a(ln/d) q^{dl}.$$

From this equality we can read off the Fourier coefficients of $T_n f$.
Notice that ii) is a direct consequence of i) and that iii) is a special case of i) when $m = p, n = p^r$.

□

4.3 First application

Suppose $f(\tau) = a_0 + a_1 q + a_2 q^2 + \cdots \in M_k$. Then,

$$T_n f(\tau) = \sigma_{k-1} a_0 + a_n q + \cdots.$$

We see once again that $T_n : S_k \to S_k$, so cuspforms are mapped to cuspforms. In particular, $T_n : S_{12} \to S_{12}$ for every n. So $\Delta(\tau)$ is a common eigenform for all T_n. We know that $T_n \Delta = \tau(n) q + \cdots$ hence the eigenvalue of T_n equals $\tau(n)$ and we obtain that $T_n \Delta = \tau(n)\Delta$. Using Theorem 4.2.2 we get the following result.

Theorem 4.3.1 (Mordell, 1917) *Let $\tau(n)$ be the n-th coefficient of the q-expansion of Δ. Then, for every $m, l \in \mathbb{N}$,*

$$\tau(n)\tau(l) = \sum_{d|\gcd(l,n)} d^{11}\tau(nl/d^2).$$

In particular, when $\gcd(n, l) = 1$ we get $\tau(n)\tau(l) = \tau(ln)$, hence τ is a multiplicative function. When p is prime and $r \in \mathbb{N}$ we get

$$\tau(p)\tau(p^r) = \tau(p^{r+1}) + p^{11}\tau(p^{r-1}).$$

5 L-series

5.1 Multiplicative functions

Let $a_n \in \mathbb{C}$ $n = 1, 2, 3, \ldots$ be a sequence of complex numbers. Very often we shall interpret these numbers as the values of the function $\mathbb{N} \to \mathbb{C}$ given by $k \mapsto a_k$. A formal series of the form

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where $s \in \mathbb{C}$, is called a Dirichlet series or L-series. We can multiply two L-series formally as follows,

$$\left(\sum_{n=1}^{\infty} \frac{a_n}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{b_n}{n^s}\right) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$$

where

$$c_n = \sum_{d|n} a_d b_{n/d}.$$

The function c_n is called the *convolution product* of the arithmetic functions a_n and b_m.
A function $f : \mathbb{N} \to \mathbb{C}$ is called *multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all coprime $m, n \in \mathbb{N}$.

5.2 L-series and Eulerpoducts

We have the following characterisation of multiplicative functions.

Theorem 5.2.1 *The function $a(n)$ of n is multiplicative if and only if its L-series can be written in the form*

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{p \text{ prime}} \left(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots\right).$$

Proof. Suppose $a(n)$ is multplicative. Let $p_1, p_2, \ldots$ be the sequence of prime numbers. By unique factorisation in primes we can write

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{a(n)}{n^s} &= \sum_{r_1, r_2, \ldots \geq 0} \frac{a(p_1^{r_1} p_2^{r_2} \cdots)}{(p_1^{r_1} p_2^{r_2} \cdots)^s} \\ &= \sum_{r_1, r_2, \ldots \geq 0} \frac{a(p_1^{r_1}) a(p_2^{r_2}) \cdots}{(p_1^{r_1} p_2^{r_2} \cdots)^s} \\ &= \prod_{p \text{ prime}} \left(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots\right)\end{aligned}$$

Conversely it follows from the product expansion that

$$a(n) = a(p_1^{r_1} \cdots p_k^{r_k}) = a(p_1^{r_1}) \cdots a(p_k^{r_k}).$$

□

Examples of Euler products
Example 1) $a(n) = 1$ for all $n \in \mathbb{N}$.

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod_p \frac{1}{1 - p^{-s}}.$$

Example 2)

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{\phi(n)}{n^s} &= \prod_p\left(1+\frac{\phi(p)}{p^s}+\frac{\phi(p^2)}{p^{2s}}+\cdots\right)\\ &= \prod_p\left(1+(1-1/p)\sum_{r=1}^{\infty}p^{r-rs}\right)\\ &= \prod_p\left(1+(1-1/p)\frac{p^{1-s}}{1-p^{1-s}}\right)\\ &= \left(\frac{1-p^{-s}}{1-p^{1-s}}\right)=\frac{\zeta(s-1)}{\zeta(s)}\end{aligned}$$

Example 3)

$$\sum_{n=1}^{\infty}\frac{\tau(n)}{n^s}=\prod_p\left(1+\frac{\tau(p)}{p^s}+\frac{\tau(p^2)}{p^{2s}}+\cdots\right).$$

The relation $\tau(p)\tau(p^r)=\tau(p^{r+1})+p^{11}\tau(p^{r-1})$ implies that

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

Hence

$$\sum_{n=1}^{\infty}=\prod_p\frac{1}{1-\tau(p)p^{-s}+p^{11-2s}}.$$

Theorem 5.2.2 *Let $f=\sum_{n=0}^{\infty}c_nq^n\not\equiv 0$ with $q=e^{2\pi i\tau}$ be a modular form of weight k which is an eigenform with respect to the Hecke operator T_n for every $n\in\mathbb{N}$. Let λ_n be the eigenvalue of T_n. Then $c_1\neq 0,\ c_n=\lambda_nc_1$ for all n and*

$$\sum_{n=1}^{\infty}\frac{\lambda_n}{n^s}=\prod_p\frac{1}{\lambda_pp^{-s}+p^{k-1-2s}}.$$

Proof. By comparison of the coefficient of q in $T_nf=\lambda_nf$ we find that $c_n=\lambda_nc_1$. Since $c_n\neq 0$ for at least one n, we infer that $c_1\neq 0$. From the relations $T_mT_n=T_nT_m=T_{mn}$ when $\gcd(m,n)=1$ we see that λ_n is a multiplicative function of n. Together with the relation $\lambda(p)\lambda(p^r)=\lambda(p^{r+1})+p^{k-1}\lambda(p^{r-1})$ this yields our last assertion.

□

Consequence: Let $f=q+a_2q^2+a_3q^3+\cdots$ be a cuspform of weight k which is a common eigenform for all T_n. Then

$$\sum_{n=1}^{\infty}=\prod_p\frac{1}{1-a_pp^{-s}+p^{k-1-2s}}.$$

We call f a normalised eigenform of the Hecke operators. In particular, if $\dim(S_k)=1$ there is always a normalised eigenform. Notice that $\dim(S_k)=1\iff k=12,16,18,20,22,26$.

5.3 Convergence

Let $f\in S_k$ with q-series $\sum_{n=1}^{\infty}c_nq^n$ and let

$$L(f,s)=\sum_{n=1}^{\infty}\frac{c_n}{n^s}$$

be its associated L-series. We shall be interested in the region of convergence for this L-series.

Theorem 5.3.1 *Let f be as above and c_n the coefficients of its q-series expansion. Then there exists $\gamma > 0$ such that*

$$|c_n| < \gamma n^{k/2}$$

for all $n \in \mathbb{N}$.

Proof. Notice that $|f(\tau)|y^{k/2}$ is invariant under $\mathrm{SL}(2,\mathbb{Z})$, where $y = \mathrm{Im}\tau$. Hence, letting F be the fundamental domain of $\mathrm{SL}(2,\mathbb{Z})$,

$$\begin{aligned}
\max_{\tau\in\mathcal{H}} |f(\tau)|y^{k/2} &= \max_{\tau\in F} |f(\tau)|y^{k/2} \\
&\le \max_{y\ge\sqrt{3}/2} y^{k/2}\sum_{n=1}^{\infty}|c_n|e^{-2\pi n y} \\
&\le (\max_{y\ge\sqrt{3}/2} y^{k/2}e^{-2\pi y})\sum_{n=1}^{\infty}|c_n|e^{-(n-1)\pi\sqrt{3}} \\
&\le A
\end{aligned}$$

for some $A > 0$. From

$$c_n = \frac{1}{2\pi i}\int_{|q|=e^{-2\pi y}} \frac{f}{q^{n+1}}\,dq$$

follows the estimate

$$|c_n| \le e^{2n\pi y}\max_{\tau\in\mathcal{H}} Ae^{2\pi n y}y^{-k/2}.$$

Choose $y = 1/n$ and we obtain $|c_n| \le Ae^{2\pi}n^{k/2}$.

□

As a consequence we see that the L-series $L(f,s)$ converges for all $\mathrm{Re}s > k/2+1$. The *Ramanujan-Peterson conjecture* asserts that if f is a normalised (i.e. $c_1 = 1$) eigenform for the Hecke-operators, then $|c_p| < 2p^{(k-1)/2}$ for all primes p. In particular, $|\tau(p)| < 2p^{11/2}$, as conjectured by Ramanujan. The Ramanujan-Peterson conjecture is a special case of the so-called Weil conjectures for algebraic varieties over finite fields. This conjecture was only proved in 1973 by P.Deligne.

Theorem 5.3.2 *Let f and $L(f,s)$ be as above. Then $L(f,s)$ converges for all $s \in \mathbb{C}$ with $\mathrm{Re}s > k/2+1$. Furthermore $L(f,s)$ can be continued analytically to the $\mathbb{C}$ and we have the functional equation*

$$Z(k-s) = (-1)^{k/2}Z(s)$$

where $Z(s) = \Gamma(s)(2\pi)^{-s}L(f,s)$.

Recall that the Γ-function is defined by

$$\Gamma(s) = \int_0^{\infty} y^{s-1}e^{-y}\,dy$$

when $\mathrm{Re}s > 0$. It can be continued meromorphically to all of $\mathbb{C}$.

Proof. The convergence when $\mathrm{Re}s > k/2+1$ follows from the previous Theorem. From the definition of the Γ-function it follows that

$$\Gamma(s)(2\pi n)^{-s} = \int_0^{\infty} e^{-2\pi n y}y^{s-1}dy$$

for all $\mathrm{Re}s > 0$. Now assume that $\mathrm{Re}s > k/2+1$, multiply on both sides by c_n and sum over all n. We obtain

$$(2\pi)^{-s}\Gamma(s)L(f,s) = \int_0^{\infty} f(iy)y^{s-1}dy.$$

Since f is modular, we have $f(i/y) = (iy)^k f(iy)$. Hence

$$(2\pi)^{-s}\Gamma(s)L(f,s) = \int_1^\infty f(iy)y^{s-1}dy + \int_0^1 (iy)^{-k} f(i/y)y^{s-1}\, dy$$
$$\int_1^\infty f(iy)y^{s-1}dy + i^{-k}\int_1^\infty f(iw)w^{k-s-1}\, dw$$

Since $f(iy) = O(e^{-2\pi y})$ for all y we see that the integrals on the right hand side converge absolutely for any choice of $s \in \mathbb{C}$. Hence the right hand side exists and is analytic for all $s \in \mathbb{C}$. If we denote right hand side by $Z(s)$ we easily see that $Z(k-s) = (-1)^{k/2}Z(s)$ which proves our functional equation.

□

6 Peterson inner product

6.1 Fundamental domains

We first make the concept of a fundamental domain a bit more precise.

Definition 6.1.1 *Let* Γ *be a subgroup of* $\mathrm{SL}(2,\mathbb{Z})$. *A fundamental domain* D *for the group* Γ *is a measurable subset of* $\mathcal{H}$ *such that*

1. *To every* $z \in \mathcal{H}$ *there exists* $g \in \Gamma$ *such that* $g(z) \in D$.
2. *For any two* $z_1, z_2 \in D$ *we have* $z_2 = g(z_1), g \in \Gamma \Rightarrow z_1 = z_2$.

For example, a fundamental domain for $\mathrm{SL}(2,\mathbb{Z})$ itself is given by the points with $-1/2 < \mathrm{Re} z < 1/2$ and $|z| > 1$ together with the half line $\mathrm{Re} z = -1/2, |z| > 1$ and the arc $|z| = 1, \pi/2 \geq \arg(z) \leq 2\pi/3$.
Notice that if D is a fundamental domain for $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$ then so is gD for any $g \in \Gamma$.

Lemma 6.1.2 *Let* Γ *be a subgroup of* $\mathrm{SL}(2,\mathbb{Z})/\pm 1$ *of finite index* r. *Let* $\mathrm{SL}(2,\mathbb{Z})/\pm 1 = \cup_{i=1}^r \Gamma\alpha_i$ *be a decomposition of* $\mathrm{SL}(2,\mathbb{Z})/\pm 1$ *into disjoint left-cosets. Let* F *be a fundamental domain of* $\mathrm{SL}(2,\mathbb{Z})$. *Then* $\cup_{i=1}^r \alpha_i(F)$ *is a fundamental domain for* Γ.

Proof. Exercise

6.2 Determinant p matrices

Let p be a prime. Let $\mathcal{M}_p$ be the set of 2×2-matrices with integer entries and determinant p.

Lemma 6.2.1 *Denote* $\Gamma(1) = \mathrm{SL}(2,\mathbb{Z})$. *Then*

$$\mathcal{M}_p = \Gamma(1) \cdot \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \cdot \Gamma(1),$$

in other words, $\mathcal{M}_p$ *is a single double coset of a determinant* p *matrix.*

Let D be a fundamental domain of $\mathrm{SL}(2,\mathbb{Z})$. On the space S_k we define the Peterson inner product as

$$\langle f, g \rangle = \int_D f(\tau)\overline{g(\tau)} y^k \frac{dxdy}{y^2}$$

where $\tau = x + iy$. We know that we have for every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\mathbb{R})^+$ (positive determinant)

$$\begin{aligned} \mathrm{Im}\frac{a\tau+b}{c\tau+d} &= (ad-bc)\frac{\mathrm{Im}\tau}{|c\tau+d|^2} \\ d\frac{a\tau+b}{c\tau+d} &= (ad-bc)\frac{d\tau}{(c\tau+d)^2} \end{aligned}$$

Hence

$$\frac{dxdy}{y^2} = \frac{i}{2}\frac{d\tau \wedge \overline{\tau}}{\mathrm{Im}\tau^2}$$

is invariant under $\mathrm{GL}(2,\mathbb{R})^+$. Furthermore, for every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ we have

$$f\left(\frac{a\tau+b}{c\tau+d}\right)\overline{g\left(\frac{a\tau+b}{c\tau+d}\right)}\left(\mathrm{Im}\frac{a\tau+b}{c\tau+d}\right)^k = f(\tau)\overline{g(\tau)}(\mathrm{Im}\tau)^k.$$

Hence $f(\tau)\overline{g(\tau)}y^k$ is invariant under $\mathrm{SL}(2,\mathbb{Z})$ and $\langle f, g \rangle$ is independent of the choice of fundamental domain of $\mathrm{SL}(2,\mathbb{Z})$.

6.3 Hermitean forms and operators

Lemma 6.3.1 *The product form $\langle f, g\rangle$ is a hermitean product on the complex vector space S_k.*

Proof We must check the following properties

1. $\langle \alpha f_1 + \beta f_2, g\rangle = \alpha \langle f_1, g\rangle + \beta \langle f_2, g\rangle$ for every $\alpha, \beta \in \mathbb{C}$ and $f, g \in S_k$.
2. $\langle f, g\rangle = \overline{\langle g, f\rangle}$ for every $f, g \in S_k$.
3. $\langle f, f\rangle > 0$ for every non-trivial $f \in S_k$.

Remarks
Suppose $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$ is a subgroup of finite index in $\mathrm{SL}(2,\mathbb{Z})$. Let $\mathrm{SL}(2,\mathbb{Z}) = \cup_{i=1}^r \alpha_i \Gamma$ be a disjoint union of right cosets. When D is a fundamental domain of $\mathrm{SL}(2,\mathbb{Z})$ then $\cup_{i=1}^r \alpha_i^{-1} D$. Notice,

$$\int_D f(\tau)\overline{g(\tau)} y^k \frac{dxdy}{y^2} = \frac{1}{r}\int_{D(\Gamma)} f(\tau)\overline{g(\tau)} y^k \frac{dxdy}{y^2}$$

where $D(\Gamma)$ is a fundamental domain of Γ.

Let $D(N)$ be a fundamental domain of $\Gamma(N)$. Suppose $S = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathcal{M}_N$. Then $S^{-1}\Gamma(N)S \subset \mathrm{SL}(2,\mathbb{Z})$ and $S^{-1}D(N)$ is a fundamental domain of $S^{-1}D(N)S$. Furthermore $\Gamma(N)$ and $S^1 D(N)S$ have the same index in $\mathrm{SL}(2,\mathbb{Z})$.

Proof that T_p is Hermitean.
Suppose $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathcal{M}_p$. Suppose $f, g \in S_k$. Then $(C\tau + D)^{-k} f(S\tau)$ is a modular form with respect to $\Gamma(p)$ and $S^{-1}\Gamma(p)S$. Let $S^* = \begin{pmatrix} D & -B \\ -C & A \end{pmatrix}$ and notice that $S^* \in \mathcal{M}_p$ and $SS^* = p\mathrm{Id}$. Then

$$\begin{aligned} I_S : &= \int_{D(p)} (C\tau + D)^k f(S\tau)\overline{g(\tau)} y^k \frac{dxdy}{y^2} \\ &= \int_{S^{-1}D(p)} (C\tau + D)^{-k} f(S\tau)\overline{g(\tau)} y^k dxdy\overline{y}^2 \end{aligned}$$

Replace τ by $S^*\tau$ and use $\mathrm{Im}(S^*\tau) = p\mathrm{Im}(\tau)|-C\tau + A|^2$ to get

$$\begin{aligned} I_S &= \int_{D(p)} (-C\overline{\tau} + A)^{-k} f(\tau)\overline{g(S^*\tau)} y^k \frac{dxdy}{y^2} \\ &= \int_{D(p)} f(\tau)\overline{(-C\tau + A)^{-k} g(S^*\tau)} y^k \frac{dxdy}{y^2} \end{aligned}$$

So,if we take $M_0, M_1, \ldots, M_p$ as above and write $M_i = \begin{pmatrix} A_i & B_i \\ C_i & D_i \end{pmatrix}$,then

$$\begin{aligned} \langle T_p f, g\rangle &= [\Gamma(1) : \Gamma(p)] p^{k-1} \sum_{i=0}^{p} \int_{D(p)} (C_i\tau + D_i)^{-k} f(M_i\tau)\overline{g(\tau)} y^k \frac{dxdy}{y^2} \\ &= [\Gamma(1) : \Gamma(p)] p^{k-1} \sum_{i=0}^{p} \int_{D(p)} f(\tau)\overline{(-C_i\tau + A_i)^{-k} g(M_i^*\tau)} y^k \frac{dxdy}{y^2} \\ &= \langle f, T_p g\rangle \end{aligned}$$

□

Proposition 6.3.2 *Let V be a finite-dimensional vectorspace over $\mathbb{C}$ with hermitean product. Let $A_1, A_2, \ldots$ be a sequence of Hermitean operators which all commute. Then there exists an orthonormal basis of V consisting of common eigenvetors for all A_i.*

Proof. We use induction with respect to $\dim(V)$. When $\dim(V) = 1$ we are done trivially. Suppose that $\dim(V) = k > 1$ and that our theorem has been proved for all dimensions $\le k$. When all A_i are scalar multiplication we are done. Suppose that at least one A_i, say A_1, is non-scalar. Then V is a direct sum of pairwise orthogonal subspaces E_i of A_1, with distinct eigenvalues λ_i. Furthermore $\dim(E_i) < \dim(V)$ for all i.
Let $\mathbf{v} \in E_i$ for some i. Then $A_1\mathbf{v} = \lambda_i\mathbf{v}$. For any A_j we have $A_jA_1\mathbf{v} = \lambda_iA_j\mathbf{v}$. Now use $A_jA_1 = A_1A_j$. We find $A_1(A_j\mathbf{v}) = \lambda_iA_j\mathbf{v}$. Hence $A_j\mathbf{v} \in E_i$. We thus see that for any i and j, $A_j(E_i) \subset E_i$. So we can apply our induction hypothesis on each eigenspace E_i and conclude the induction.

□

6.4 Main theorem on Hecke eigenforms on SL(2, ℤ)

Theorem 6.4.1 *Let S_k be the space of cupsforms of weight k with respect to* $\mathrm{SL}(2,\mathbb{Z})$. *Then there is a basis of $f_1, \ldots, f_r$ of common eigenvectors under the Hecke-operators such that*

$$f_i(\tau) = \sum_{n=1}^{\infty} c_{in}q^n, \qquad c_{i1} = 1.$$

Moreover,

$$\sum_{n=1}^{\infty} \frac{c_{in}}{n^s} = \prod_p \frac{1}{1 - c_{ip}p^{-s} + p^{k-1-2s}}$$

and $f_1, \ldots, f_r$ are uniquely determined and orthogonal with repect to the Peterson product.

Proof We know that the T_n are Hermitean under the Peterson product and $T_mT_n = T_nT_m$ for all m, n. So there is basis of S_k consisting of eigenforms for all T_n. Call these $f_1, \ldots, f_r$ where we normalise f_i such that $c_{i1} = 1$. This is possible because a priori $c_{i1} \neq 0$ for a Hecke eigenform. The product expansion of the L-series follows from the multaplicative properties of the Hecke-operators.
Let f, g be two normalised Hecke-eigenforms and suppose $f \neq g$. That means that there exist Fourier coefficients f_n, g_n of f, g such that $f_n \neq g_n$. Now oberve

$$f_n \langle f, g\rangle = \langle T_nf, g\rangle = \langle f, T_ng\rangle = g_n \langle f, g\rangle$$

Since $f_n \neq g_n$ we conclude that $\langle f, g\rangle = 0$. So for any normalised eigenform $f \neq f_1, \ldots, f_r$ we have that $\langle f, f_i\rangle = 0$ for $i = 1, \ldots, r$. Moreover, $f_1, \ldots, f_r$ form an orthogonal basis of S_k, hence they are uniquely determined.

□