Modular Forms

David Loeffler

University of Warwick
Autumn term 2011/12

Notes by Fabian Völz

Contents

0 Prologue: The history of a function **4**

1 Modular forms of level 1 **5**

1.1 The upper half-plane 5
1.2 The modular group 6
1.3 Modular forms and modular functions 8
1.4 Eistenstein series 10
1.5 The valence formula 13
1.6 Hecke operators 20
1.7 The L-function of a modular form 29

2 Modular forms of higher level **34**

2.1 Congruence subgroups 34
2.2 Behaviour at ∞ 35
2.3 Cusps 38
2.4 The valence formula in arbitrary levels 41
2.5 Eisenstein series revisited 47
2.6 The Petersson product 52
2.7 Hecke operators 55
2.8 The Hecke algebras of $\Gamma_0(N)$ and $\Gamma_1(N)$ 59
2.8.1 Interlude: Dirichlet characters 61
2.9 Hecke operators and the Petersson product 65
2.10 Old and new modular forms 69

3 Miscellany **75**

3.1 Riemann surfaces 75
3.2 Modular forms and elliptic curves 76
3.3 Theta functions and quadratic forms 77
3.4 Galois representations 77

0 Prologue: The history of a function

Let $z \in \mathbb{C}$ with $\mathrm{Im}(z) > 0$. Put $q = e^{2\pi i z}$ and let

$$\Delta(z) = q \cdot \prod_{n \in \mathbb{N}} (1 - q^n)^{24}.$$

This is one of the simplest examples of a modular form. Note that we can "multiply out" the product which leads us to

$$\Delta(z) = \sum_{n \in \mathbb{N}} \tau(n) q^n$$

for some integers $\tau(n)$.

Facts. (1) In 1850 Weierstrass showed that

$$\Delta(z) = z^{-12} \cdot \Delta\left(-\frac{1}{z}\right).$$

(2) Ramanujan proved in 1916 that the integers $\tau(n)$ satisfy the equation

$$\tau(n) = \sum_{d|n} d^{11} \mod 691.$$

(3) Ramanujan also conjectured $\tau(nm) = \tau(n)\tau(m)$ for n, m coprime. This was proved by Mordell in 1917.

(4) In 1972 Swinnerton-Dyer proved $\tau(n)$ satisfies congruences like the one in (2) modulo 2, 3, 5, 7, 23 and 691, but no other primes.

(5) Ramanujan conjectured in 1916 for p prime holds $|\tau(p)| < 2\, p^{11/2}$. This was proved in 1974 by Deligne.

(6) The quantity

$$\frac{\tau(p)}{2p^{11/2}} \in [-1, 1]$$

is distributed in the interval $[-1, 1]$ with density function proportional to $\sqrt{1 - x^2}$. This was conjectured by Sato and Tate (1960s) and proved by Barnet-Lamb, Geraghty, Harris and Taylor in 2009 using Bau Chau Ngo's *Fundamental Lemma* which got Ngo the 2010 Fields Medal.

1 Modular forms of level 1

This chapter is based mainly on chapter 7 of the book "A course in Arithmetic" by Serre and gives an introduction to the theory of modular forms on the modular group $\mathrm{SL}_2(\mathbb{Z})$.

1.1 The upper half-plane

Definition 1.1.1. We call the set of complex numbers with positive imaginary part the **upper half-plane** and denote it by $\mathcal{H}$, so $\mathcal{H} = \{z \in \mathbb{C} \colon \operatorname{Im}(z) > 0\}$.

Recall that the **special linear group** $\mathrm{SL}_2(\mathbb{R})$ is the set of invertible 2×2 matrices with entries in $\mathbb{R}$ and determinant 1.

Proposition 1.1.2. $\mathrm{SL}_2(\mathbb{R})$ *acts on* $\mathcal{H}$ *via*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.z = \frac{az+b}{cz+d}.$$

Proof. Let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $z = x + iy \in \mathcal{H}$ with $x, y \in \mathbb{R}$. Then either c or d is nonzero and $y > 0$, so $cz + d \neq 0$. Further

$$\begin{aligned} \operatorname{Im}\left(\frac{az+b}{cz+d}\right) &= \frac{\operatorname{Im}\left((az+b)(c\overline{z}+d)\right)}{|cz+d|^2} \\ &= \frac{\operatorname{Im}\left((ax+b)(cx+d) + acy^2 + i(ad-bc)y\right)}{|cz+d|^2} = \frac{\operatorname{Im}(z)}{|cz+d|^2} > 0. \end{aligned}$$

Therefore $g.z \in \mathcal{H}$ for any $z \in \mathcal{H}$, $g \in \mathrm{SL}_2(\mathbb{R})$. Moreover, we have $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)z = z$ and it is easy to check that indeed $g.(h.z) = (gh).z$ for any $z \in \mathcal{H}$, $g, h \in \mathrm{SL}_2(\mathbb{R})$. Thus $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathcal{H}$. □

Notice that $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ acts trivially on $\mathcal{H}$, so the action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathcal{H}$ factors through the quotient $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/(\pm 1)$, the **projective special linear group**.

Proposition 1.1.3. *For any* $k \in \mathbb{Z}$*, there is a right action of* $\mathrm{SL}_2(\mathbb{R})$ *on the set of functions* $\mathcal{H} \to \mathbb{C}$ *given by*

$$\left(f|_k g\right)(z) = j(g,z)^{-k}\, f(g.z)$$

where $f \colon \mathcal{H} \to \mathbb{C}$, $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{R})$ *and* $j(g,z) = cz + d$*. We call this the* ***weight*** k ***action****.*

Proof. Firstly we need to show that $f|_k g$ is a well-defined function $\mathcal{H} \to \mathbb{C}$. But this is obvious since $cz + d \neq 0$ and $g.z \in \mathcal{H}$ for all $z \in \mathcal{H}$, $g \in \mathrm{SL}_2(\mathbb{R})$. Clearly also $f|_k 1 = f$ holds as $j(1, z) = 1$. Therefore it remains to show that $(f|_k g)|_k h = f|_k(gh)$ for arbitrary $g, h \in \mathrm{SL}_2(\mathbb{R})$. The left hand side of the equation can be rewritten as

$$\begin{aligned}(f|_k g)|_k h &= j(h, z)^{-k} \left((f|_k g)(h.z)\right) \\ &= j(h, z)^{-k} j(g, hz)^{-k} f(g.(h.z))\end{aligned}$$

and the right hand side results in

$$f|_k(gh) = j(gh, z)^{-k} f((gh).z).$$

We already know $(gh).z = g.(h.z)$. So it remains to show $j(gh, z) = j(h, z)j(g, h.z)$. This is the so called "cocycle relation" and can be easily checked. □

1.2 The modular group

Definition 1.2.1. We call $\mathrm{SL}_2(\mathbb{Z}) = \{g \in \mathbb{Z}^{2\times 2} \colon \det(g) = 1\}$ the **modular group** and $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/(\pm 1)$ the **projective modular group**.

Theorem 1.2.2. *(a) The group* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by* $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ *and* $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

(b) Every orbit of $\mathrm{SL}_2(\mathbb{Z})$ *acting on* $\mathcal{H}$ *contains a point of the set* D *defined by*

$$D = \left\{ z \in \mathcal{H} \colon -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2} \text{ and } |z| \geq 1 \right\}.$$

(c) If $z \in D$ *and* $g.z \in D$ *for some* $g \in \mathrm{SL}_2(\mathbb{Z})$*, then either* $g = \pm 1$ *and* $g.z = z$ *or* z *lies on the boundary of* D.

(d) The stabiliser of $z \in \mathcal{H}$ *in* $\mathrm{PSL}_2(\mathbb{Z})$ *is trivial unless* z *is in the orbit of* i *or in the orbit of* $\rho = e^{2\pi i/3}$.

Proof. We will prove all of these statements in 4 steps using an argument of Serre. Let $G = \mathrm{PSL}_2(\mathbb{Z})$ and $G' = \langle S, T \rangle \leq G$.

Step 1. Every G' orbit in $\mathcal{H}$ contains a point of D.

Proof of Step 1. Let $z \in \mathcal{H}$. Since $|cz + d| > |c\,\mathrm{Im}(z)|$ and $|cz + d| > |c\,\mathrm{Re}(z) + d|$ there exist only finitely many $(c, d) \in \mathbb{Z}^2$ such that $|cz + d| < 1$. Recall that

$$\mathrm{Im}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}.z\right) = \frac{\mathrm{Im}(z)}{|cz + d|^2}.$$

Hence the G' orbit of z contains a point of maximal imaginary part. Let this point be z. Note that z is not unique as its real part is not fixed. But since $T.z = z + 1$ we can assume $\mathrm{Re}(z) \in [-\frac{1}{2}, \frac{1}{2}]$.

We will now show that this z indeed lies in D. We have $\mathrm{Im}(S.z) = |z|^{-2}\,\mathrm{Im}(z)$. By construction z is a point of maximal imaginary part in the orbit of G', so we must have $|z|^{-2}\,\mathrm{Im}(z) \leq \mathrm{Im}(z)$. This implies $|z| \geq 1$ and thus $z \in D$. Clearly this proves part (b) of the theorem. $\square$

Step 2. If $z \in D$ and $g.z \in D$ for some $g \in G$, then one of the following holds:

(i) $g = 1$

(ii) $g = T$ and $\mathrm{Re}(z) = -\frac{1}{2}$, or $g = T^{-1}$ and $\mathrm{Re}(z) = \frac{1}{2}$

(iii) $g = S$ and $|z| = 1$

(iv) $g = ST = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ or $g = T^{-1}S = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ or $g = ST^{-1}S = \left(\begin{smallmatrix} -1 & 0 \\ -1 & -1 \end{smallmatrix}\right)$ and $z = \rho$

(v) $g = TS = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ or $g = ST^{-1} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ or $g = STS = \left(\begin{smallmatrix} -1 & 0 \\ 1 & -1 \end{smallmatrix}\right)$ and $z = \rho + 1$

Note that $g = -g$ in G as $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/(\pm 1)$.

Proof of Step 2. Let $z \in D$ and $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ such that $w = g.z \in D$. Being free to replace g by g^{-1} and z by w we can assume that $\mathrm{Im}(w) \geq \mathrm{Im}(z)$. Again recalling $\mathrm{Im}(g.z) = |cz + d|^{-2}\ \mathrm{Im}(z)$ we gain $|cz + d| \leq 1$. Since $z \in D$ we therefore see

$$1 \geq |cz + d| \geq |c|\,\mathrm{Im}(z) \geq |c|\,\mathrm{Im}(\rho) = \frac{\sqrt{3}}{2}|c| > \frac{1}{2}|c|.$$

So $|c| < 2$. As $c \in \mathbb{Z}$ we get $c = 0$ or $c = \pm 1$.

- Let $c = 0$. Since $1 \geq |cz + d| = |d|$ we have $d = 0$ or $d = \pm 1$. But $c = d = 0$ is impossible, so $d = \pm 1$ and hence $a = \pm 1$. Therefore $g = \left(\begin{smallmatrix} \pm 1 & b \\ 0 & \pm 1 \end{smallmatrix}\right)$ is the translation by b. But since $\mathrm{Re}(z)$ and $\mathrm{Re}(gz)$ lie between $-\frac{1}{2}$ and $\frac{1}{2}$ this implies $b = 0$ or $b = \pm 1$. So either $g = \pm 1$ (case (i)) or $g = T^{\pm 1}$ and $\mathrm{Re}(z) = \mp\frac{1}{2}$ (case (ii)).

- Let $c = 1$. Assuming $|d| \geq 2$ leads to the following contradiction:

$$1 \geq |cz + d| = |z + d| \geq |\,\mathrm{Re}(z) + d| \geq |d| - |\,\mathrm{Re}(z)| \geq 2 - \frac{1}{2} = \frac{3}{2}$$

  Thus we have $d = 0$ or $d = \pm 1$ as in the first case. Assume that $d = 0$. Then $b = -1$, so $g = \left(\begin{smallmatrix} a & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Moreover, we know $1 \geq |cz + d| = |z|$. On the other hand we have $|z| \geq 1$ as $z \in D$. Therefore $|z| = 1$. It can be checked that this implies $a = 0$ (case (iii)) or $a = \pm 1$ (case (iv) and case (v)). Now let $d = 1$. Then $1 \geq |z + 1|$. This is only possible for $z \in D$ if $z = \rho$ (case (iv)). Similarly $d = -1$ implies $z = \rho + 1$ (case (v)).

- The case $c = -1$ runs analoguesly to the case $c = 1$.

This shows Step 2 (it remains to check the matrices in case (iv) and (v)) and therefore part (c) of the theorem. $\square$

Step 3. Let $z \in D$ such that the stabilizer G_z of z is not trivial, hence $|G_z| > 1$. Then $z = i$, $z = \rho$ or $z = \rho + 1$.

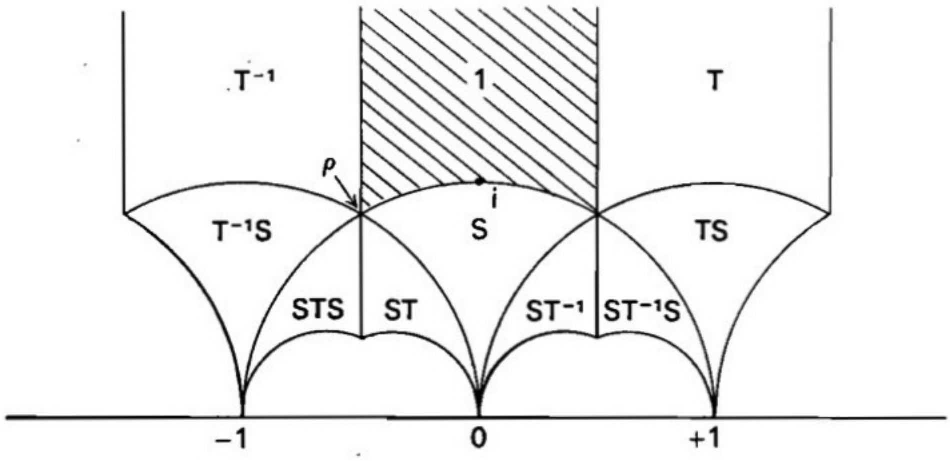
Proof of Step 3. As $g.z = z \in D$ for all $g \in G_z$ it sufficies to check the matrices seen in step 2. Clearly $S.z = z$ if and only if $z = i$ and $T.z \neq z$ for all z. Moreover, we can check $g.\rho = \rho$ if and only if $g = ST$ or $g = T^{-1}S$, and $g.(\rho + 1) = \rho + 1$ if and only if $g = TS$ or $g = ST^{-1}$, but they do not fix any other point in D. Finally, the matrices $ST^{-1}S$ and STS do not fix any point in D. This shows step 3 and proves part (d) of the theorem. □

Step 4. It remains to show that $SL_2(\mathbb{Z})$ is generated by S and T.

Proof of Step 4. Let g be an arbitrary element of G and let z be an arbitrary point of the interior of D. Then $gz \in \mathcal{H}$ and by step 1 exists $g' \in G'$ such that $g'(gz) \in D$. Moreover step 2 implies that either $g'g = 1$ or z is on the boundary of D which is by assumption not the case. Thus $g'g = 1$ and hence $g = (g')^{-1} \in G'$. So S and T generate G, and since $S^2 = -1$, S and T indeed generate $SL_2(\mathbb{Z})$. This proves part (a) of the theorem. □

Therefore the theorem is proved. □

Remark. The set D is called the **fundamental domain**. The figure below represents D itself and the transforms of D by some group elements of $\mathrm{SL}_2(\mathbb{Z})$. Part (c) of the theorem shows that two sets gD and $g'D$ where $g, g' \in \mathrm{SL}_2(\mathbb{Z})$ only interesect along their edges. Furthermore part (a) implies that $\mathcal{H}$ is covered by the sets $\{gD\colon g \in \mathrm{SL}_2(\mathbb{Z})\}$.



1.3 Modular forms and modular functions

Definition 1.3.1. A **weakly modular function of weight** k **and level 1** is a meromorphic function $\mathcal{H} \to \mathbb{C}$ such that $f|_k g = f$ for all $g \in \mathrm{SL}_2(\mathbb{Z})$.

So weakly modular functions are meromorphic functions on the upper-half plane which are invariant under the weight k action of the modular group. Note that for a meromorphic function $f\colon \mathcal{H} \to \mathbb{C}$ being invariant under $\mathrm{SL}_2(\mathbb{Z})$ is equivalent to being invariant under the elements S and T of Theorem 1.2.2 as these generate $\mathrm{SL}_2(\mathbb{Z})$. Moreover, Theorem 1.2.2 shows that a weakly modular function f is completly determined by its values on the fundamental domain D.

Remark. (1) Constant functions are weakly modular of weight 0.

(2) Let f be a weakly modular function of weight k and level 1. Then $f(z+1) = f(z)$ since $f|_k\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = f(\,\cdot\, + 1)$. So f is periodic with period 1 and thus it sufficies to consider f on a strip like $\{z \in \mathcal{H}\colon 0 \leq \mathrm{Re}(z) < 1\}$. This motivates the following definition of a function $\tilde{f}$.

Recall that the complex exponential function exp is holomorphic on $\mathbb{C}$ and that its restriction $\exp\colon \{z \in \mathbb{C}\colon 0 \leq \mathrm{Im}(z) < 2\pi i\} \to \mathbb{C} \setminus \{0\}$ is bijective. Hence its invers, the complex logarithm $\log\colon \mathbb{C} \setminus \{0\} \to \{z \in \mathbb{C}\colon 0 \leq \mathrm{Im}(z) < 2\pi i\}$, is well-defined, though not holomorphic (not even continuous) since it has a $2\pi i$-skip while crossing the postive real axis.

We would like to define a composition of the complex logarithm log and the weakly modular function f to compensate for the $2\pi i$-skip with the periodicity of f. To do so we need to rescale the skip and hence obtain

$$g\colon \mathbb{C} \setminus \{0\} \to \{z \in \mathbb{C}\colon 0 \leq \mathrm{Re}(z) < 1\},\ q \mapsto \frac{\log(q)}{2\pi i}.$$

Furthermore we need to restrict the image of g to $\mathcal{H}$ which can be done easily by restricting the domain of g to $\{q \in \mathbb{C}\colon 0 < |q| < 1\}$. Finally we get a well-defined and meromorphic function

$$\tilde{f}\colon \{q \in \mathbb{C}\colon 0 < |q| < 1\} \to \mathbb{C},\ q \mapsto f\left(\frac{\log(q)}{2\pi i}\right)$$

which contains all the information of f. However, $\tilde{f}$ could still have a nasty singularity at 0.

(3) There are no nonzero weakly modular functions of odd weight. To see this let k be odd and let f be a weakly modular function of weight k. Then

$$f(z) = (-1)^k f((-1).z) = -f(z)$$

for all $z \in \mathcal{H}$ since $-1 \in \mathrm{SL}_2(\mathbb{Z})$ and thus $f = 0$.

Definition 1.3.2. Let f be a weakly modular function of weight k and level 1. We say that f is **meromorphic at** ∞ if $\tilde{f}$ is meromorphic at 0. Similarly we define f to be **holomorphic at** ∞ if $\tilde{f}$ is holomorphic at 0. In this case we define $f(\infty) := \tilde{f}(0)$.

Informally spoken the term $\frac{log(q)}{2\pi i}$ converges to $i\infty$ as q converges to 0. This justifies the expression meromorphic or holomorphic at ∞.

We note that any weakly modular function can be written as

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n$$

for some $a_n \in \mathbb{C}$ where $q = e^{2\pi i z}$. This is just the Laurent series of $\tilde{f}(q) = f(z)$ in $q = 0$. The sum converges for all sufficiently large values of $\mathrm{Im}(z)$ as these correspond to sufficiently small values of $|q|$. If f is meromorphic at ∞, $a_n = 0$ for $n < -N$ and some $N \in \mathbb{N}$. Similarly, if f is holomorphic at ∞, $a_n = 0$ for $n < 0$. We call the above series the **q-expansion** of f.

Definition 1.3.3. Let f be a weakly modular function of weight k and level 1. If f is meromorphic at ∞ we say f is a **modular function** (of weight k and level 1). If f is holomorphic on $\mathcal{H}$ and holomorphic at ∞ we say f is a **modular form** (of weight k and level 1). A modular form f with $f(\infty) = 0$ is called a **cuspidal modular form** or **cusp form**.

As noted above the q-expansion of a weakly modular function f tells us directly whether f is a modular function, a modular form or a cups form.

1.4 Eistenstein series

We are now going to introduce the easiest example of a general modular form of nearly arbitrary weight k. Clearly we consider k to be even, since there are no non-trivial modular forms of odd weight as mentioned before. Following the notion introduced in the previous section we write q for $e^{2\pi i z}$.

Proposition 1.4.1. *Let $k \geq 4$ even. Define a function $G_k \colon \mathcal{H} \to \mathbb{C}$ by*

$$G_k(z) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{0\}} \frac{1}{(mz+n)^k}.$$

G_k is a modular form of weight k and level 1. The q-expansion of G_k is given by

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

where $\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$ (the Riemann zeta function) and $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$.

Proof. It can be shown that the sum defining G_k converges absolutely and uniformly on compact subsets of $\mathcal{H}$. Thus $G_k(z)$ is well-defined and holomorphic. Moreover we find that $G_k(z+1) = G_k(z)$ and

$$\begin{aligned} G_k\left(-\frac{1}{z}\right) &= \sum_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} \frac{1}{(m(-\frac{1}{z})+n)^k} \\ &= z^k \sum_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} \frac{1}{(-m+nz)^k} \\ &= z^k\, G_k(z). \end{aligned}$$

Therefore $G_k|_k S = G_k$ and $G_k|_k T = G_k$ where S, T as in Theorem 1.2.2 and thus G_k is a weakly modular function of weight k and level 1.

It remains to show that G_k is holomorphic at ∞. To see this we will determine the q-extension of G_k. Consider the formula $\sum_{n\in\mathbb{Z}} \frac{1}{z+n} = \pi \cdot \cot(\pi z)$. Using this we obtain

$$\sum_{n\in\mathbb{Z}} \frac{1}{z+n} = \pi \cdot \frac{\cos(\pi z)}{\sin(\pi z)} = i\pi \left(\frac{e^{2\pi i z}+1}{e^{2\pi i z}-1}\right) = i\pi\left(1+\frac{2}{q-1}\right) = i\pi - 2\pi i \sum_{n=0}^{\infty} q^n.$$

Differentiating $(k-1)$ times (remember that k is even by assumption) with respect to z leads to

$$\begin{aligned} \sum_{n\in\mathbb{Z}} \frac{-(k-1)!}{(z+n)^k} &= \frac{\partial^{k-1}}{\partial z^{k-1}}\left(i\pi - 2\pi i \sum_{n=0}^{\infty} q^n\right) \\ &= -2\pi i \sum_{n=1}^{\infty} (2\pi i n)^{k-1} q^n \\ &= -(2\pi i)^k \sum_{n=1}^{\infty} n^{k-1} q^n \end{aligned}$$

Hence we get

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

Now we can split up the original sum of the function G_k into two parts, one where $m = 0$ and one where $m \neq 0$. Afterwards we will simplify both parts using the above formula and symmetry of the sums (remember again that k is even):

$$\begin{aligned}
G_k(z) &= \sum_{n\in\mathbb{Z}\setminus\{0\}} \frac{1}{n^k} + \sum_{m\in\mathbb{Z}\setminus\{0\}} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^k} \\
&= 2\sum_{n=1}^{\infty} \frac{1}{n^k} + 2\sum_{m=1}^{\infty} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^k} \\
&= 2\zeta(k) + 2\sum_{m=1}^{\infty} t_k(mz) \\
&= 2\zeta(k) + 2\sum_{m=1}^{\infty} \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} e^{2\pi i n m z} \\
&= 2\zeta(k) + \frac{2\cdot(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n^{k-1} q^{nm}
\end{aligned}$$

From there we obtain the proposed q-expansion by resorting the last sum:

$$G_k(z) = 2\zeta(k) + \frac{2\cdot(2\pi i)^k}{(k-1)!} \sum_{l=1}^{\infty}\sum_{d|l} d^{k-1} q^l$$

Since G_k has a q-expansion without any negative powers of q, G_k is holomorphic at ∞. Thus G_k is indeed a modular form. □

Definition 1.4.2. Let $k \geq 4$ be even. The normalised **Eistenstein series** of weight k is given by

$$E_k(z) = \frac{1}{2\zeta(k)} G_k(z) = 1 + \gamma_k \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

where $\gamma_k = \frac{(2\pi i)^k}{(k-1)!\zeta(k)}$.

Remark. It can be shown that γ_k (for $k \geq 4$ even) is always rational. So for example

$$\gamma_4 = \frac{(2\pi i)^4}{3!\ \zeta(4)} = \frac{16\pi^4}{6\cdot\frac{\pi^4}{90}} = 240$$

and thus

$$E_4 = 1 + 240\sum_{n=1}^{\infty} \sigma_3(n) q^n.$$

But γ_k is not always an integer, for example $\gamma_{12} = \frac{65520}{691}$. In fact, it can even be shown $\gamma_k = -\frac{2k}{B_k}$ where B_k is the k'th Bernoulli number.

1.5 The valence formula

Let $f \neq 0$ be a meromorphic function $G \to \mathbb{C}$ and let $p \in G$. Recall that the unique integer n such that $(z-p)^{-n} f(z)$ is holomorphic and non-vanishing at p is called the order of f at p and denoted by $v_p(f)$. We say f has a zero of order n at p if n is positive, and f has a pole of order n at p if n is negative.

Let now f be a weakly modular funktion (of weight k and level 1). We claim that $v_p(f)$ is well-defined for p being a $\mathrm{SL}_2(\mathbb{Z})$ orbit in $\mathcal{H}$. To see this let n be the order of f at p, so $(z-p)^{-n} f(z) \to c \neq 0$ as $z \to p$. Moreover, let g be an element of $\mathrm{SL}_2(\mathbb{Z})$. An easy computation yields $g.z - g.p = (z-p) j(g,z)^{-1} j(g,p)^{-1}$. Hence

$$\begin{aligned}\lim_{z \to g.p} (z - g.p)^{-n} f(z) &= \lim_{z \to p} (g.z - g.p)^{-n} f(g.z) \\ &= \lim_{z \to p} \left(\frac{z-p}{g.z - g.p} \right)^n (z-p)^{-n} j(g,z)^k f(z) \\ &= j(g,p)^{k+2n} c.\end{aligned}$$

Therefore the order of f at $g.p$ is n since $j(g,p) \neq 0$, so $v_{g.p}(f) = v_p(f)$ as claimed. Further, if f is a modular function, we can define the order of f at ∞ by $v_\infty(f) := v_0(\tilde{f})$.

Theorem 1.5.1 (The valence formula)**.** *Let $f \neq 0$ be a modular function (of weight k and level 1). Then f has finitely many $\mathrm{SL}_2(\mathbb{Z})$-orbits of zeros and poles in $\mathcal{H}$, and*

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{p \in W} v_p(f) = \frac{k}{12}$$

where $\rho = e^{2\pi i/3}$ and W is the set of all $\mathrm{SL}_2(\mathbb{Z})$-orbits in $\mathcal{H}$ except the orbits of i and ρ.

Proof. Recall the fundamental domain from Theorem 1.2.2 and let $\mathcal{C}$ be the contour as shown in the figure below. Here $\mathrm{Im}(A) = \mathrm{Im}(E) = R$ and the three small cirlces have radius r.

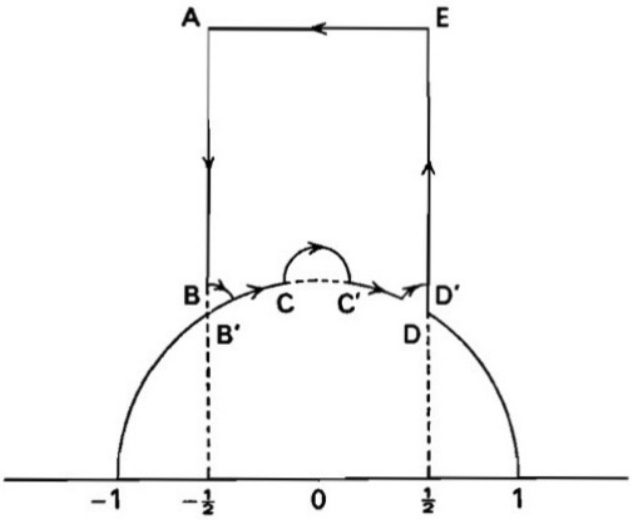
Let f be a modular function (of weight k and level 1) and assume for simplicity f has no zeros or poles on the boundary of D apart from possibly i, ρ and $\rho + 1$. We will now estimate $\int_{\mathcal{C}} f'(z)/f(z) dz$ in two different ways and compose the results afterwards.

(1) Estimating the integral by residue theorem yields

$$\int_{\mathcal{C}} \frac{f'(z)}{f(z)} dz = 2\pi i \sum_{p \in \mathrm{interior}(\mathcal{C})} \mathrm{Res}_p \left(\frac{f'}{f} \right).$$

It can be checked that f'/f has a pole at p if and only if $v_p(f) \neq 0$. In this case we have $\mathrm{Res}_p(f'/f) = v_p(f)$. Thus we get

$$\int_{\mathcal{C}} \frac{f'(z)}{f(z)} dz = 2\pi i \sum_{p \in \mathrm{interior}(\mathcal{C})} v_p(f) = 2\pi i \sum_{p \in W} v_p(f),$$



where W is the set described in the stated theorem. The last equality is satisfied for sufficiently small $r > 0$ since the interior of the fundamental domain contains exactly one representative of every pole or zero $\mathrm{SL}_2(\mathbb{Z})$-orbit of $\mathcal{H}$. This is true because by assumption no pole or zero of f lies on $\mathcal{C}$.

(2) Secondly, we estimate the integral by splitting up the contour in 8 parts. Let $\mathcal{C}_1$ be the part from E to A, $\mathcal{C}_2$ be the part from A to B, and so on, such that in the end $\mathcal{C}_8$ is the part from D' to E.

(i) First, note that $f = f(\,\cdot\, + 1)$ implies $f' = f'(\,\cdot\, + 1)$. Thus we have

$$\int_{\mathcal{C}_2} \frac{f'(z)}{f(z)} dz = \int_{\mathcal{C}_2} \frac{f'(z+1)}{f(z+1)} dz = -\int_{\mathcal{C}_8} \frac{f'(z)}{f(z)} dz.$$

So

$$\int_{\mathcal{C}_2} \frac{f'(z)}{f(z)} dz + \int_{\mathcal{C}_8} \frac{f'(z)}{f(z)} dz = 0.$$

(ii) Now we consider $\mathcal{C}_1$ and change the variable by $q(z) = e^{2\pi i z}$. This maps $\mathcal{C}_1$ to a clockwise oriented circle around the origin with radius $e^{-2\pi R}$. Furthermore we have $f(z) = \tilde{f}(q(z))$, thus $f'(z) = \tilde{f}'(q(z))\; q'(z)$ and since f is a modular function, $\tilde{f}$ is meromorphic at 0. Therefore

$$\begin{aligned}\int_{\mathcal{C}_1} \frac{f'(z)}{f(z)} dz &= \int_{\mathcal{C}_1} \frac{\tilde{f}'(q(z))q'(z)}{\tilde{f}(q(z))} dz = \int_{q(\mathcal{C}_1)} \frac{\tilde{f}'(q)}{\tilde{f}(q)} dq \\ &= -2\pi i \operatorname{Res}_0\left(\frac{\tilde{f}'}{\tilde{f}}\right) = -2\pi i\; v_0(\tilde{f}) = -2\pi i\; v_\infty(f).\end{aligned}$$

(iii) $\mathcal{C}_5$ is half of a circle around i. Recall that f'/f has a pole at p if and only if $v_p(f) \neq 0$, and that in this case $\operatorname{Res}_p(f'/f) = v_p(f)$. If $v_i(f) \neq 0$ we can use the residue theorem to compute

$$\lim_{r\to 0}\int_{\mathcal{C}_5}\frac{f'(z)}{f(z)}dz = -\frac{1}{2}\ 2\pi i\ v_i(f).$$

If $f(i)=0$ the integrand f'/f is holomorphic at i and the left hand side goes to zero as $r\to 0$. Hence we still have equality since the right hand side is zero, too. Similarly we get for $\mathcal{C}_3$

$$\lim_{r\to\infty}\int_{\mathcal{C}_3}\frac{f'(z)}{f(z)}dz = -\frac{1}{6}\ 2\pi i\ v_\rho(f),$$

and for $\mathcal{C}_7$

$$\lim_{r\to\infty}\int_{\mathcal{C}_7}\frac{f'(z)}{f(z)}dz = -\frac{1}{6}\ 2\pi i\ v_{\rho+1}(f) = -\frac{1}{6}\ 2\pi i\ v_\rho(f).$$

(v) So it remains to study $\mathcal{C}_4$ and $\mathcal{C}_6$. Consider $u(z)=-z^{-1}$. This maps $\mathcal{C}_6$ to $-\mathcal{C}_4$ and we have $f(z)=z^{-k}f(u(z))$, hence

$$f'(z) = -kz^{-k-1}f(u(z)) + z^{-k}f'(u(z))q'(z).$$

So

$$\begin{aligned}\int_{\mathcal{C}_4}\frac{f'(z)}{f(z)}dz &= \int_{\mathcal{C}_4}\frac{-k}{z}dz + \int_{\mathcal{C}_4}\frac{f'(u(z))q'(z)}{f(u(z))}dz\\ &= \frac{2\pi ik}{12} + \int_{u(\mathcal{C}_4)}\frac{f'(u)}{f(u)}du\\ &= \frac{2\pi ik}{12} - \int_{\mathcal{C}_6}\frac{f'(u)}{f(u)}du\end{aligned}$$

and thus

$$\int_{\mathcal{C}_4}\frac{f'(z)}{f(z)}dz + \int_{\mathcal{C}_6}\frac{f'(z)}{f(z)}dz = 2\pi i\frac{k}{12}.$$

Composing (i) to (v) yields

$$\int_{\mathcal{C}}\frac{f'(z)}{f(z)}dz = 2\pi i\left(\frac{k}{12} - \frac{1}{3}v_\rho(f) - \frac{1}{2}v_i(f) - v_\infty(f)\right).$$

Combining this with the result in (1) gives us exactly the proposed formula. □

The valence formula is a very powerful tool in the study of modular forms. In the following we will investigate some of its consequences.

Definition 1.5.2. Let M_k be the set of all modular forms of weight k and level 1 and let S_k be the set of all cusp forms of weight k and level 1.

Remark. It can be easily checked that M_k and S_k are vektor spaces over $\mathbb{C}$ for all $k \in \mathbb{Z}$.

Proposition 1.5.3. *(a) $M_k = \{0\}$ for $k < 0$ and $k = 2$.*

(b) $S_k = \{0\}$ for $k < 12$.

(c) M_0 is the set of all constant functions $\mathcal{H} \to \mathbb{C}$ and thus isomorphic to $\mathbb{C}$.

Proof. For (a) let $f \in M_k$, $f \neq 0$. Then $v_z(f) \geq 0$ for all $z \in \mathcal{H} \cup \{\infty\}$. So by the valence formula we get $k \geq 0$. Moreover a sum of non-negative integer multiples of $\frac{1}{2}$ and $\frac{1}{3}$ can't equal $\frac{1}{6}$. Thus $k \neq 2$. To see (b), let $f \in S_k$, $f \neq 0$. Then $v_\infty(f) \geq 1$ and hence $k \geq 12$ by valence formula. Finally, let $f \in M_0$ for (c). Then the constant function $g := f(\infty)$ is also in M_0, so $f - g \in S_0$ and therefore $f = g$ since $S_0 = \{0\}$. □

Proposition 1.5.4. *S_{12} is one-dimensional over $\mathbb{C}$ and spanned by the cusp form*

$$\Delta(z) = \frac{E_4^3 - E_6^2}{1728} = q - 24q^2 + 252q^3 + \dots .$$

Moreover, Δ vanishes nowhere on $\mathcal{H}$.

Proof. By definition Δ is clearly in M_{12} and a direct calculation of the q expansion of Δ using the q-expansions of E_4 and E_6 gives that Δ vanishes at ∞. Hence $\Delta \in S_{12}$. The valence formula yields

$$v_\infty(\Delta) + \frac{1}{2}v_i(\Delta) + \frac{1}{3}v_\rho(\Delta) + \sum_{p \in W} v_p(\Delta) = 1,$$

so $v_\infty(\Delta) = 1$ and $v_p(\Delta) = 0$ for all $p \in \mathcal{H}$ since $v_\infty(\Delta) \geq 1$. Therefore Δ is non-vanishing on $\mathcal{H}$. To see that S_{12} is spanned by Δ let $f \in S_{12}$. We define a function g by

$$g(z) = f(z) - \frac{f(i)}{\Delta(i)}\Delta(z).$$

This function is well-defined since Δ does not vanish on $\mathcal{H}$, so $\Delta(i) \neq 0$. Clearly $g \in S_{12}$ and $g(i) = 0$. By the valence formula we have

$$v_\infty(g) + \frac{1}{2}v_i(g) + \frac{1}{3}v_\rho(g) + \sum_{p \in W} v_p(g) = 1.$$

But this is a contradiction since $v_\infty(g) \geq 1$ and $v_i(g) \geq 1$. Therefore g has to be zero and

$$f = \frac{f(i)}{\Delta(i)}\Delta \in \mathbb{C}\,\Delta.$$

□

Remark. In the prologue of this lecture we defined $\Delta = q \cdot \prod_{n \in \mathbb{N}}(1 - q^n)^{24}$. We will prove later that this is indeed the same Δ as the one from the previous proposition.

Corollary 1.5.5. *The map*

$$M_k \to S_{k+12},\ f \mapsto f \cdot \Delta$$

is an isomorphism and for $k \geq 4$ we have

$$M_k = S_k \oplus (\mathbb{C}\ E_k)\,.$$

Proof. The first statement is trivial for $k < 0$ since then $M_k = S_{k+12} = \{0\}$. So let $k \geq 0$. As Δ is non-vanishing the given map is clearly an injection. Now let $g \in S_{k+12}$. Then $\frac{g}{\Delta}$ is weakly modular of weight $(k+12) - 12 = k$ and holomorphic on $\mathcal{H}$ since Δ is non-vanishing. Furthermore $v_\infty(g) \geq 1$, hence

$$v_\infty\left(\frac{g}{\Delta}\right) = v_\infty(g) - v_\infty(\Delta) = v_\infty(g) - 1 \geq 0.$$

So $\frac{g}{\Delta} \in M_k$. Therefore the given map is also onto, thus bijectiv.

For the second part of the corollary we just have to note that S_k is the kernel of the linear map $M_k \to \mathbb{C},\ f \mapsto f(\infty)$. Thus we have $\dim(M_k/S_k) \leq 1$. On the other hand we know that $E_k \in M_k \setminus S_K$ since $E_k(\infty) \neq 0$. So $M_k = S_k \oplus (\mathbb{C}\ E_k)$. □

In particular the previous corollary shows that $M_k = (M_{k-12}\,\Delta) \oplus (\mathbb{C}\ E_k)$ since the isomorphism gives $S_k = M_{k-12}\Delta$. We will use this fact to prove the following theorem.

Theorem 1.5.6. *For $k \geq 0$ even we have*

$$\dim(M_k) = \begin{cases} 1 + \left\lfloor \frac{k}{12} \right\rfloor, & k \not\equiv 2 \bmod 12, \\ \left\lfloor \frac{k}{12} \right\rfloor, & k = 2 \bmod 12. \end{cases}$$

Otherwise, so if k is negative or odd, then $M_k = \{0\}$. In particular, M_k is finite dimensional over $\mathbb{C}$ for all $k \in \mathbb{Z}$. For any $k \in \mathbb{Z}$ a basis for M_k is given by the set

$$\left\{E_4^a E_6^b \colon a, b \in \mathbb{N}_0, 4a + 6b = k\right\}.$$

Proof. We will prove the formula for the dimension of M_k by induction on k. First of all note that the statement is clear for odd k since there aren't any nonzero weakly modular functions of odd weight, and for $k < 0$ since $M_k = \{0\}$ in this case by part (a) of Proposition 1.5.3.

Let us now consider even k's between 0 and 10. Using again Proposition 1.5.3 we have $\dim(M_0) = 1$, $\dim(M_2) = 0$ and $S_k = \{0\}$ for $k = 4, 6, 8, 10$. Hence $\dim(M_k) = 1$ for $k = 4, 6, 8, 10$ since $\dim(M_k) = \dim(S_k) + 1$ by Corollary 1.5.5. Therefore the statement is true for $k = 0, 2, \ldots, 10$. Let now $k \geq 12$ even. Corollary 1.5.5 yields

$$\dim(M_k) = \dim(S_k) + 1 = \dim(M_{k-12}) + 1.$$

Hence the statement is true for all k by induction in steps of 12.

It remains to prove that the set $\{E_4^a E_6^b \colon a, b \in \mathbb{N}_0, 4a + 6b = k\}$ is a basis of M_k for any k. First note that there is nothing to show for odd k, $k < 0$ and $k = 2$ since in these cases $M_k = \{0\}$. The case $k = 0$ is also trivial because M_0 is the set of all constant functions, hence generated by $1 = E_4^0 E_6^0$.

Let now $k \geq 4$ be even. We will again use induction in steps of 12. Note that there is always a pair (a, b) such that $a, b \in \mathbb{N}_0$ and $4a + 6b = k$. Pick such a pair. Let $f \in M_k$. Then f can be written in the form

$$f = \lambda \; E_4^a E_6^b + g$$

for some $\lambda \in \mathbb{C}$ and $g \in S_k$ since the modular form $E_4^a E_6^b$ is in M_k and does not vanish at infinity. So there is an $h \in M_{k-12}$ such that $g = h \cdot \Delta$ by Corollary 1.5.5 and by induction we may assume h to be a linear combination of $E_4^r E_6^s$ where $r, s \in \mathbb{N}_0$ and $4r + 6s = k - 12$. Hence

$$h \cdot \Delta = h \cdot \left(\frac{E_4^3 - E_6^2}{1726} \right)$$

is a linear combination of $E_4^{r+3} E_6^s$ and $E_4^r E_6^{s+2}$ and since

$$4(r + 3) + 6s = 4r + 6(s + 2) = k$$

the function h is a linear combination of $E_4^p E_6^q$ with $p + q = k$. So the linear span of these functions contains g and hence also f. Therefore

$$M_k = \operatorname{span}\{E_4^a E_6^b \colon a, b \in \mathbb{N}_0, 4a + 6b = k\}.$$

To show that the given set is indeed a basis of M_k it suffices to check that

$$\left| \left\{ (a, b) \in \mathbb{N}_0^2 \colon 4a + 6b = k \right\} \right| = \dim(M_k).$$

This can again be easily seen by induction in steps of 12. □

Example. Both, E_4^2 and E_8 are in M_8. But $\dim(M_8) = 1$ by Theorem 1.5.6. Hence E_4^2 and E_8 are linearly dependent and as both are 1 at infinity, we can conclude that E_4^2 and E_8 are equal. So

$$\left(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \right)^2 = E_4^2 = E_8 = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n,$$

or

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m) \sigma_3(n - m).$$

This is very hard to prove without using the theory of modular forms.

Proposition 1.5.7. *The q-expansion of Δ is given by*

$$\Delta(z) = q \cdot \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

Proof. Let $D(z) = q \cdot \prod_{n=1}^{\infty}(1-q^n)^{24}$ where $q = e^{2\pi i z}$ as usual. We can check that this product converges sufficiently fast for D to be defined and holomorphic on $\mathcal{H}$. Evidently $D(z+1) = D(z)$ and $D(z) \to 0$ as $\mathrm{Im}(z) \to \infty$. So it suffices to show that $D(-\frac{1}{z}) = z^{12}D(z)$. Define

$$E_2(z) = \frac{3}{\pi^2}\sum_{m\in\mathbb{Z}}\left(\sum_{n\in\mathbb{Z},(m,n)\neq 0}\frac{1}{(mz+n)^2}\right).$$

This is convergent and defines a holomorphic function on $\mathcal{H}$, but E_2 is no modular form of weight 2, thus not in M_2. Nevertheless, by arguing as in the proof of Proposition 1.4.1 we get

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n.$$

Moreover it can be shown that

$$E_2\left(-\frac{1}{z}\right) = z^2E_2(z) + \frac{6z}{\pi i}.$$

This can be found in the mentioned book of Serre, for example. Now we choose a branch of the complex logarithm holomorphic on $\mathbb{C}\setminus\{z \in \mathbb{C}\colon\ \mathrm{Re}(z) \leq 0, \mathrm{Im}(z) = 0\}$. We have $\log(q) = 2\pi i z + c$ for some constant c. Thus we get

$$\begin{aligned}
\frac{\partial}{\partial z}(\log(D(z))) &= \frac{\partial}{\partial z}\left(\log(q) + \sum_{n=1}^{\infty}24\log(1-q^n)\right)\\
&= 2\pi i + 24\sum_{n=1}^{\infty}\frac{-2\pi i n q^n}{1-q^n}\\
&= 2\pi i\left(1 - \sum_{n=1}^{\infty}nq^n\sum_{r=0}^{\infty}q^r\right)\\
&= 2\pi i\left(1 - \sum_{n=1}^{\infty}\sum_{r=0}^{\infty}nq^{nr}\right)\\
&= 2\pi i\left(1 - \sum_{n=1}^{\infty}\sigma_1(n)q^n\right)\\
&= 2\pi i\ E_2(z).
\end{aligned}$$

Hence finally

$$\begin{aligned}
\frac{\partial}{\partial z}\left(\log\left(\frac{D(-1/z)}{z^{12}D(z)}\right)\right) &= \frac{1}{z^2}2\pi i\ E_2\left(-\frac{1}{z}\right) - \frac{12}{z} - 2\pi i\ E_2(z)\\
&= \frac{2\pi i}{z^2}\left(E_2\left(-\frac{1}{z}\right) - \left(z^2E_2(z) + \frac{6z}{i\pi}\right)\right)\\
&= 0.
\end{aligned}$$

So there is a constant λ sucht that $D(-\frac{1}{z}) = \lambda z^{12}D(z)$ for all $\lambda \in \mathcal{H}$. For $z = i$ solves this to $D(i) = D(-\frac{1}{i}) = \lambda D(i)$, and since $D(i) \neq 0$ we have $\lambda = 1$. Therefore we finally see $D(-\frac{1}{z}) = z^{12}D(z)$. □

1.6 Hecke operators

In this section, we will first interpret level 1 modular forms as functions on lattices and use this correspondance afterwards to define linear operators on the spaces of modular forms. These operators will be so called Hecke operators. We start by introducing the concept of lattices.

Definition 1.6.1. A **lattice** $\Lambda \subseteq \mathbb{C}$ is a discrete subgroup of $(\mathbb{C}, +)$ which is isomorphic to $\mathbb{Z}^2$. We say that lattices Λ and Λ' are **homothetic** if $\Lambda = \alpha\Lambda'$ for some $\alpha \in \mathbb{C}^\times$.

Examples. (i) The square lattice is given by $\mathbb{Z} + \mathbb{Z}i$.

(ii) The lattice $\mathbb{Z} + \mathbb{Z}\rho$ where $\rho = e^{2\pi i/3}$ is called grid of equivalental triangles.

Remark. Any lattice looks like $\mathbb{Z}\tau_1 + \mathbb{Z}\tau_2$ for some $\tau_1, \tau_2 \in \mathbb{C}$ with $\mathrm{Im}(\frac{\tau_1}{\tau_2}) \neq 0$ since otherwise the lattice lies inside a line in $\mathbb{C}$ and would thus not be discrete. Moreover, any lattice is clearly homothetic to $\mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathcal{H}$.

Lemma 1.6.2. *The lattices $\mathbb{Z} + \mathbb{Z}\tau$ and $\mathbb{Z} + \mathbb{Z}\sigma$, $\tau, \sigma \in \mathcal{H}$, are homothetic if and only if σ is in the $\mathrm{SL}_2(\mathbb{Z})$ orbit of τ.*

Proof. Let $\tau, \sigma \in \mathcal{H}$ such that σ is in the $\mathrm{SL}_2(\mathbb{Z})$ orbit of τ, so $\sigma = g.\tau$ for some $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then $\mathbb{Z} + \mathbb{Z}\tau$ is spanned by $\{a\tau + b, c\tau + d\}$ since $\det(g) = 1$. Thus

$$\mathbb{Z} + \mathbb{Z}\tau = \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d) = (c\tau + d)\left(\mathbb{Z} + \mathbb{Z}\frac{a\tau + b}{c\tau + d}\right) = \lambda(\mathbb{Z} + \mathbb{Z}(g.\tau))$$

with $\lambda = (c\tau + d) \in \mathbb{C}^\times$. Therefore $\mathbb{Z} + \mathbb{Z}\tau$ is homothetic to $\mathbb{Z} + \mathbb{Z}\sigma$.

Conversly let $\mathbb{Z} + \mathbb{Z}\tau$ be homthetic to $\mathbb{Z} + \mathbb{Z}\sigma$, $\tau, \sigma \in \mathcal{H}$. Then there is a $\lambda \in \mathbb{C}^\times$ such that

$$\mathbb{Z} + \mathbb{Z}\sigma = \lambda(\mathbb{Z} + \mathbb{Z}\tau) = \mathbb{Z}\lambda + \mathbb{Z}(\lambda\tau).$$

Clearly there are integers a, b, c, d such that $\lambda\tau = a\sigma + b$ and $\lambda = c\sigma + d$. Moreover, we see that $\{\lambda, \lambda\tau\}$ is a basis of $\mathbb{Z} + \mathbb{Z}\sigma$. Hence there are integers e, f, g, h such that

$$\sigma = e(\lambda\tau) + f\lambda = (ea + fc)\sigma + (eb + fd)$$
$$1 = g(\lambda\tau) + h\lambda = (ga + hc)\sigma + (gb + hd).$$

So $ea + fc = 1$, $eb + fd = 0$, $ga + hc = 0$, $gb + hd = 1$ and thus $\left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = 1$. As these are integer matrices we must have $\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \pm 1$. Finally note that

$$\tau = \frac{\lambda\tau}{\lambda} = \frac{a\sigma + b}{c\sigma + d} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.\sigma.$$

So the determinant of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is positive since $\tau, \sigma \in \mathcal{H}$. Therefore $\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = 1$, and thus $\tau \in \mathrm{SL}_2(\mathbb{Z})\sigma$ as claimed. □

Notice that Eisenstein series G_k are naturally sums over lattices. So we can see modular forms as functions on lattices.

Definition 1.6.3. Let $\mathcal{L}$ be the set of lattices. We say a function $F\colon \mathcal{L} \to \mathbb{C}$ is **homogenous of weight** k if $F(\alpha\Lambda) = \alpha^{-k}F(\Lambda)$ for all $\alpha \in \mathbb{C}^\times$, $\Lambda \in \mathcal{L}$.

Proposition 1.6.4. *(a) Let $F\colon \mathcal{L} \to \mathbb{C}$ be homogenous of weight k. Then $f\colon \mathcal{H} \to \mathbb{C}$ defined by*

$$f(\tau) = F(\mathbb{Z} + \mathbb{Z}\tau)$$

satisfies $f|_k g = f$ for all $g \in \mathrm{SL}_2(\mathbb{Z})$.

(b) Conversly, if $f\colon \mathcal{H} \to \mathbb{C}$ satisfies $f|_k g = f$ for all $g \in \mathrm{SL}_2(\mathbb{Z})$, we can find a homogenous function $F\colon \mathcal{L} \to \mathbb{C}$ of weight k such that

$$F(\mathbb{Z} + \mathbb{Z}\tau) = f(\tau).$$

Proof. For (a) let $F\colon \mathcal{L} \to \mathbb{C}$ be homogenous of weight k and $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Defining $f\colon \mathcal{H} \to \mathbb{C}$ by $f(\tau) = F(\mathbb{Z} + \mathbb{Z}\tau)$ we see that

$$\begin{aligned} f(g.\tau) &= F\left(\mathbb{Z} + \mathbb{Z}\frac{a\tau + b}{c\tau + d}\right) = F\Big(\frac{1}{c\tau + d}\big(\underbrace{\mathbb{Z}(c\tau + d) + \mathbb{Z}(a\tau + b)}_{=\mathbb{Z}+\mathbb{Z}\tau}\big)\Big) \\ &= (c\tau + d)^k F(\mathbb{Z} + \mathbb{Z}\tau) = j(g, z)^k f(\tau). \end{aligned}$$

Conversly, suppose for (b) that $f\colon \mathcal{H} \to \mathbb{C}$ satisfies $f|_k g = f$ for all $g \in \mathrm{SL}_2(\mathbb{Z})$ and define $F\colon \mathcal{L} \to \mathbb{C}$ by

$$F(\mathbb{Z}\tau_1 + \mathbb{Z}\tau_2) = \tau_1^{-k} f\left(\frac{\tau_2}{\tau_1}\right)$$

where $\mathrm{Im}(\frac{\tau_2}{\tau_1}) > 0$. It is easy to see $f|_k g = f$ implies that the definition of F is independent of the choice of basis (τ_1, τ_2). Moreover, F is clearly homogenous of weight k and satisfies $F(\mathbb{Z} + \mathbb{Z}\tau) = f(\tau)$. □

We will now define operators on the space of complex valued functions on lattices and afterwards use the above correspondance to let these operators act on the space of modular forms.

Definition 1.6.5. Let $F\colon \mathcal{L} \to \mathbb{C}$.

(a) For $n \in \mathbb{N}$ define $T_n(F)\colon \mathcal{L} \to \mathbb{C}$ by

$$T_n(F)(\Lambda) = \sum_{\substack{\Lambda' \leq \Lambda \\ [\Lambda:\Lambda'] = n}} F(\Lambda')$$

where the sum goes over all subgroups Λ' of Λ of index n.

(b) For $\alpha \in \mathbb{C}^\times$ define $R_\alpha(F)\colon \mathcal{L} \to \mathbb{C}$ by

$$R_\alpha(F)(\Lambda) = F(\alpha\Lambda).$$

Obviously T_n and R_α are linear operators on the space of functions $F\colon \mathcal{L} \to \mathbb{C}$. Moreover, it can be easily checked that T_n and R_α commute for any $n \in \mathbb{N}$ and any $\alpha \in \mathbb{C}^\times$. Therefore they preserve each others eigenspaces. Now consider $F\colon \mathcal{L} \to \mathbb{C}$ being homogenous of weight k and fix any $\alpha \in \mathbb{C}^\times$. Then

$$R_\alpha(F)(\Lambda) = F(\alpha\Lambda) = \alpha^{-k}F(\Lambda).$$

Hence F is an eigenvector of R_α with eigenvalue α^{-k}. Conversly, any function $F\colon \mathcal{L} \to \mathbb{C}$ that is a simultaneous eigenvector of R_α with eigenvalue α^{-k} for all $\alpha \in \mathbb{C}^\times$ is homogenous of weight k. This shows that T_n preserves homogenous functions of weight k for any k and any n since T_n preserves all eigenspaces of all R_α, $\alpha \in \mathbb{C}^\times$.

Proposition 1.6.6. *Let $F\colon \mathcal{L} \to \mathbb{C}$. Then*

(a) $T_m(T_n(F)) = T_{mn}(F)$ for all m, n coprime,

(b) $T_{p^n}(F) = T_p(T_{p^{n-1}}(F)) - p \cdot R_p(T_{p^{n-2}}(F))$ for all $n \geq 2$ and p prime.

Proof. For (a) note that

$$T_m(T_n(F))(\Lambda) = \sum_{\substack{\Lambda' \leq \Lambda \\ [\Lambda:\Lambda']=m}} T_n(F)(\Lambda') = \sum_{\substack{\Lambda' \leq \Lambda \\ [\Lambda:\Lambda']=m}} \sum_{\substack{\Lambda'' \leq \Lambda' \\ [\Lambda':\Lambda'']=n}} F(\Lambda'').$$

Claim. Let m, n coprime and $\Lambda'' \leq \Lambda$ be a subgroup of index mn. Then there is a unique Λ' such that $\Lambda'' \leq \Lambda' \leq \Lambda$, $[\Lambda' : \Lambda''] = n$ and $[\Lambda : \Lambda'] = m$.

Proof of claim. The abelian group Λ/Λ'' has order mn. Since m, n are coprime an element of this group has order dividing m if and only if it's a multiple of n. Thus there is a unique subgroup of order n. Let Λ' be the preimage of this subgroup. $\square$

Hence the above sum over all $\Lambda' \leq \Lambda$ of index m and all $\Lambda'' \leq \Lambda$ of index n contains every sublattice Λ'' exactly once. So

$$T_m(T_n(F))(\Lambda) = \sum_{\substack{\Lambda'' \leq \Lambda \\ [\Lambda:\Lambda'']=mn}} F(\Lambda'') = T_{mn}(F)(\Lambda'').$$

It remains to prove part (b). If m, n are not coprime the above claim does not work. (For example $\mathbb{Z}_2 \times \mathbb{Z}_2$ does not have a unique subgrup of order 2.) In fact the following holds:

Claim. Let $\Lambda'' \leq \Lambda$ be a subgroup of index mn, then either

- $\Lambda'' \subset p\Lambda$ and there are $(p+1)$ lattices $\Lambda' \leq \Lambda$ of index p containing Λ'', or
- $\Lambda'' \not\subset p\Lambda$, in which case there is exactly one such Λ'.

Proof of claim. Consider the image of Λ'' in $\Lambda/p\Lambda \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Since this is not everything it has either order 1 or order p. If the order is 1 then $\Lambda'' \subset p\Lambda$, and any index p sublattice of Λ contains Λ'' since they all contain $p\Lambda$. There are $p+1$ of these sublattices. On the contrary, if the order is p then any index p sublattice $\Lambda' \leq \Lambda$ containing Λ'' must also contain $\Lambda'' + p\Lambda$. But this has already index p in Λ, so it's the only possibility. □

Hence

$$\begin{aligned} T_p\left(T_{p^{n-1}}(F)\right)(\Lambda) &= \sum_{\substack{\Lambda' \leq \Lambda \\ [\Lambda:\Lambda']=p}} \sum_{\substack{\Lambda'' \leq \Lambda' \\ [\Lambda':\Lambda'']=p^{n-1}}} F(\Lambda'') \\ &= \sum_{\Lambda'' \text{ of case } 1} (p+1)F(\Lambda'') + \sum_{\Lambda'' \text{ of case } 2} F(\Lambda''). \end{aligned}$$

On the other hand

$$T_{p^n}(F)(\Lambda) = \sum_{\substack{\Lambda'' \leq \Lambda \\ [\Lambda:\Lambda'']=p^n}} F(\Lambda''),$$

so

$$T_p\left(T_{p^{n-1}}(F)\right)(\Lambda) - T_{p^n}(F)(\Lambda) = p \sum_{\Lambda'' \text{ of case } 1} F(\Lambda'').$$

But lattices of the first case are exactly index p^{n-2} sublattices of $p\Lambda$. Thus

$$\sum_{\Lambda'' \text{ of case } 1} F(\Lambda'') = T_{p^{n-2}}(F)(p\Lambda) = R_p\left(T_{p^{n-2}}(F)\right)(\Lambda).$$

This proves the second formula. □

Corollary 1.6.7. *The family of operators $(T_n)_{n\in\mathbb{N}}$ on the space of functions $\mathcal{L} \to \mathbb{C}$ all commute and can be written as polynomials in $(T_p)_{p \text{ prim}}$ and $(R_p)_{p \text{ prim}}$.*

Proof. By induction and Proposition 1.6.6 (b) every T_{p^n} where p prim can be written as a polynomial in T_p and R_p. Using part (a) of the same proposition we get the statement for all T_n. □

Definition 1.6.8. Let $f\colon \mathcal{H} \to \mathbb{C}$ satisfy $f|_k g = f$ for all $g \in \mathrm{SL}_2(\mathbb{Z})$. Further, let $F\colon \mathcal{L} \to \mathbb{C}$ be the function corresponding to f in terms of Proposition 1.6.4. We define $T_n(f)$ for $n \in \mathbb{N}$ as the function $\mathcal{H} \to \mathbb{C}$ corresponding to $n^{k-1}T_n(F)\colon \mathcal{L} \to \mathbb{C}$, so

$$T_n(f)(\tau) = n^{k-1}T_n(F)(\mathbb{Z} + \mathbb{Z}\tau).$$

Remark. The fudge factor n^{k-1} will give us nicer formulae later.

Proposition 1.6.9. *(a) Let p be prime. Then*

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

(b) *The operators T_n preserve the spaces of (weakly) modular functions, modular forms and cusp forms.*

(c) *Let m, n be coprime and p be prime. Then*

$$T_{mn}(f) = T_m T_n(f)$$

and for all $n \geq 2$

$$T_{p^n}(f) = T_p T_{p^{n-1}}(f) - p^{k-1} T_{p^{n-2}}(f).$$

Proof. We will first prove (c). Let $f\colon \mathcal{H} \to \mathbb{C}$ satisfy $f|_k g = f$ for all $g \in \mathrm{SL}_2(\mathbb{Z})$ and correspond to $F\colon \mathcal{L} \to \mathbb{C}$. Then $T_n(f)$ corresponds to $n^{k-1} T_n(F)$ for all $n \in \mathbb{N}$. Let m, n be coprime and p be prime. By part (a) of Proposition 1.6.6 we have

$$(mn)^{k-1} T_{mn}(F) = \left(m^{k-1} T_m\right) \left(n^{k-1} T_n\right)(F),$$

so the first relation is clear. For the second one consider

$$\begin{aligned}
(p^n)^{k-1}\ T_{p^n}(F) &= p^{(k-1)n}\ T_p T_{p^{n-1}}(F) - p^{(k-1)n} p\ R_p T_{p^{n-2}}(F) \\
&= \left(p^{k-1}\ T_p\right)\left(\left(p^{n-1}\right)^{k-1}\ T_{p^{n-1}}\right)(F) - p^{(k-1)n+1-k}\ T_{p^{n-2}}(F) \\
&= \left(p^{k-1}\ T_p\right)\left(\left(p^{n-1}\right)^{k-1}\ T_{p^{n-1}}\right)(F) - p^{k-1}\left(\left(p^{n-2}\right)^{k-1}\ T_{p^{n-2}}\right)(F),
\end{aligned}$$

where we used Proposition 1.6.6 (b). So (c) is done and we will prove (a) next. Therefore consider the index p sublattices of $\mathbb{Z} + \mathbb{Z}\tau$. These are given by

$$\left\{\mathbb{Z}p + \mathbb{Z}\tau, \mathbb{Z}p + \mathbb{Z}(\tau+1), \ldots, \mathbb{Z}p + \mathbb{Z}(\tau + p - 1), \mathbb{Z} + \mathbb{Z}(p\tau)\right\}.$$

So

$$\begin{aligned}
T_p(f)(\tau) &= p^{k-1}\ T_p(F)(\mathbb{Z} + \mathbb{Z}\tau) \\
&= p^{k-1}\ \left(\sum_{j=0}^{p-1} p^{-k} F\left(\mathbb{Z} + \mathbb{Z}\frac{\tau+j}{p}\right) + F\left(\mathbb{Z} + \mathbb{Z}(p\tau)\right)\right) \\
&= \frac{1}{p}\ \sum_{j=0}^{p-1} F\left(\mathbb{Z} + \mathbb{Z}\frac{\tau+j}{p}\right) + p^{k-1} F\left(\mathbb{Z} + \mathbb{Z}(p\tau)\right) \\
&= \frac{1}{p}\ \sum_{j=0}^{p-1} f\left(\frac{\tau+j}{p}\right) + p^{k-1} f(p\tau).
\end{aligned}$$

as required. It remains to prove (b). Therefore we have to show that if $f\colon \mathcal{H} \to \mathbb{C}$ is a weakly modular function, a modular function, a modular form or a cusp form, then the same holds for $T_n(f)$ for all $n \in \mathbb{N}$.

Obviously $T_n(f)$ respects the weight k action of $SL_2(\mathbb{Z})$. So it remains to prove that $T_n(f)$ is holomorphic (meromorphic) at $z \in \mathcal{H} \cup \{\infty\}$ if f is, and vanishing at ∞ if f is.

By construction we can assume without loss of generality that $n = p$ prime since T_n is a polynomial in the T_q for primes q dividing n by part (c) of this proposition. By part (a) we have

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

So $T_p(f)$ is holomorhpic (meromorphic) on $\mathcal{H}$ if f is. To handle $T_p(f)$ at ∞ we calculate the q expansion of $T_p(f)$. Suppose $f(z) = \sum_{n=-N}^{\infty} a_n q^n$ for some $N \in \mathbb{Z}$. Since

$$q\left(\frac{z+j}{p}\right) = e^{2\pi i(z+j)/p} = e^{2\pi iz/p} e^{2\pi ij/p}$$

we have

$$\begin{aligned} T_p(f)(z) &= \frac{1}{p} \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) + p^{k-1} f(pz) \\ &= \frac{1}{p} \sum_{j=0}^{p-1} \sum_{n=-N}^{\infty} a_n e^{2\pi inz/p} e^{2\pi inj/p} + p^{k-1} \sum_{n=-N}^{\infty} a_n e^{2\pi inpz} \\ &= \sum_{n=-N}^{\infty} a_n e^{2\pi inz/p} \left(\frac{1}{p} \sum_{j=0}^{p-1} e^{2\pi inj/p}\right) + p^{k-1} \sum_{n=-N}^{\infty} a_n e^{2\pi inpz} \end{aligned}$$

Consider the sum in the brackets: If p divides n, it's 1, and if p does not divide n, it's a sum of all the p'th roots of 1 in $\mathbb{C}$ which sum up to zero. So

$$\begin{aligned} T_p(f)(z) &= \sum_{n \geq -N,\ p|n} a_n e^{2\pi inz/p} + p^{k-1} \sum_{n=-N}^{\infty} a_n e^{2\pi inpz} \\ &= \sum_{n=-\lfloor N/p \rfloor}^{\infty} a_{np} e^{2\pi inz} + p^{k-1} \sum_{n=-N}^{\infty} a_n e^{2\pi inpz} \\ &= \sum_{n=-\lfloor N/p \rfloor}^{\infty} a_{np} q^n + p^{k-1} \sum_{n=-N}^{\infty} a_n q^{np}. \end{aligned}$$

Therefore $T_p(f)$ has a pole at ∞ of order lower or equal than pN (by the second sum), so it's meromorphic at ∞ if f is, and if f is holomorphic at ∞, we can take $N = 0$, thus $T_p(f)$ is also holomorphic at ∞ if f is. Finally $T_p(f)(\infty) = (1 + p^{k-1}) f(\infty)$, so $T_p(f)(\infty) = 0$ if $f(\infty) = 0$. □

In particular the last proposition shows that the operators $(T_n)_{n \in \mathbb{N}}$ act on the finite dimensional spaces M_k and S_k. We will see later that M_k and S_k have a basis of simultaneous eigenvectors for these operators.

In the following we will denote the n-th coefficient of the q-expansion of a modular form f by $a_n(f)$.

Lemma 1.6.10. *(a) For $f \in M_k$, p prime and $j \in \mathbb{N}$ we have*

$$\begin{aligned} T_{p^j}(f) \;=\; & \sum_{n=0}^{\infty} a_{np^j}(f)q^n \;+\; p^{k-1}\sum_{n=0}^{\infty} a_{np^{j-1}}(f)q^{np} \\ & + \; p^{2(k-1)}\sum_{n=0}^{\infty} a_{np^{j-2}}(f)q^{np^2} \;+\; \ldots \;+\; p^{j(k-1)}\sum_{n=0}^{\infty} a_n(f)q^{np^j}. \end{aligned}$$

(b) If m and n are coprime, then $a_m(T_n(f)) = a_{mn}(f)$ for $f \in M_k$. In particular, $a_n(f) = a_1(T_n(f))$ for all $n \in \mathbb{N}$.

Proof. We prove (a) by induction using the formula for T_p and recurrence for T_{p^j}. Therefore we define operators U,V on formal power series in q by

$$U\left(\sum b_n q^n\right) = \sum b_{np}q^n, \quad V\left(\sum b_n q^n\right) = p^{k-1}\sum b_n q^{np}.$$

We can easily check $U \circ V = p^{k-1}$, but U and V do not commute. Recall that we have seen at the end of the proof of Proposition 1.6.9 that

$$T_p(f)(z) = \sum_{n=-\lfloor N/p \rfloor}^{\infty} a_{np}(f)q^n + p^{k-1}\sum_{n=-N}^{\infty} a_n(f)q^{np}.$$

for f weakly modular of weight k. But as f is a modular form here, we can choose $N = 0$, so $\lfloor N/p \rfloor = N$, and thus $T_p = U + V$.

Claim. $T_{p^j} = U^j + VU^{j-1} + \ldots + V^{j-1}U + V^j$

Proof of claim. The statement is true for $j = 1$. So assume that it also holds for $j-1$. We have $T_{p^j} = T_p T_{p^{j-1}} - p^{k-1}T_{p^{j-2}}$ by part (c) of Proposition 1.6.9, so

$$\begin{aligned} T_{p^j} &= (U+V)(U^{j-1} + VU^{j-2} + \ldots + V^{j-1}) - UV(U^{j-2} + VU^{j-3} + \ldots + V^{j-2}) \\ &= U^j + (UVU^{j-2} + \ldots + UV^{j-1}) + (VU^{j-1} + \ldots + V^j) - (UVU^{j-2} + \ldots + UV^{j-1}) \\ &= U^j + VU^{j-1} + \ldots + V^{j-1}U + V^j \end{aligned}$$

as required. □

For (b) let $n = p_1^{\alpha_1}\ldots p_d^{\alpha_d}$ such that no p_i divides m. Then

$$a_m(T_n f) = a_m(T_{p_1^{\alpha_1}}\ldots T_{p_d^{\alpha_d}}f).$$

From part (a) we know that if p does not divide m then $a_m(T_{p_j}f) = a_{mp^j}(f)$. So

$$a_m(T_n f) = a_{mp_1^{\alpha_1}}(T_{p_2^{\alpha_2}}\ldots T_{p_d^{\alpha_d}}f) = \ldots = a_{mp_1^{\alpha_1}\ldots p_d^{\alpha_d}}(f) = a_{mn}(f).$$

□

Definition 1.6.11. A modular form $f \in M_k$, $f \neq 0$, is called an **eigenform** if f is an eigenvector for all T_n, $n \in \mathbb{N}$. If in addition $a_1(f) = 1$, we say f is a **normalised eigenform**.

Proposition 1.6.12. *(a) If f is an eigenform then $a_1(f) \neq 0$ unless $k = 0$.*

(b) If f is a normalised eigenform then

- *$a_{mn}(f) = a_m(f)a_n(f)$ for all m, n coprime, and*
- *$a_{p^j}(f) = a_p(f)a_{p^{j-1}}(f) - p^{k-1}a_{p^{j-2}}(f)$ for p prime, $j \geq 2$.*

Proof. For (a) let f be an eigenform, so $T_n f = \lambda_n f$ for some λ_n and all n. If $a_1(f) = 0$, then $a_1(T_n f) = 0$ for all n as $T_n f$ is a scalar multiple of f, and thus $a_n(f) = a_1(T_n f) = 0$ by Lemma 1.6.10 (b) for all n. Therefore all terms of the q-expansion of f after the constant term are zero. Thus f is constant, and hence $k = 0$.

For (b) let f be a normalised eigenform, so $a_1(f) = 1$ and $T_n f = \lambda_n f$ for some λ_n and all n. Then again $a_n(f) = a_1(T_n f) = \lambda_n a_1(f) = \lambda_n$ by Lemma 1.6.10 (b) for all n. Moreover, we have $a_{mn}(f) = a_m(T_n f)$ by the same lemma, so

$$a_{mn}(f) = a_m(\lambda_n f) = \lambda_n a_m(f) = a_n(f)a_m(f).$$

Similarly we see

$$\begin{aligned} a_{p^j}(f) &= a_1(T_{p^j} f) = a_1\left(T_p(T_{p^{j-1}} f) - p^{k-1}T_{p^{j-2}} f\right) \\ &= a_p(\lambda_{p^{j-1}} f) - p^{k-1}a_{p^{j-2}}(f) = a_{p^{j-1}}(f)a_p(f) - p^{k-1}a_{p^{j-2}}(f). \end{aligned}$$

□

Note that the previous proposition implies that the q-expansion of a normalised eigenform f is fully determined by its prime coefficients $a_p(f)$, p prime. Moreover, part (a) tells us that if $k > 0$ eigenforms can always be normalised. We will close this section with some examples.

Examples. (1) E_k is an eigenform for all $k \geq 4$ even, but not normalised.

Proof. It sufficies to show that E_k is an eigenvector of all T_p for p prime. Fix a prime p. We claim that E_k is eigenvector of T_p with eigenvalue $\sigma_{k-1}(p)$, so

$$T_p(E_k) = \sigma_{k-1}(p)E_k.$$

By Lemma 1.6.10 (a) we have

$$T_p(E_k) = \gamma_k \sum_{n=0}^{\infty} \sigma_{k-1}(np)q^n + p^{k-1}\gamma_k \sum_{n=0}^{\infty} \sigma_{k-1}(n)q^{np},$$

so

$$a_n(T_p(E_k)) = \gamma_k \cdot \begin{cases} \sigma_{k-1}(np), & \text{if } p \text{ does not divide } n, \\ \sigma_{k-1}(np) + p^{k-1}\sigma_{k-1}\left(\frac{n}{p}\right), & \text{if } p \text{ divides } n. \end{cases}$$

On the other hand we have $a_0(\sigma_{k-1}(p)E_k) = \sigma_{k-1}(p)$ and

$$a_n(\sigma_{k-1}E_k) = \gamma_k \sigma_{k-1}(p)\sigma_{k-1}(n)$$

for $n \geq 1$. The coefficients for $n = 0$ match since

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

So it remains to show

$$\sigma_{k-1}(p)\sigma_{k-1}(n) = \begin{cases} \sigma_{k-1}(np), & \text{if } p \text{ does not divide } n, \\ \sigma_{k-1}(np) + p^{k-1}\sigma_{k-1}\left(\frac{n}{p}\right), & \text{if } p \text{ divides } n, \end{cases}$$

for $n \geq 1$. This is clear if p does not divide n since then p and n are coprime. So assume $n = q^j$ for some $j \geq 1$. Then

$$\begin{aligned} \sigma_{k-1}(p)\sigma_{k-1}\left(p^j\right) &= \left(1 + p^{k-1} + \ldots + p^{j(k-1)}\right)\left(1 + p^{k-1}\right) \\ &= \left(1 + p^{k-1} + \ldots + p^{(j+1)(k-1)}\right) + \left(p^{k-1} + \ldots + p^{j(k-1)}\right) \\ &= \sigma_{k-1}\left(p^{j+1}\right) + p^{k-1}\sigma_{k-1}\left(p^{j-1}\right). \end{aligned}$$

as required. □

(2) A non-Eisenstein eigenform is given by Δ. This is clear since all T_n preserve S_{12} and S_{12} is spanned by Δ. Moreover Δ is obviously normalised. Let $\tau(n) = a_n(\Delta)$. Then

$$\tau(mn) = \tau(m)\tau(n)$$

for m and n coprime by Proposition 1.6.12 (b). This shows a statement which was made in the prologue of this lecture.

(3) Similarly we can show that the cusp forms $E_4\Delta$, $E_6\Delta$, $E_4^2\Delta$, $E_4E_6\Delta$ and $E_4^2E_6\Delta$ of weight 16, 18, 20, 22 and 26 are normalised eigenforms since the corresponding spaces of cusp forms are one-dimensional.

(4) More interesting is the case $k = 24$ since S_{24} is two-dimensional. It can easily be shown that S_{24} is spanned by $f_1 = E_4^3\Delta$ and $f_2 = \Delta^2$. The q-expansion of these are given by

$$\begin{aligned} f_1 &= q + 696q^2 + 162252q^3 + 12831808q^4 + \ldots \\ f_1 &= q^2 - 48q^3 + 1080q^4 + \ldots. \end{aligned}$$

We want to know how T_2 acts on this basis. By Lemma 1.6.10 (a) we have

$$\begin{aligned} T_2(f_1) &= \left(696q + 12831808q^2 + \ldots\right) + 2^{23}\left(q^2 + 696q^4 + \ldots\right) \\ &= 696q + 21220416q^2 + \ldots \end{aligned}$$

and

$$\begin{aligned} T_2(f_2) &= \left(q + 1080q^2 + \dots\right) + 2^{23}\left(q^4 + \dots\right) \\ &= q + 1080q^2 + \dots \end{aligned}$$

In terms of the given basis we therefore have

$$\begin{aligned} T_2(f_1) &= 696f_1 + 20736000f_2 \\ T_2(f_2) &= f_1 + 384f_2. \end{aligned}$$

Thus T_2 is given by the matrix

$$\begin{pmatrix} 696 & 1 \\ 20736000 & 384 \end{pmatrix}.$$

Clearly we can compute the matrix as in the last example for any T_n on any S_k and the computation can be done in finite time. Moreover this matrix has always entries in $\mathbb{Q}$ by construction. (In fact we can even show that the entries are in $\mathbb{Z}$.) But eigenforms are not generally defined over $\mathbb{Q}$. For example for $k = 24$, the eigenvalues of T_2 (and hence of T_n for all n) live in $\mathbb{Q}\left(\sqrt{144169}\right)$.

Open conjecture (Maeda's conjecture)**.** *The galois group of the splitting field of the characteristic polynomial of T_2 on S_k is as large as possible, so isomorphic to* $\mathrm{Sym}(d)$ *where $d = \dim(S_k)$.*

This conjecture was checked for many values of k by K. Buzzard.

Theorem 1.6.13. *For any k, S_k admits a basis of normalised eigenforms.*

Proof. Later in the course we will see that S_k has an inner product with respect to which the T_n's are self-adjoint. □

1.7 The L-function of a modular form

In this last section of the first chapter we will develop some analytic properties of modular forms. We start by describing the growth of the coefficients of the q-expansion of a modular form.

Proposition 1.7.1. *Let $f \in M_k$. Then there is $C > 0$ such that*

$$|a_n(f)| \leq C\,n^k.$$

Proof. It sufficies to show that this holds for $f = E_k$. So we have to find a $C > 0$ such that $\sigma_{k-1}(n) \leq Cn^k$. But $\sigma_{k-1}(n)$ is a sum of at most n integers each of which is less or equal than n^{k-1}. Thus $\sigma_{k-1}(n) \leq n^k$. □

We can improve this bound for cusp forms.

Proposition 1.7.2. *Let $f \in S_k$. Then there is $C > 0$ such that*

$$|a_n(f)| \leq C\, n^{\frac{k}{2}}.$$

To prove this proposition we will use the following lemma, which is also interesting on its own.

Lemma 1.7.3. *Let $f \in S_k$. Then there is $C > 0$ such that*

$$|f(z)| \leq C\ \mathrm{Im}(z)^{-k/2}.$$

In particular, the function $f(z)\,\mathrm{Im}(z)^{k/2}$ is bounded.

Proof. Let $f \in S_k$. Define $g(z) = |f(z)|^2\,\mathrm{Im}(z)^k$. We can check that g is $\mathrm{PSL}_2(\mathbb{Z})$-invariant. So it is bounded on $\mathcal{H}$ if and only if it is bounded on the funcamental domain D. But $D \cap \{z \in \mathbb{C} \colon |\mathrm{Im}(z)| \leq R\}$ is compact and $|f(z)\,\mathrm{Im}(z)^{k/2}| \to 0$ as $\mathrm{Im}(z) \to \infty$ since $\tilde{f}$ is holomorphic at 0 and vanishes there, so $|\tilde{f}(q)| < C|q|$ for small q and some $C > 0$. But $q = e^{2\pi i z}$ decreases faster than $\mathrm{Im}(z)^{k/2}$ increases. □

We are now able to prove the previous proposition.

Proof of Proposition 1.7.2. Let $f \in S_k$ and $\mathcal{C}$ be a circle around the origin with radius $r = e^{-2\pi/n}$, so $\mathcal{C}(t) = re^{2\pi i t} = e^{2\pi i(t+i/n)}$ for $t \in [0,1]$. Note that $r < 1$ for all $n \in \mathbb{N}$. Since $\tilde{f}$ is holomorphic on $\{q \in \mathbb{C} \colon |q| < 1\}$ with $\tilde{f}(e^{2\pi i z}) = f(z)$ we have

$$\begin{aligned} a_n(f) &= \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{\tilde{f}(q)}{q^{n+1}}dq = \frac{1}{2\pi i}\int_0^1 \frac{\tilde{f}(e^{2\pi i(t+i/n)})}{e^{2\pi i(t+i/n)(n+1)}}(2\pi i)e^{2\pi i(t+i/n)}dt \\ &= \int_{i/n}^{1+i/n} \frac{\tilde{f}(e^{2\pi i s})}{e^{2\pi i s n}}ds = \int_{i/n}^{1+i/n} \frac{f(s)}{e^{2\pi i n s}}ds. \end{aligned}$$

Using the previous lemma we get

$$|a_n(f)| \leq \int_{i/n}^{1+i/n} \frac{C\,\mathrm{Im}(s)^{-k/2}}{|e^{2\pi i n s}|}ds = \int_{i/n}^{1+i/n} \frac{Cn^{k/2}}{e^{2\pi n\,\mathrm{Im}(s)}}ds = \frac{Cn^{k/2}}{e^{2\pi}}\int_{i/n}^{1+i/n} ds = C'n^{\frac{k}{2}}.$$

□

Remark. It can be shown that $a_n(f) = O(n^{k-1+\varepsilon})$ for any $f \in M_k$ and any $\varepsilon > 0$. This is not very hard to prove. Moreover, one can show that $a_n(g) = O(n^{(k-1)/2+\varepsilon})$ for any $g \in S_k$ and any $\varepsilon > 0$, but this is very hard to prove and was shown by Deligne in 1970's.

Corollary 1.7.4. *The series*

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

converges for $\mathrm{Re}(s) > k+1$ if $f \in M_k$ and for $\mathrm{Re}(s) > \frac{k}{2}+1$ if $f \in S_k$.

Proof. Let $f \in M_k$. We know $\sum_{n=1}^{\infty} n^{-k}$ converges for $k > 1$. Using the bounds of Proposition 1.7.1 we get

$$\left| \frac{a_n(f)}{n^s} \right| \leq C n^{-(\mathrm{Re}(s)-k)}$$

since $|n^s| = n^{\mathrm{Re}(s)}$. So $L(f,s)$ converges if $\mathrm{Re}(s) > k+1$. Similarly we can show that $L(f,s)$ converges for $\mathrm{Re}(s) > \frac{k}{2} + 1$ if $f \in S_k$ by using Proposition 1.7.2. □

We call $L(f,s)$ the ***L*-function** attached to the modular form f and may see $L(f,s)$ as a generalisation of the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ which is convergent for $\mathrm{Re}(s) > 1$. It is well-known that

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

This identity was discovered by Euler. The following proposition tries to get a similar representation for $L(f,s)$.

Proposition 1.7.5. *If $f \in M_k$ is a normalised eigenform then*

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

*This is called the **Euler product** for $L(f,s)$.*

Proof. Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a normalised eigenform of weight k. By multiplicity of the a_n's for coprime arguments we have

$$a_{p_1^{b_1} \dots p_r^{b_r}} = a_{p_1^{b_1}} \dots a_{p_r^{b_r}}.$$

So

$$L(f,s) = \sum_{n = p_1^{b_1} \dots p_r^{b_r} \geq 1} \frac{a_{p_1^{b_1}} \dots a_{p_r^{b_r}}}{\left(p_1^{b_1}\right)^s \dots \left(p_r^{b_r}\right)^s} = \prod_{p \text{ prime}} \left(1 + \frac{a_p(f)}{p} + \frac{a_{p^2}(f)}{p^2} + \dots\right).$$

Define $L_p(f,s) = \sum_{b=0}^{\infty} a_{p^b}(f) p^{-bs}$. Then $L(f,s) = \prod_{p \text{ prime}} L_p(f,s)$ since the first term of the sum defining $L_p(f,s)$ is 1 as f is a normalised eigenform. To prove the claimed identity it remains to show that $L_p(f,s)\left(1 - a_p p^{-s} + p^{k-1}p^{-2s}\right) = 1$. This can be done by reordering the sums and using part (b) of Proposition 1.6.12.

$$\begin{aligned}
&L_p(f,s)\left(1 - a_p p^{-s} + p^{k-1}p^{-2s}\right) \\
&\quad = \sum_{b=0}^{\infty} a_{p^b} p^{-bs} - a_p \left(\sum_{b=0}^{\infty} a_{p^b} p^{-bs}\right) p^{-s} + p^{k-1} \left(\sum_{b=0}^{\infty} a_{p^b} p^{-bs}\right) p^{-2s} \\
&\quad = \sum_{b=0}^{\infty} a_{p^b} p^{-bs} - a_p \left(\sum_{b=1}^{\infty} a_{p^{b-1}} p^{-bs}\right) + p^{k-1} \left(\sum_{b=2}^{\infty} a_{p^{b-2}} p^{-bs}\right) \\
&\quad = \left(1 + a_p p^{-s}\right) - a_p p^{-s} + \sum_{b=2}^{\infty} \underbrace{\left(a_{p^b} - a_p a_{p^{b-1}} + p^{k-1} a_{p^{b-2}}\right)}_{=0} p^{-bs} \\
&\quad = 1.
\end{aligned}$$

So we have $L_p(f,s) = \left(1 - a_p p^{-s} + p^{k-1}p^{-2s}\right)^{-1}$ as required. □

Proposition 1.7.6. *Let $k \geq 4$ even. If $E'_k = \gamma_k^{-1} E_k$ is the normalised eigenform attached to E_k then*

$$L(E'_k, s) = \zeta(s)\zeta(s-k+1).$$

Proof. Using the previous proposition we directly get

$$\begin{aligned} L(E'_k, s) &= \prod_{p \text{ prime}} \left(1 - \sigma_{k-1}(p)p^{-s} + p^{k-1-2s}\right)^{-1} \\ &= \prod_{p \text{ prime}} \left(1 - \left(1 + p^{k-1}\right)p^{-s} + p^{k-1-2s}\right)^{-1} \\ &= \prod_{p \text{ prime}} \left(1 - p^{-s}\right)^{-1}\left(1 - p^{k-1-s}\right)^{-1} \\ &= \zeta(s)\zeta(s-k+1). \end{aligned}$$

□

Note that $L(E'_k, s)$ has a pole for $s = k$ since $\zeta(1)$ is not defined. But we also know that $\zeta(s)$ has an analytic continuation to all of $\mathbb{C}$ except for a simple pole at $s = 1$. Moreover, the Riemann zeta function has a functional equation which relates $\zeta(s)$ and $\zeta(1-s)$, namely

$$\zeta(1-s) = \frac{2}{(2\pi)^s}\cos\left(\frac{\pi s}{2}\right)\Gamma(s)\zeta(s).$$

This was proved by Riemann in 1843. Recall that $\Gamma(s) = \int_0^\infty y^{s-1}e^{-y}dy$. The integral is convergent for all $\mathrm{Re}(s) > 0$ and we have $\Gamma(n) = (n-1)!$, in fact $\Gamma(s+1) = s\Gamma(s)$ for all s. Defining the Riemann Xi function by

$$\xi(s) = \frac{s(s-1)}{2}\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

it is possible to prove that $\xi(1-s) = \xi(s)$. We will show that something similar holds for normalised eigenforms.

Proposition 1.7.7. *Define Λ for $f \in M_k$ by*

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

If $f \in S_k$ is a normalised eigenform then $\Lambda(f,s)$ has an analytic continuation to all $s \in \mathbb{C}$ and

$$\Lambda(f, k-s) = (-1)^{k/2}\Lambda(f,s).$$

Proof. Let $f \in S_k$ be a normalised eigenform. We have $L(f,s) = \sum_{n=1}^\infty a_n(f)n^{-s}$. By substitution we get

$$\int_0^\infty t^{s-1}e^{-2\pi n t}dt = \int_0^\infty \left(\frac{y}{2\pi n}\right)^{s-1} e^{-y}\frac{dy}{2\pi n} = \frac{\Gamma(s)}{(2\pi)^s}n^{-s}.$$

So

$$L(f,s) = \sum_{n=1}^{\infty} \left(a_n(f) \frac{(2\pi)^s}{\Gamma(s)} \int_0^{\infty} t^{s-1} e^{-2\pi n t} dt \right)$$

and

$$\Lambda(f,s) = \sum_{n=1}^{\infty} \left(a_n(f) \int_0^{\infty} t^{s-1} e^{-2\pi n t} dt \right).$$

For $\mathrm{Re}(s)$ being sufficiently large we can interchange sum an integral to get

$$\Lambda(f,s) = \int_0^{\infty} t^{s-1} \left(\sum_{n=1}^{\infty} a_n(f) e^{-2\pi n t} \right) dt = \int_0^{\infty} t^{s-1} f(it) dt.$$

Splitting the integral in two gives

$$\Lambda(f,s) = \int_0^{1} t^{s-1} f(it) dt + \int_1^{\infty} t^{s-1} f(it) dt.$$

We will now consider only the first integral. Substituting $t = u^{-1}$ yields

$$\int_0^1 t^{s-1} f(it) dt = \int_1^{\infty} u^{1-s} f\left(\frac{i}{u}\right) \left(-\frac{du}{u^2}\right).$$

Since f is a modular form

$$f\left(\frac{i}{u}\right) = \left(\frac{i}{u}\right)^{-k} f\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \left(\frac{i}{u}\right) \right) = (-1)^{\frac{k}{2}}\ u^k\ f(iu).$$

Hence

$$\int_0^1 t^{s-1} f(it) dt = (-1)^{\frac{k}{2}} \int_1^{\infty} u^{1-s} u^k f(iu) u^{-2} du = (-1)^{\frac{k}{2}} \int_1^{\infty} u^{k-1-s} f(iu) du,$$

and therefore

$$\Lambda(f,s) = \int_1^{\infty} \left(u^s + (-1)^{\frac{k}{2}} u^{k-s}\right) \frac{f(iu)}{u} du.$$

Now $f(iu)$ goes to zero so fast this integral converges for all $s \in \mathbb{C}$ and up to the factor $(-1)^{k/2}$ it's symmetric, so $\Lambda(k-s) = (-1)^{k/2}\Lambda(s)$. □

2 Modular forms of higher level

This second chapter will extend the definition of modular forms seen in the first chapter. Instead of considering functions that are invariant under the whole modular group, we will now investigate functions transforming nicely under subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

2.1 Congruence subgroups

Definition 2.1.1. For $N \in \mathbb{N}$ define the subgroup

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

We will call this group the **principal congruence subgroup of level** N. It is the kernel of the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, so it is normal in $\mathrm{SL}_2(\mathbb{Z})$. A soubgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing $\Gamma(N)$ for some N is called a **congruence subgroup**. The least N such that $\Gamma \geq \Gamma(N)$ is called the **level** of Γ.

Proposition 2.1.2. *Any congruence subgroup has finite index in* $\mathrm{SL}_2(\mathbb{Z})$.

Proof. It sufficies to show that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] < \infty$ for all $N \in \mathbb{N}$. But this is clear as $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \hookrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is finite. □

Remark. (i) In fact $\mathrm{SL}_2(\mathbb{Z})$ surjects onto $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for any N, but this is not obvious. (Moreover it can be shown that this is false for $\mathrm{GL}_2(\mathbb{Z})$). This statement goes by the name of "strong approximation for SL_2".

(ii) The converse to Proposition 2.1.2 is false. There exist finite index $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ which don't contain $\Gamma(N)$ for any N. (For example there is one of index 7.) But every finite index subgroup of $\mathrm{SL}_n(\mathbb{Z})$ is congruence for $n \geq 3$. So SL_2 is quite unusual. (Bass-Serre-Milnor theorem)

Definition 2.1.3. The standard congruence subgroups of level N are given by

- $\Gamma(N)$ as defined above,
- $$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\},$$
- $$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}.$$

For example $\left(\begin{smallmatrix} 3 & 4 \\ 5 & 7 \end{smallmatrix}\right)$ is in $\Gamma_0(5)$ but not in $\Gamma_1(5)$, $\left(\begin{smallmatrix} 11 & 13 \\ 5 & 6 \end{smallmatrix}\right)$ is in $\Gamma_1(5)$ but not in $\Gamma(5)$, and $\left(\begin{smallmatrix} 11 & 35 \\ 5 & 16 \end{smallmatrix}\right)$ is in $\Gamma(5)$. We will mostly be working with $\Gamma_0(N)$ and $\Gamma_1(N)$.

Definition 2.1.4. If $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, we say Γ is **even** if $-1 \in \Gamma$ and **odd** if $-1 \notin \Gamma$. Moreover, we write $\overline{\Gamma}$ for the image of Γ in $\mathrm{PSL}_2(\mathbb{Z})$. If Γ has finite index we define the **projective index** of Γ as $d_\Gamma = [\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}]$.

Note that

$$d_\Gamma = \begin{cases} [\mathrm{SL}_2(\mathbb{Z}) : \Gamma], & \text{for } \Gamma \text{ even}, \\ \frac{1}{2}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma], & \text{for } \Gamma \text{ odd}. \end{cases}$$

Definition 2.1.5. If $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ has finite index and $f \colon \mathcal{H} \to \mathbb{C}$, we say f is **a weakly modular function of weight** k **and level** Γ for some $k \in \mathbb{Z}$ if f is meromorhpic on $\mathcal{H}$ and $f|_k\gamma = f$ for all $\gamma \in \Gamma$.

Remark. If Γ is even, then there are no nonzero weakly modular functions of odd weight and level Γ as in the level 1 case. This is clear since $-1 \in \Gamma$ and k being odd directly implies $f(z) = -f(z)$ for all $z \in \mathcal{H}$.

Example 2.1.6. Let f be weakly modular of level $\mathrm{SL}_2(\mathbb{Z})$ and weight k. Then $f(Nz)$ is weakly modular of level $\Gamma_0(N)$ and weight k.

Proof. Define $F(z) = f(Nz)$ for $z \in \mathcal{H}$ and let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Note that

$$N(g.z) = \frac{aNz + bN}{cz + d} = \frac{aNz + bN}{\frac{c}{N}Nz + d} = \begin{pmatrix} a & bN \\ c/N & d \end{pmatrix}.(Nz).$$

Put $g' = \left(\begin{smallmatrix} a & Nb \\ c/N & d \end{smallmatrix}\right)$. Then $g' \in \mathrm{SL}_2(\mathbb{Z})$ since $g \in \Gamma_0(N)$. Moreover, we easily see that $j(g, z) = j(g', Nz)$. Hence

$$(F|_k g)(z) = j(g, z)^{-k} f(N(g.z)) = j(g', Nz)^{-k} f(g'.(Nz)) = f(Nz) = F(z).$$

So $z \mapsto f(Nz)$ is weakly modular of level $\Gamma_0(N)$. □

2.2 Behaviour at ∞

Let

$$P_\infty = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon c = 0 \right\}.$$

Any elemnt of P_∞ looks like $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} -1 & x \\ 0 & -1 \end{smallmatrix}\right)$ for $x \in \mathbb{Z}$, so there is an obvious isomorphism $P_\infty \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ let $\Gamma_\infty = \Gamma \cap P_\infty$. If $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] < \infty$ then $[P_\infty : \Gamma_\infty] < \infty$ also.

Proposition 2.2.1. *For $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index exactly one of the following holds:*

- *Γ is even and there is $h \in \mathbb{N}$ such that $\Gamma_\infty = \left\{ \pm\left(\begin{smallmatrix} 1 & th \\ 0 & 1 \end{smallmatrix}\right) \colon t \in \mathbb{Z} \right\}$.*

- Γ *is odd and there is* $h \in \mathbb{N}$ *such that* $\Gamma_\infty = \left\{ \left(\begin{smallmatrix} 1 & th \\ 0 & 1 \end{smallmatrix}\right) : t \in \mathbb{Z} \right\}$. *In this case we say* Γ *is odd and regular at* ∞.

- Γ *is odd and there is* $h \in \mathbb{N}$ *such that* $\Gamma_\infty = \left\{ (-1)^t \left(\begin{smallmatrix} 1 & th \\ 0 & 1 \end{smallmatrix}\right) : t \in \mathbb{Z} \right\}$. *In this case we say* Γ *is odd and irregular at* ∞.

Proof. Look at $\overline{\Gamma}_\infty = \Gamma_\infty / (\Gamma_\infty \cap \{\pm 1\})$. This is a finite index subgroup of $\overline{P}_\infty$ and clearly $\overline{P}_\infty \cong \mathbb{Z}$. So $\overline{\Gamma}_\infty \cong h\mathbb{Z}$ for some $h \in \mathbb{N}$. Now choose an element $g \in \Gamma_\infty$ whose image generates $\overline{\Gamma}_\infty$. Then either

- $g \in \Gamma_\infty$ and $-g \in \Gamma_\infty$, so we may assume $g = \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ and $\{g, -1\}$ generate Γ_∞,

- or $-1 \notin \Gamma_\infty$, so $g = \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right)$ but $-g \notin \Gamma_\infty$, giving the other two cases.

□

We will call the integer h introduced in the previous proposition the **width of the cusp** ∞ **for** Γ. So the width of ∞ for $\Gamma_1(N)$ is 1 for all N, as $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$, but the width of ∞ for $\Gamma(N)$ is N. We will denote the width by $h_\infty(\Gamma)$ and note that $h_\infty(\Gamma) = [\overline{P}_\infty : \overline{\Gamma}_\infty]$ which matches the least $h \in \mathbb{N}$ such that at least one of $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & -h \\ 0 & -1 \end{smallmatrix}\right)$ lies in Γ.

Proposition 2.2.2. *Let* $f\colon \mathcal{H} \to \mathbb{C}$ *be weakly modular of weight* k *and level* Γ. *Moreover, put* $h = h_\infty(\Gamma)$ *and* $q_h(z) = e^{2\pi i z/h}$.

- *If* k *is even or if* k *is odd and* Γ *is odd and regular at* ∞ *then there is a meromorphic function* $\tilde{f}$ *on the punctured disc* $B = \{q\colon 0 < |q| < 1\}$ *such that* $f(z) = \tilde{f}(q_h(z))$ *for all* $z \in B$.

- *If* k *is odd and* Γ *is odd and irregular at* ∞ *then there is a meromorphic function* $\tilde{f}$ *on the punctured disc* B *such that* $f(z) = e^{\pi i z/h} \tilde{f}(q_h(z))$ *for all* $z \in B$.

Note that we are not considering the case k being odd and Γ being even since this case is trivial by a previous remark.

Proof. We have that at least one of $\pm\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ lies in Γ by Proposition 2.2.1, so for all $z \in \mathcal{H}$ holds

$$f(z) = \left(f|_k \pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)\right)(z) = (\pm 1)^k f(z+h).$$

If k is even then $(\pm 1)^k = 1$, so $f = f(\cdot + h)$, and if Γ is odd and regular at ∞ then $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$, so we also have $f = f(\cdot + h)$. In both cases we can argue as in Section 1.3.

If k is odd and Γ is odd but not regular at ∞ then we only have $-\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$ and therefore $f = -f(\cdot + h)$. Define a function g on $\mathcal{H}$ by $g(z) = f(z)e^{-\pi i z/h}$. Then

$$g(z+h) = e^{-\pi i} f(z+h) e^{-\pi i z/h} = f(z) e^{-\pi i z/h} = g(z).$$

So we can argue for g as before and get $f(z) = e^{\pi i z/h} \tilde{g}(q_h(z))$. □

Definition 2.2.3. Let $f\colon \mathcal{H} \to \mathbb{C}$ be weakly modular of weight k and level Γ. We say that f is **meromorphic at** ∞ if $\tilde{f}$ is meromorphic at 0. Similarly we define f to be **holomorphic at** ∞ if $\tilde{f}$ is holomorphic at 0. If f is meromorphic at ∞ we define

$$v_{\infty,\Gamma}(f) = \begin{cases} v_0\left(\tilde{f}\right), & \text{if } k \text{ is even or if } k \text{ is odd and} \\ & \quad \Gamma \text{ is odd and regular at } \infty, \\ v_0\left(\tilde{f}\right) + \frac{1}{2}, & \text{if } k \text{ is odd and } \Gamma \text{ is odd and irregular at } \infty. \end{cases}$$

If $v_{\infty,\Gamma}(f) > 0$ we say f is **vanishing at** ∞. If f is holomorphic at ∞ we define

$$f(\infty) = \begin{cases} \tilde{f}(0), & \text{if } k \text{ is even or if } k \text{ is odd and} \\ & \quad \Gamma \text{ is odd and regular at } \infty, \\ 0, & \text{if } k \text{ is odd and } \Gamma \text{ is odd and irregular at } \infty. \end{cases}$$

The definition of $v_{\infty,\Gamma}(f)$ and $f(\infty)$ in the irregular case need some explanation: Let k be odd, Γ be odd and irregular at ∞ and let f be weakly modular of weight k and level Γ. Recall that the q-expansion of f is given by $f = e^{\pi i z/h}\tilde{f}(q_h)$ and note that $e^{\pi i z/h} = q_h^{1/2}$. This motivates the additional term $\frac{1}{2}$. Furthermore, the term ensures that $v_{\infty,\Gamma}(fg) = v_{\infty,\Gamma}(f) + v_{\infty,\Gamma}(g)$ since this would fail otherwise in the irregular case.

Now assume that f is holomorphic at ∞ and let $(z_n)_n \subseteq \mathbb{C}$ be a sequence with $\operatorname{Im}(z_n) \to \infty$. Then $\tilde{f}(q_h(z_n)) \to \tilde{f}(0)$ and therefore

$$|f(z_n)| = \left|e^{\pi i z/h}\tilde{f}(q_h)\right| = e^{-\pi \operatorname{Im}(z)/h}\left|\tilde{f}(q_h(z_n))\right| \to 0 \cdot \tilde{f}(0) = 0.$$

Hence also the definition of $f(\infty)$ in the irregular case is reasonable, and so f being holomorphic at ∞ implies f vanishes at ∞ in this case.

Lemma 2.2.4. *Let $f\colon \mathcal{H} \to \mathbb{C}$ be weakly modular of weight k and level Γ and let $g \in P_\infty$ but not necessarily in Γ_∞. Then $f|_k g$ is weakly modular of weight k and level $g^{-1}\Gamma g$. Moreover, $f|_k g$ is meromorphic at ∞ if and only if f is, $v_{\infty,g^{-1}\Gamma g}(f|_k g) = v_{\infty,\Gamma}(f)$ and $(f|_k g)(\infty) = f(\infty)$ if defined and if k is even.*

Proof. We first see that $f|_k g$ is indeed weakly modular of weight k and level $g^{-1}\Gamma g$ since

$$(f|_k g)\,|_k\left(g^{-1}\gamma g\right) = (f|_k\gamma)\,|_k g = f|_k g.$$

Now let $\gamma \in \Gamma$. Then $g^{-1}\gamma g \in P_\infty$ if and only if $\gamma \in P_\infty$ since $g \in P_\infty$. Therefore $(g^{-1}\Gamma g)_\infty = g^{-1}\Gamma_\infty g$, and as $\overline{P}_\infty$ is abelian we have $\overline{(g^{-1}\Gamma g)_\infty} = \overline{\Gamma}_\infty$. Thus

$$h_\infty\left(g^{-1}\Gamma g\right) = \left[\overline{P}_\infty : \overline{(g^{-1}\Gamma g)_\infty}\right] = \left[\overline{P}_\infty : \overline{\Gamma}_\infty\right] = h_\infty(\Gamma).$$

Put $h = h_\infty(\Gamma)$ and let $g = \pm\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$. Then $(f|_k g)(z) = (-1)^k f(z+t)$ and thus we have for k even or k being odd and Γ being odd an regular at ∞ that

$$(f|_k g)(z) = (\pm 1)^k\tilde{f}\left(q_h(z+t)\right) = (\pm 1)^k\tilde{f}\left(e^{2\pi i t/h}q_h(z)\right).$$

In the irregular case, so if k is odd and Γ is odd and irregular at ∞ we have

$$(f|_k g)(z) = (\pm 1)^k e^{\pi i(z+t)/h} \tilde{f}\left(q_h(z+t)\right) = e^{\pi iz/h}\left((\pm 1)^k e^{\pi it/h} \tilde{f}\left(e^{2\pi it/h} q_h(z)\right)\right).$$

Hence we get

$$\widetilde{(f|_k g)}(q_h) = \begin{cases} (\pm 1)^k \tilde{f}\left(e^{2\pi it/h} q\right), & \text{if } k \text{ is even or if } k \text{ is odd and} \\ & \Gamma \text{ is odd and regular at } \infty, \\ (\pm 1)^k e^{\pi it/h} \tilde{f}\left(e^{2\pi it/h} q\right), & \text{if } k \text{ is odd and } \Gamma \text{ is odd and irregular at } \infty. \end{cases}$$

So $\widetilde{f|_k g}$ is meromorphic or holomorphic at ∞ if and only if f is and the orders of vanishing agree if defined. Finally, we can note that also the value of f and $f|_k g$ at ∞ are equal if defined and if k is even. □

2.3 Cusps

Remember that the $\mathrm{SL}_2(\mathbb{Z})$-orbits in $\mathcal{H}$ all have representatives in the fundamental domain D as shown in Theorem 1.2.2. Similarly one can check that any $\Gamma_0(2)$-orbit in $\mathcal{H}$ contains a point of $D \cup (SD) \cup (STD)$ where $S, T \in \mathrm{SL}_2(\mathbb{Z})$ as in Theorem 1.2.2. Now consider $f\colon \mathcal{H} \to \mathbb{C}$ weakly modular of weight k and level $\Gamma_0(2)$. To control f at the boundary of $\mathcal{H}$ we need to impose restrictions as $z \to i\infty$ and as $z \to 0$ because of the new fundamental domain corresponding to $\Gamma_0(2)$. In this section we want to generalize this concept.

Definition 2.3.1. The **projective line over** $\mathbb{Q}$ is the set $\mathbb{P}^1_{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$. We give this an action of $\mathrm{SL}_2(\mathbb{Z})$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} .x = \frac{ax+b}{cx+d}$$

where the right hand side is interpreted as $\frac{a}{c}$ if $x = \infty$, and as ∞ if $cx + d = 0$.

We can see this action as a restriction of the action of $\mathrm{SL}_2(\mathbb{C})$ on the Riemann sphere $\mathbb{P}^1_{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$.

Proposition 2.3.2. $\mathrm{SL}_2(\mathbb{Z})$ *acts transitively on* $\mathbb{P}^1_{\mathbb{Q}}$.

Proof. Clearly it sufficies to show that for any $x \in \mathbb{P}^1_{\mathbb{Q}}$ we can map ∞ to x. For $x = \infty$ we have $\infty.1 = \infty$. So let $x = \frac{a}{c}$ with $a, c \in \mathbb{Z}$ coprime. Then there are $r, s \in \mathbb{Z}$ such that $ar + cs = 1$, thus $\left(\begin{smallmatrix} a & -s \\ c & r \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\left(\begin{smallmatrix} a & -s \\ c & r \end{smallmatrix}\right).\infty = x$. □

Definition 2.3.3. For $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index we define **the set of cusps of** Γ, denoted by $C(\Gamma)$, as the set of Γ-orbits in $\mathbb{P}^1_{\mathbb{Q}}$.

Example. Let p be prime. Then $C(\Gamma_0(p)) = \{[\infty], [0]\}$.

Proof. Let $\frac{u}{v} \in \mathbb{Q}$ with $u, v \in \mathbb{Z}$ coprime. Then there are $r, s \in \mathbb{Z}$ such that $ur + vs = 1$, so $\left(\begin{smallmatrix} u & -s \\ v & r \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\left(\begin{smallmatrix} u & -s \\ v & r \end{smallmatrix}\right).\infty = \frac{u}{v}$. We will distinguish two cases:

(1) If p divides v then $\left(\begin{smallmatrix} u & -s \\ v & r \end{smallmatrix}\right) \in \Gamma_0(p)$, so $\frac{u}{v} \in [\infty]$. Conversly, if $\gamma \in \Gamma_0(p)$ then p divides the denominator of $\gamma.\infty$ by definition. So the orbit of ∞ is given by all fractions $\frac{u}{v}$ with p dividing the denominator v.

(2) If v is not divisible by p we can note that

$$u(r + \lambda v) + v(s - \lambda u) = 1$$

and since p is not a divisor of v we find $\lambda \in \mathbb{Z}$ such that $r' = r+\lambda v \in p\mathbb{Z}$. Therefore $\left(\begin{smallmatrix} s' & u \\ -r' & v \end{smallmatrix}\right) \in \Gamma_0(p)$ where $s' = s - \lambda u$ and $\left(\begin{smallmatrix} s' & u \\ -r' & v \end{smallmatrix}\right).0 = \frac{u}{v}$ by definition. So $\frac{u}{v} \in [0]$. Conversly, if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(p)$ then p does not divide d since c, d are coprime. Thus p cannot divide the denominator of $\gamma.0$. Therefore the orbit of 0 is given by all fractions $\frac{u}{v}$ with p not dividing the denominator v.

Hence we have shown that $C(\Gamma_0(p)) = \{[\infty], [0]\}$. □

Remark. It can be shown that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(p)] = p + 1$ for p prime. So even though the index of $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathbb{Z})$ increases, the number of cusps stays the same.

In the following we want to describe the behaviour of a finite index subgroup Γ at its cusps in the way we already handled ∞. This will be done by using that $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1_{\mathbb{Q}}$. Hence, instead of considering a cusp c of Γ, we can consider the cusp ∞ of $g^{-1}\Gamma g$ choosing g such that $[g.\infty] = c$ in $C(\Gamma)$. But as g is not unique, we first need to show that this concept is independent of the choice of g.

Lemma 2.3.4. *Let $\Gamma \le \mathrm{SL}_2(\mathbb{Z})$ be of finite index and let $g, h \in \mathrm{SL}_2(\mathbb{Z})$. Then $[g.\infty] = [h.\infty]$ in $C(\Gamma)$ if and only if $h = \gamma g g_\infty$ for some $\gamma \in \Gamma$ and some $g_\infty \in P_\infty$.*

Proof. First let $[g.\infty] = [h.\infty]$ in $C(\Gamma)$. Then there is $\gamma \in \Gamma$ such that $\gamma(g.\infty) = h.\infty$ in $\mathbb{P}^1_{\mathbb{Q}}$, so $(h^{-1}\gamma g).\infty = \infty$. The stabilizer of ∞ in $\mathrm{SL}_2(\mathbb{Z})$ is precisely P_∞. Thus we have $h^{-1}\gamma g \in P_\infty$. Put $g_\infty = h^{-1}\gamma g$. Then $h = \gamma g (g_\infty)^{-1}$ as required.

Conversly suppose there are $\gamma \in \Gamma$ and $g_\infty \in P_\infty$ such that $h = \gamma g g_\infty$. Since g_∞ fixes ∞ we have $h.\infty = (\gamma g g_\infty).\infty = \gamma.(g.\infty)$. Hence $[g.\infty] = [h.\infty]$ in $C(\Gamma)$. □

An highbrow way of expressing the previous lemma is to say $C(\Gamma)$ is the double coset space $\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})/P_\infty$.

Lemma 2.3.5. *Let $\Gamma \le \mathrm{SL}_2(\mathbb{Z})$ be of finite index, $c \in C(\Gamma)$ and $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $[g.\infty] = c$. Then the set $(g^{-1}\Gamma g) \cap P_\infty$ is independent of the choice of g.*

Proof. Let $g, h \in \mathrm{SL}_2(\mathbb{Z})$ such that $[g.\infty] = [h.\infty] = c$. Then there are $\gamma \in \Gamma$ and $g_\infty \in P_\infty$ such that $h = \gamma g g_\infty$ by Lemma 2.3.4, so

$$\begin{aligned}\left(h^{-1}\Gamma h\right) \cap P_\infty &= \left(g_\infty^{-1} g^{-1} \gamma^{-1} \Gamma \gamma g g_\infty\right) \cap P_\infty \\ &= g_\infty^{-1}\left(\left(g^{-1}\Gamma g\right) \cap P_\infty\right) g_\infty = \left(g^{-1}\Gamma g\right) \cap P_\infty\end{aligned}$$

since $g_\infty \in P_\infty$ and P_∞ is abelian. □

Definition 2.3.6. For $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index and $c \in C(\Gamma)$ we define Γ_c to be $(g^{-1}\Gamma g)_\infty = (g^{-1}\Gamma g) \cap P_\infty$ where g is any element of $\mathrm{SL}_2(\mathbb{Z})$ with $[g.\infty] = c$.

Moreover, we write $h_\Gamma(c)$ for $[\overline{P}_\infty : \overline{\Gamma}_c] = h_\infty(g^{-1}\Gamma g)$. This is called the **width of the cusp** c **for** Γ. Similarily we define Γ to be **even**, **regular** or **irregular at** c if $g^{-1}\Gamma g$ is even, odd and regular, or odd and irregular at ∞.

The previous lemma ensures that this definition is well-defined. Note that Γ is even at a cusp c if and only if Γ itself is even since $-1 \in \Gamma$ if and only if $-1 \in \Gamma_c$.

Example. We want to determine the width of the cusps of $\Gamma_0(p)$ for p prime. Recall that $C(\Gamma_0(p)) = \{[\infty], [0]\}$. We already know how to compute the width of the cusp ∞: By finding the least $h \in \mathbb{N}$ such that at least one of $\pm\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ lies in Γ. So $h_{\Gamma_0(p)}(\infty) = 1$ since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(p)$.

It remains to consider the cusp 0. Note that $g.\infty = 0$ for $g = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Moreover,

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

so $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in g^{-1}\Gamma_0(p)g$ if and only if p divides b. In particular,

$$(\Gamma_0(p))_{[0]} = \left(g^{-1}\Gamma_0(p)g\right) \cap P_\infty = \pm \begin{pmatrix} 1 & p\mathbb{Z} \\ 0 & 1 \end{pmatrix}.$$

So the width of the cusp 0 is p.

Remarks. (1) If $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ is a normal subgroup then $g^{-1}\Gamma g = \Gamma$ for all $g \in \Gamma$. So all cusps have the same width and they are either all regular or all irregular.

(2) One can show that

$$\sum_{c \in C(\Gamma)} h_\Gamma(c) = d_\Gamma.$$

This will be a special case of Lemma 2.4.3 and shows in particular that the index of $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathbb{Z})$ is $p+1$ for p prime as remarked earlier in this section, since $\Gamma_0(p)$ is even, so $d_{\Gamma_0(p)} = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(p)]$.

Finally we are able to investigate the behaviour of weakly modular functions at cusps.

Proposition 2.3.7. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index, $c \in C(\Gamma)$ and $g, h \in \mathrm{SL}_2(\mathbb{Z})$ such that $[g.\infty] = [h.\infty] = c$. Moreover, let f be weakly modular of weight k and level Γ. Then $f|_k g$ is meromorphic at ∞ if and only if $f|_k h$ is, and the orders of vanishing at ∞ agree if defined.*

Proof. Since $[g.\infty] = [h.\infty]$ there are $\gamma \in \Gamma$ and $g_\infty \in P_\infty$ by Lemma 2.3.4 such that $h = \gamma g g_\infty$. Thus

$$f|_k h = ((f|_k\gamma)|_k g)\,|_k g_\infty = (f|_k g)|_k g_\infty.$$

By Lemma 2.2.4 we have that $(f|_k g)|_k g_\infty$ is indeed meromorphic if and only if $f|_k g$ is, and that they have the same order of vanishing at ∞ if defined. ∎

So we can define $v_{c,\Gamma}(f)$ as $v_{\infty,g^{-1}\Gamma g}(f|_k g)$ since this is independent of the choice of g. Moreover, we can define $f(c) = (f|_k g)(\infty)$ if f is holomorphic at c and if k is even, but if k is odd $f(c)$ is only defined up to change of sign, as shown in Lemma 2.2.4. We say that f **is holomorphic at** c if $v_{c,\Gamma}(f) \geq 0$ and that f **is vanishing at** c if $v_{c,\Gamma}(f) > 0$.

Definition 2.3.8. Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index and let f be weakly modular of weight k and level Γ. We say f is a **modular function** if f is meromorphic at every cusp, f is a **modular form** if f is holomorphic on $\mathcal{H}$ and at every cusp, and f is a **cusp form** if f is holomorphic on $\mathcal{H}$ and vanishes at every cusp.

Further, we define $M_k(\Gamma)$ to be the space of modular forms of level Γ and $S_k(\Gamma)$ to be the space of cusp forms of level Γ.

Examples. (1) Let f be a modular form of level 1 and put $g(z) = f(Nz)$. One can check that g is a modular form of level $\Gamma_0(N)$, and that g is a cusp form if f is.

(2) Define $f\colon \mathcal{H} \to \mathbb{C}$ by

$$f(z) = q \cdot \prod_{n=1}^{\infty} (1-q^n)^2 \left(1-q^{11n}\right)^2$$

where $q = e^{2\pi i z}$. One can check that f is a cusp form of weight 2 and level $\Gamma_0(11)$, so $f \in S_2(\Gamma_0(11))$. Moreover, f corresponds to the elliptic curve $y^2 + y = x^3 - x$.

2.4 The valence formula in arbitrary levels

Definition 2.4.1. For $z \in \mathcal{H}$ and $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index we let

$$n_\Gamma(z) = \left|\mathrm{stab}_{\overline{\Gamma}}(z)\right|.$$

Recall that for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ we have shown in Theorem 1.2.2 that $n_\Gamma(z) = 2$ if z is in the $\mathrm{SL}_2(\mathbb{Z})$-orbit of i, $n_\Gamma(z) = 3$ if z is in the $\mathrm{SL}_2(\mathbb{Z})$-orbit of ρ, and 1 otherwise. Hence $n_\Gamma(z) \in \{1, 2, 3\}$ for arbitrary $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ and $n_\Gamma(z) = 1$ unless z is in the $\mathrm{SL}_2(\mathbb{Z})$-orbit of i or ρ. If $n_\Gamma(z) > 1$ we say z is an **elliptic point of** Γ. Since Γ has finite index in $\mathrm{SL}_2(\mathbb{Z})$, there are only finitely many Γ-orbits of elliptic points. Often there are even none at all, for example for $\Gamma_1(N)$, $N \geq 4$.

Using this new definition we can restate the valence formula of Section 1.5: If f is a nonzero modular function of weight k and level 1, then

$$\sum_{z \in \mathrm{SL}_2(\mathbb{Z}) \backslash \mathcal{H}} \frac{v_z(f)}{n_{\mathrm{SL}_2(\mathbb{Z})}(z)} + v_\infty(f) = \frac{k}{12}.$$

Indeed, a more general statement holds for arbitrary finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 2.4.2 (The valence formula). *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index. If f is a nonzero modular function of weight k and level Γ then*

$$\sum_{z \in \Gamma \backslash \mathcal{H}} \frac{v_z(f)}{n_\Gamma(z)} + \sum_{c \in C(\Gamma)} v_{c,\Gamma}(f) = \frac{k\, d_\Gamma}{12}.$$

The proof of this will take us a while. We define $V_\Gamma(f)$ to be the left hand side of the formula and start by stating a purely group theoretic lemma which we will need in the following.

Lemma 2.4.3. *Let G be a group acting transitively on a set X and let H be a finite index subgroup of G. Then for any $x \in X$ the stabilizer of x in H has finite index in the stabilizer of x in G, so $[\mathrm{stab}_G(x) : \mathrm{stab}_H(x)] < \infty$, and*

$$\sum_{x \in H\backslash X} [\mathrm{stab}_G(x) : \mathrm{stab}_H(x)] = [G : H].$$

Note that this is a consequence of the orbit-stabilizer theorem if G and H are finite groups, but this is not enough for our purposes.

Proof. Let $g_1, \dots, g_n$ be representatives for $H\backslash G$, so $G = \bigcup_{i=1}^n Hg_i$ and $Hg_i \cap Hg_j = \emptyset$ for $i \neq j$. Pick any $x_0 \in X$ and fix a representative g_i. Let $u \in \mathrm{stab}_G(g_i x_0)$. There is $\alpha \in H$ and a unique g_j such that $ug_i = \alpha g_j$ since $G = \cup_{l=1}^n Hg_l$. So $g_i x_0 = ug_i x_0 = \alpha g_j x_0$ and thus $g_i x_0$ and $g_j x_0$ lie in the same H-orbit. Therefore we can define a map

$$\mathrm{stab}_G(g_i x_0) \to \{j \colon [g_j x_0] = [g_i x_0]\}$$

which maps u to j as described above. We claim that this map is surjectiv. To see this let k be in $\{j \colon [g_j x_0] = [g_i x_0]\}$. Then there is $h \in H$ such that $g_k x_0 = hg_i x_0$. Put $u := h^{-1} g_k g_i^{-1}$. Then $u \in \mathrm{stab}_G(g_i x_0)$ since $u(g_i x_0) = h^{-1} g_k x_0 = g_i x_0$. Let l be the image of u under the defined map, so $ug_i = \alpha g_l$ for some $\alpha \in H$. Then $h^{-1} g_k = ug_i = \alpha g_l$ which implies $l = k$ since $Hg_l \cap Hg_k = \emptyset$ for $l \neq k$. So we found $u \in \mathrm{stab}_G(g_i x_0)$ such that u is mapped to k.

Now consider $u, v \in \mathrm{stab}_G(g_i x_0)$ which map to the same j, so $ug_i = \alpha g_j$, $vg_i = \beta g_j$ for some $\alpha, \beta \in H$. Then

$$uv^{-1} = \alpha g_j g_i^{-1} g_i g_j^{-1} \beta^{-1} = \alpha\beta^{-1} \in \mathrm{stab}_G(g_i x_0) \cap H = \mathrm{stab}_H(g_i x_0).$$

Therefore the map

$$\mathrm{stab}_H(g_i x_0)\backslash \mathrm{stab}_G(g_i x_0) \to \{j \colon [g_j x_0] = [g_i x_0]\}$$

is also injective, so a bijection. In particular, for any i we have

$$[\mathrm{stab}_G(g_i x_0) : \mathrm{stab}_H(g_i x_0)] = \left|\{j \colon [g_j x_0] = [g_i x_0]\}\right|.$$

The right hand side of this equality is clearly finite as H has finite index in G. So by choosing $g_1 = 1_G$ we find $[\mathrm{stab}_G(x_0) : \mathrm{stab}_H(x_0)] < \infty$ as claimed.

Finally note that every H-orbit in X contains at least one of $g_1 x_0, \dots, g_n x_0$. To see this pick any y in a given H-orbit. Then there is $g \in G$ such that $gx_0 = y$ since G acts transitively on X. Moreover there is $h \in H$ and i such that $g = hg_i$ since $G = \cup_{i=1}^n Hg_i$. Thus we have $g_i x_0 = h^{-1} y$ and so $g_i x_0$ is in the H-orbit of y. Hence

$$\sum_{x \in H\backslash X} [\mathrm{stab}_G(x) : \mathrm{stab}_H(x)] = |\{1, \dots, n\}| = [G : H].$$

□

Before we continue to prove the valence formula we use the previous lemma to prove the following corollary which was remarked in Section 2.3.

Corollary 2.4.4. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index. Then*

$$\sum_{c \in C(\Gamma)} h_\Gamma(c) = d_\Gamma.$$

Proof. Put $G = \mathrm{PSL}_2(\mathbb{Z})$, $H = \overline{\Gamma}$ for some $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index and $X = \mathbb{P}^1_{\mathbb{Q}}$. Then G acts transitively on X. Recall that $\mathrm{stab}_G(\infty) = \overline{P}_\infty$. Now let $x \in X$ and choose $g \in G$ such that $g.\infty = x$. One can check that

$$\mathrm{stab}_G(x) = g\,\mathrm{stab}_G(\infty)g^{-1}, \quad \mathrm{stab}_H(x) = g\,\mathrm{stab}_{g^{-1}Hg}(\infty)g^{-1}.$$

Hence

$$[\mathrm{stab}_G(x) : \mathrm{stab}_H(x)] = [\mathrm{stab}_G(\infty) : \mathrm{stab}_{g^{-1}Hg}(\infty)]\,.$$

Finally note that

$$\mathrm{stab}_{g^{-1}Hg}(\infty) = (g^{-1}\overline{\Gamma}g) \cap \overline{P}_\infty = \overline{(g^{-1}\Gamma g) \cap P_\infty} = \overline{\Gamma}_c,$$

so $[\mathrm{stab}_G(x) : \mathrm{stab}_H(x)] = [\overline{P}_\infty : \overline{\Gamma}_c] = h_\Gamma(c)$. Therefore Lemma 2.4.3 yields

$$\sum_{c \in C(\Gamma)} h_\Gamma(c) = \sum_{x \in H \backslash X} [\mathrm{stab}_G(x) : \mathrm{stab}_H(x)] = [G : H] = d_\Gamma$$

since the set of Γ-orbits in $\mathrm{SL}_2(\mathbb{Z})$ matches the set of $\overline{\Gamma}$-orbits in $\mathrm{PSL}_2(\mathbb{Z})$. □

We will now have four more lemmas before we are finally able to prove the valence formula.

Lemma 2.4.5. *Let $\Gamma, \Gamma' \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index such that $\Gamma' \leq \Gamma$. Moreover, let f be a nonzero modular function of weight k and level Γ. Then*

$$V_{\Gamma'}(f) = \frac{d_{\Gamma'}}{d_\Gamma} \cdot V_\Gamma(f),$$

where $V_\Gamma(f)$ respectively $V_{\Gamma'}(f)$ denote the left hand side of the valence formula with respect to f and Γ respectively Γ'.

Proof. Fix $z \in \mathcal{H}$. We apply Lemma 2.4.3 with X being the $\overline{\Gamma}$-orbit of z, $G = \overline{\Gamma}$ and $H = \overline{\Gamma}'$. Clearly H has finite index in G. This yields

$$\sum_{\substack{w \in \Gamma' \backslash \mathcal{H} \\ w \in \Gamma.z}} \frac{n_\Gamma(w)}{n_{\Gamma'}(w)} = \sum_{\substack{w \in H \backslash \mathcal{H} \\ w \in X}} \frac{|\,\mathrm{stab}_{\overline{\Gamma}}(w)|}{|\,\mathrm{stab}_{\overline{\Gamma'}}(w)|} = \sum_{w \in H \backslash X} [\mathrm{stab}_{\overline{\Gamma}}(w) : \mathrm{stab}_{\overline{\Gamma'}}(w)] = \left[\overline{\Gamma} : \overline{\Gamma'}\right].$$

Recall that $d_\Gamma = [\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}]$, so $[\overline{\Gamma} : \overline{\Gamma'}] = d_{\Gamma'}/d_\Gamma$. Using that $n_\Gamma(w) = n_\Gamma(z)$ for all $w \in \Gamma.z$ we get

$$\sum_{\substack{w \in \Gamma' \backslash \mathcal{H} \\ w \in \Gamma.z}} \frac{1}{n_{\Gamma'}(w)} = \frac{1}{n_\Gamma(z)} \frac{d_{\Gamma'}}{d_\Gamma}.$$

Furthermore, we have $v_w(f) = v_z(f)$ for all $w \in \Gamma.z$ since f is weakly modular of level Γ, and hence

$$\sum_{w \in \Gamma' \backslash \mathcal{H}} \frac{v_w(f)}{n_{\Gamma'}(w)} = \sum_{z \in \Gamma \backslash \mathcal{H}} \left(v_z(f) \sum_{\substack{w \in \Gamma' \backslash \mathcal{H} \\ w \in \Gamma.z}} \frac{1}{n_{\Gamma'}(w)} \right) = \frac{d_{\Gamma'}}{d_\Gamma} \sum_{z \in \Gamma \backslash \mathcal{H}} \frac{v_z(f)}{n_\Gamma(z)}.$$

Similarily we can argue at the cusps: If $c \in C(\Gamma)$ and $d \in C(\Gamma')$ such that $[c] = [d]$ in $C(\Gamma)$ we see with $N = v_{c,\Gamma}(f)$, $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $[g.\infty] = c$ and $m = h_{\Gamma'}/h_\Gamma$ that

$$(f|_k g)(z) = \sum_{n=N}^{\infty} a_n(f) e^{2\pi i z n / h_\Gamma} = \sum_{n=N}^{\infty} a_n(f) e^{2\pi i z n m / h_{\Gamma'}} = \sum_{n=mN}^{\infty} a'_n(f) e^{2\pi i z n / h_{\Gamma'}}.$$

Therefore we have

$$v_{d,\Gamma'}(f) = \frac{h_{\Gamma'}(d)}{h_\Gamma(c)} v_{c,\Gamma}(f).$$

Now let $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $[g.\infty] = d$. Then

$$\begin{aligned}
[\mathrm{stab}_{\overline{\Gamma}}(d) : \mathrm{stab}_{\overline{\Gamma'}}(d)] &= \left[g \left(\mathrm{stab}_{g^{-1}\overline{\Gamma} g}(\infty) \right) g^{-1} : g \left(\mathrm{stab}_{g^{-1}\overline{\Gamma'} g}(\infty) \right) g^{-1} \right] \\
&= \left[\overline{(g^{-1}\Gamma g)_\infty} : \overline{(g^{-1}\Gamma' g)_\infty} \right] = \frac{h_{\Gamma'}(d)}{h_\Gamma(d)} = \frac{h_{\Gamma'}(d)}{h_\Gamma(c)}.
\end{aligned}$$

Fix $q \in P^1_\mathbb{Q}$ and let c be the Γ-orbit of q. Now we can use Lemma 2.4.3 again with $X = c$ and G, H as before:

$$\begin{aligned}
\sum_{\substack{d \in C(\Gamma') \\ [d]=[c] \text{ in } C(\Gamma)}} v_{d,\Gamma'}(f) = v_{c,\Gamma}(f) & \sum_{\substack{d \in C(\Gamma') \\ [d]=[c] \text{ in } C(\Gamma)}} \frac{h_{\Gamma'}(d)}{h_\Gamma(c)} \\
&= v_{c,\Gamma}(f) \sum_{d \in H \backslash X} [\mathrm{stab}_{\overline{\Gamma}}(d) : \mathrm{stab}_{\overline{\Gamma'}}(d)] = v_{c,\Gamma}(f) \frac{d_{\Gamma'}}{d_\Gamma}
\end{aligned}$$

Thus we have

$$\sum_{d \in C(\Gamma')} v_{d,\Gamma'}(f) = \sum_{c \in C(\Gamma)} \sum_{\substack{d \in C(\Gamma') \\ [d]=[c] \text{ in } C(\Gamma)}} v_{d,\Gamma'}(f) = \frac{d_{\Gamma'}}{d_\Gamma} \sum_{c \in C(\Gamma)} v_{c,\Gamma}(f).$$

Hence everything is shown. □

Lemma 2.4.6. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index, f a modular function of weight k and level Γ and $g \in \mathrm{SL}_2(\mathbb{Z})$. Then*

$$V_{g^{-1}\Gamma g}(f|_k g) = V_\Gamma(f).$$

Proof. We clearly have $v_z(f|_k g) = v_{gz}(f)$ for any $z \in \mathcal{H}$ and $n_{g^{-1}\Gamma g}(z) = n_\Gamma(gz)$ since $\mathrm{stab}_\Gamma(gz) = g(\mathrm{stab}_{g^{-1}\Gamma g}(z))g^{-1}$. Now note that z and z' represent the same element in $g^{-1}\Gamma g\backslash\mathcal{H}$ if and only if there is $\gamma \in \Gamma$ such that $g^{-1}\gamma g z = z'$, so if and only if gz and gz' represent the same element in $\Gamma\backslash\mathcal{H}$. Hence

$$\sum_{z \in (g^{-1}\Gamma g)\backslash\mathcal{H}} \frac{v_z(f|_k g)}{n_{g^{-1}\Gamma g}(z)} = \sum_{gz \in \Gamma\backslash\mathcal{H}} \frac{v_{gz}(f)}{n_\Gamma(gz)}.$$

This deals with the non-cusp terms in the valence formular. But similarily we can check that $v_c(f|_k g) = v_{gc}(f)$, so the cusp terms in $V_{g^{-1}\Gamma g}(f|_k g)$ and $V_\Gamma(f)$ are also equal. □

Lemma 2.4.7. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index and f_1, f_2 modular functions of weight k and level Γ. Then*

$$V_\Gamma(f_1 f_2) = V_\Gamma(f_1) + V_\Gamma(f_2).$$

Proof. Note that $v_z(f_1 f_2) = v_z(f_1) + v_z(f_2)$ for any $z \in \mathcal{H}$. But clearly the same is true for z being a cusp of Γ. Hence the claimed equality holds as $n_\Gamma(z)$ does not depend on the given function. □

We need one last lemma about normal subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

Lemma 2.4.8. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index. Then Γ has a finite index subgroup Γ' that is normal in $\mathrm{SL}_2(\mathbb{Z})$.*

Proof. Put

$$\Gamma' = \bigcap_{g \in \mathrm{SL}_2(\mathbb{Z})} g^{-1}\Gamma g.$$

Then Γ' is clearly a group and contained in Γ. Moreover, Γ' is normal since for $h \in \mathrm{SL}_2(\mathbb{Z})$

$$h^{-1}\Gamma' h = \bigcap_{g \in \mathrm{SL}_2(\mathbb{Z})} (gh)^{-1}\Gamma(gh) = \Gamma'.$$

It remains to show that Γ' has finite index in Γ. Let $g_1, \ldots, g_n$ be coset representatives for $\Gamma\backslash\mathrm{SL}_2(\mathbb{Z})$, so $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{i=1}^n \Gamma g_i$. Then for any $g \in \mathrm{SL}_2(\mathbb{Z})$ there is $\gamma_g \in \Gamma$ and a unique i_g such that $g = \gamma_g g_{i_g}$. Hence the infinite intersection defining Γ' is effectively finite in the sense that

$$\Gamma' = \bigcap_{g \in \mathrm{SL}_2(\mathbb{Z})} (\gamma_g g_{i_g})^{-1}\Gamma(\gamma_g g_{i_g}) = \bigcap_{i=1}^n g_i^{-1}\Gamma g_i.$$

Hence Γ' has finite index in Γ as we will show in Proposition 2.7.3. □

Now we can finally proof the valence formula.

Proof of Theorem 2.4.2. Let Γ' be any finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ which is normal in $\mathrm{SL}_2(\mathbb{Z})$ and contained in Γ. (Such a subgroup exists by Lemma 2.4.8.) Furthermore, put $d = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma']$ and let $g_1, \dots, g_d \in \mathrm{SL}_2(\mathbb{Z})$ be coset representatives for $\Gamma' \backslash \mathrm{SL}_2(\mathbb{Z})$. We define a function $F \colon \mathcal{H} \to \mathbb{C}$ by

$$F(z) = \prod_{i=1}^{d} (f|_k g_i)(z).$$

We claim that F is a modular function of weight dk and level $\mathrm{SL}_2(\mathbb{Z})$. The weight is clear. To see the level let $\tau \in \mathrm{SL}_2(\mathbb{Z})$. We will check that $g_1\tau, \dots, g_d\tau$ is a new set of coset representatives for $\Gamma' \backslash \mathrm{SL}_2(\mathbb{Z})$ and that F is independent of the choice of coset represenatives. The latter is clear since f is Γ'-invariant.

Fix $k \in \{1, \dots, d\}$. Since $\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i=1}^{d} \Gamma' g_i$ there is a unique $\gamma_k \in \Gamma'$ and i_k such that $g_k\tau = \gamma_k g_{i_k}$. We have to check that different k's correspond to different i_k's. Suppose that $i_k = i_l$ for $k, l \in \{1, \dots, d\}$. Then

$$\gamma_k^{-1} g_k = g_{i_k} \tau^{-1} = g_{i_l} \tau^{-1} = \gamma_l^{-1} g_l$$

and thus $g_k = \gamma_k \gamma_l^{-1} g_l \in \Gamma' g_l$, so $k = l$ as claimed. Hence $g_1\tau, \dots, g_d\tau$ is a new set of coset representatives as claimed and therefore F is indeed a modular function of weight dk and level 1. So the valence formula of level 1 gives us $V_{\mathrm{SL}_2(\mathbb{Z})}(F) = kd/12$.

Now note that each $f|_k g_i$ is a modular function of level $g^{-1}\Gamma' g = \Gamma'$ since Γ' is normal in $\mathrm{SL}_2(\mathbb{Z})$. Therefore we see using Lemma 2.4.5, Lemma 2.4.6 and Lemma 2.4.7, and again Γ' being normal in $\mathrm{SL}_2(\mathbb{Z})$ that

$$\begin{aligned} V_{\mathrm{SL}_2(\mathbb{Z})}(F) &= \frac{d_{\mathrm{SL}_2(\mathbb{Z})}}{d_{\Gamma'}} V_{\Gamma'}(F) = \frac{1}{d_{\Gamma'}} \sum_{i=1}^{d} V_{\Gamma'}(f|_k g_i) \\ &= \frac{1}{d_{\Gamma'}} \sum_{i=1}^{d} V_{g_i \Gamma' g_i^{-1}}(f) = \frac{1}{d_{\Gamma'}}\, d \cdot V_{\Gamma'}(f) = \frac{d}{d_{\Gamma'}} \frac{d_{\Gamma'}}{d_{\Gamma}} V_{\Gamma}(f), \end{aligned}$$

so

$$V_{\Gamma}(f) = \frac{d_\Gamma}{d} V_{\mathrm{SL}_2(\mathbb{Z})}(F) = \frac{d_\Gamma\, k}{12}$$

as claimed. □

Corollary 2.4.9. *For $k < 0$ and any $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index $M_k(\Gamma)$ is trivial.*

Proof. Clear since the left hand side of the valence formula must be non-negative. □

Corollary 2.4.10 ("The unreasonable effectiveness of modular forms in number theory")**.** *Let $k \in \mathbb{Z}$, $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index and $f, g \in M_k(\Gamma)$ such that their q-expansions agree up to degree $kd_\Gamma/12$, so $a_n(f) = a_n(g)$ for $n = 0, \dots, \left\lfloor \frac{k\, d_\Gamma}{12} \right\rfloor$. Then $f = g$.*

Proof. We have $v_{\infty,\Gamma}(f-g) \geq 1 + \left\lfloor \frac{k\,d_\Gamma}{12} \right\rfloor > \frac{k\,d_\Gamma}{12}$, which yields a contradiction to the valence formula unless $f - g = 0$. $\square$

Corollary 2.4.11. *For any $k \geq 0$ and any finite index subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ we have*

$$\dim\left(M_k(\Gamma)\right) \leq 1 + \left\lfloor \frac{k\,d_\Gamma}{12} \right\rfloor.$$

In particular, $M_k(\Gamma)$ is finite dimensional.

Proof. Let $m = \left\lfloor \frac{k\,d_\Gamma}{12} \right\rfloor$. Consider the linear map $M_k(\Gamma) \to \mathbb{C}^{m+1}$ mapping f to the coefficients up to q^m in its q-expansion. By Corollary 2.4.10 this map is injective, hence $\dim(M_k(\Gamma)) \leq m+1$. $\square$

Remark. (i) It can be shown that in the non trivial case, so for $k \geq 0$ and k even if Γ is even, then $\dim(M_k(\Gamma)) \geq (\frac{k}{12} - 1)d_\Gamma$.

(ii) In Diamond & Shurman there are precise formulae for the dimsion of $M_k(\Gamma)$.

2.5 Eisenstein series revisited

In this section we will construct modular forms of arbitrary weigkt and level, if the corresponding space is non-trivial. Therefore we will generalise the concept of Eisenstein series introduced in Section 1.4. Recall that $P_\infty = \pm\left(\begin{smallmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right)$ and define $P_\infty^+ = \left(\begin{smallmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right)$. For $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ we define $\Gamma_\infty^+ = \Gamma \cap P_\infty^+$.

Lemma 2.5.1. *(a) Let $g, g' \in \mathrm{SL}_2(\mathbb{Z})$, $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $g' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$. Then $c = c'$ and $d = d'$ if and only if there is an $g_\infty \in P_\infty^+$ such that $g' = g_\infty g$.*

(b) For $(c,d) \in \mathbb{Z}^2$ there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with bottom row (c,d) if and only if $\gcd(c,d) = 1$.

Proof. For (a) let $c = c'$ and $d = d'$. Then $g'g^{-1} = \left(\begin{smallmatrix} 1 & ab'-a'b \\ 0 & 1 \end{smallmatrix}\right) \in P_\infty^+$. Conversly let $g_\infty = \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$. Then $g_\infty g = \left(\begin{smallmatrix} a+cm & b+dm \\ c & d \end{smallmatrix}\right)$ implies $(c,d) = (c',d')$ if $g' = g_\infty g$. Part (b) is obvious. $\square$

Corollary 2.5.2. *The map $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto (c,d)$ defines a bijection between*

$$P_\infty^+ \backslash \mathrm{SL}_2(\mathbb{Z}) \to \{(c,d) \in \mathbb{Z}^2 \colon \gcd(c,d) = 1\}.$$

Proof. Part (a) of the previous lemma implies that the given map is a well-defined injecton $P_\infty^+ \backslash \mathrm{SL}_2(\mathbb{Z}) \to \mathbb{Z}^2$, and part (b) says that its image are all elements $(c,d) \in \mathbb{Z}^2$ with c and d being coprime. $\square$

We will now motivate the definition of a generalised Eisenstein series using this bijection. Firstly note that $1|_k\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = (cz+d)^{-k}$, so 1 is P_∞^+-invariant. Hence the unnormalised level 1 Eistenstein series $G_k(z)$ can be written as

$$\begin{aligned}
\sum_{(c,d)\in\mathbb{Z}^2\setminus\{0\}} \frac{1}{(cz+d)^k} &= \sum_{r=1}^{\infty}\left(\sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=r}} \frac{1}{(cz+d)^k}\right) \\
&= \sum_{r=1}^{\infty}\left(\frac{1}{r^k}\sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1}} \frac{1}{(cz+d)^k}\right) \\
&= \left(\sum_{r=1}^{\infty}\frac{1}{r^k}\right)\left(\sum_{[\gamma]\in P_\infty^+\setminus \mathrm{SL}_2(\mathbb{Z})} (1|_k\gamma)(z)\right) \\
&= \zeta(k) \sum_{[\gamma]\in P_\infty^+\setminus \mathrm{SL}_2(\mathbb{Z})} (1|_k\gamma)(z).
\end{aligned}$$

Proposition 2.5.3. *For any subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index and any $k \geq 3$ we define*

$$G_{k,\Gamma,\infty} = \sum_{\gamma\in\Gamma_\infty^+\setminus\Gamma} 1|_k\gamma.$$

Then $G_{k,\Gamma,\infty}$ is a weakly modular function of weight k and level Γ.

Proof. It can be shown that the sum defining $G_{k,\Gamma,\infty}$ converges absolutely and uniformly on compact subsets of $\mathcal{H}$. Thus $G_{k,\Gamma,\infty}$ is well-defined and holomorphic on $\mathcal{H}$. Moreover, $G_{k,\Gamma,\infty}$ is also clearly Γ-invariant of weight k since for any $g \in \Gamma$

$$G_{k,\Gamma,\infty}|_k g = \sum_{\gamma\in\Gamma_\infty^+\setminus\Gamma} 1|_k(\gamma g) = \sum_{\gamma\in\Gamma_\infty^+\setminus\Gamma g} 1|_k\gamma = G_{k,\Gamma,\infty}.$$

Hence $G_{k,\Gamma,\infty}$ is a weakly modular function of weight k and level Γ. □

Proposition 2.5.4. *If either k is even, or if k is odd and Γ is regular at ∞ then $G_{k,\Gamma,\infty}$ is a modular form of weight k and level Γ not vanishing at ∞, but at all other cusps. Moreover, if k is odd and Γ is irregular at ∞ then $G_{k,\Gamma,\infty} = 0$.*

Proof. First suppose that k is odd and Γ is odd and irregular at ∞, so $g = -\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$ for some $h \in \mathbb{Z}$. Then we see for all $\gamma \in \Gamma$ that

$$1|_k\gamma + 1|_k(g\gamma) = (cz+d)^k + (-1)^k(cz+d)^k = 0.$$

Hence we have

$$G_{k,\Gamma,\infty} = \sum_{\gamma\in\Gamma_\infty^+\setminus\Gamma} 1|_k\gamma = \sum_{\alpha\in\Gamma_\infty\setminus\Gamma}\ \sum_{\beta\in\Gamma_\infty^+\setminus\Gamma_\infty} 1|_k(\beta\alpha) = \sum_{\alpha\in\Gamma_\infty\setminus\Gamma} (1|_k\alpha + 1|_k(g\alpha)) = 0.$$

Now let k be even or let k be odd and Γ be regular at ∞. Consider $G_{k,\Gamma,\infty}(z)$ as $\mathrm{Im}(z) \to \infty$ and note that we have already shown in the level 1 case that

$$\lim_{\mathrm{Im}(z)\to\infty} \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ m\neq 0}} \frac{1}{(mz+n)^k} = \lim_{\mathrm{Im}(z)\to\infty} (G_k(z) - 2\zeta(k)) = 0.$$

Therefore we only need to consider terms that come from some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_\infty^+\backslash\Gamma$ with $c = 0$, so elements in $\Gamma_\infty^+\backslash\Gamma_\infty$. If Γ is even then $\Gamma_\infty^+\backslash\Gamma_\infty = \{\pm 1\}$ and thus

$$\lim_{\mathrm{Im}(z)\to\infty} G_{k,\Gamma,\infty}(z) = \lim_{\mathrm{Im}(z)\to\infty} \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma_\infty} 1|_k\gamma = 1^{-k} + (-1)^{-k} = 2$$

since k is even by assumption in this case. Now consider Γ to be regular at ∞. Then $\Gamma_\infty^+ = \Gamma_\infty$, so their quotient is trivial and thus $G_{k,\Gamma,\infty}(z) \to 1$ as $\mathrm{Im}(z) \to \infty$. It remains to consider Γ being irregular at ∞. For k odd the sum cancels as remarked at the beginning, so let k be even. Recall that $\Gamma_\infty = \{(-1)^t\left(\begin{smallmatrix} 1 & th \\ 0 & 1 \end{smallmatrix}\right) : t \in \mathbb{Z}\}$ for some $h \in \mathbb{Z}$. Hence $\Gamma_\infty^+\backslash\Gamma_\infty = \{1, -\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)\}$ and thus $G_{k,\Gamma,\infty}(z) \to 1^{-k} + (-1)^{-k} = 2$ as $\mathrm{Im}(z) \to \infty$. Combining these results we get

$$\lim_{\mathrm{Im}(z)\to\infty} G_{k,\Gamma,\infty}(z) = \begin{cases} 2, & \text{if } k \text{ is even and } \Gamma \text{ is even} \\ 1, & \text{if } \Gamma \text{ is regular at } \infty \\ 2, & \text{if } k \text{ is even and } \Gamma \text{ is irregular at } \infty \end{cases}.$$

Finally consider a cusp c of Γ different from ∞. Choose $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $[g.\infty] = c$. Then

$$G_{k,\Gamma,\infty}|_k g = \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma} 1|_k(\gamma g) = \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma g} 1|_k\gamma.$$

As before we only need to consider terms that come from $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_\infty^+\backslash\Gamma g$ with $c = 0$. We claim that no such element exists. To see this suppose there is $\gamma \in \Gamma$ such that $\gamma g \in P_\infty$. Then $\gamma g.\infty = \infty$ and thus $[g.\infty] = [\infty]$ in $C(\Gamma)$ which is a contradiction. Hence none of the γ's in the sum, $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, have $c = 0$, so the sum goes to zero as $\mathrm{Im}(z) \to \infty$. Therefore

$$G_{k,\Gamma,\infty}(c) = (G_{k,\Gamma,\infty}|_k g)(\infty) = 0.$$

In particular, we have seen that $G_{k,\Gamma,\infty}|_k g$ is bounded as $\mathrm{Im}(z) \to \infty$ for all $g \in \mathrm{SL}_2(\mathbb{Z})$, so $G_{k,\Gamma,\infty}$ is indeed a modular form. □

Note that we indeed have constructed a modular form that does not vanish at ∞ for all pairs (k, Γ) where this isn't trivially impossible.

Corollary 2.5.5. *For any finite index subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ and any cusp c of Γ such that Γ is regular at c if k and Γ are odd, we define*

$$G_{k,\Gamma,c} = G_{k,g^{-1}\Gamma g,\infty} \;|_k\; g^{-1}$$

where $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $[g.\infty] = c$. Then $G_{k,\Gamma,c}$ is a modular form of weight k and level Γ vanishing not at c but at all other cusps of Γ.

Proof. Clearly $G_{k,\Gamma,c}$ is holomorphic on $\mathcal{H}$. For $\gamma \in \Gamma$ we see

$$G_{k,\Gamma,c}|_k\gamma = \big(G_{k,g^{-1}\Gamma g,\infty}|_k(g^{-1}\gamma g)\big)\,|_k g^{-1} = G_{k,g^{-1}\Gamma g,\infty}|_k g^{-1} = G_{k,\Gamma,c}.$$

So $G_{k,\Gamma,c}$ is weakly modular of weight k and level Γ. Now let d be any cusp of Γ and $h \in \mathrm{SL}_2(\mathbb{Z})$ such that $[h.\infty] = d$. Then we have up to sign

$$G_{k,\Gamma,c}(d) = \big(G_{k,g^{-1}\Gamma g,\infty}\ |_k\ (g^{-1}h)\big)\,(\infty).$$

Hence $G_{k,\Gamma,c}$ is holomorphic at all cusps as $G_{k,g^{-1}\Gamma g,\infty}$ is. Further, if $d = c$ we can choose $h = g$ and thus $G_{k,\Gamma,c}$ is non-vanishing at c as $G_{k,g^{-1}\Gamma g,\infty}$ is at ∞. Conversly, if $d \neq c$ then $[g^{-1}h.\infty] \neq [\infty]$ and thus $G_{k,\Gamma,c}(d) = G_{k,g^{-1}\Gamma g,\infty}([g^{-1}h.\infty]) = 0$. Therefore $G_{k,\Gamma,c}$ is a modular form of weight k and level Γ vanishing not at c but at all other cusps. □

Note that $G_{k,\Gamma,c}$ is well-defined if k is even, and in this case independent of the choice of c, but if k is odd $G_{k,\Gamma,c}$ is only well-defined up to sign.

We define $\mathcal{E}_k(\Gamma)$ as the subspace of $M_k(\Gamma)$ spanned by the corresponding $G_{k,\Gamma,c}$'s. Note that

$$\dim(\mathcal{E}_k(\Gamma)) = \begin{cases} |C(\Gamma)|, & \text{if } k \text{ is even} \\ |C_{\mathrm{reg}}(\Gamma)|, & \text{if } k \text{ is odd and } \Gamma \text{ is odd} \end{cases},$$

where we define $C_{\mathrm{reg}}(\Gamma)$ as the set of cusps of Γ at which Γ is regular. Moreover, define $B_k(\Gamma)$ by

$$B_k(\Gamma) = \begin{cases} \{f\colon C(\Gamma) \to \mathbb{C}\}, & \text{if } k \text{ is even} \\ \{f\colon C_{\mathrm{reg}}(\Gamma) \to \mathbb{C}\}, & \text{if } k \text{ is odd and } \Gamma \text{ is odd} \end{cases}.$$

Corollary 2.5.6. *Let $k \geq 3$ and $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index. For any fixed choice of $g_1, \ldots, g_r$ sending ∞ to the cusps of Γ the map*

$$\partial\colon M_k(\Gamma) \to B_k(\Gamma),\ f \mapsto \Big(c \mapsto f(c)\Big)$$

sending f to its values at the (regular) cusps is surjective.

Proof. This is clear since the $G_{k,\Gamma,c}$'s map to a basis of $B_k(\Gamma)$. □

The map ∂ is called the boundary map and has by definition kernel $S_k(\Gamma)$. (Recall that every modular form vanishes at all irregular cusps by definition.) Moreover, its image $B_k(\Gamma)$ is clearly isomorphic to the subspace $\mathcal{E}_k(\Gamma)$ of $M_k(\Gamma)$ and therefore we get

$$M_k = S_k(\Gamma) \oplus \mathcal{E}_k(\Gamma).$$

Remark. If $k = 1$ or $k = 2$ one can check that the image of M_k has codimension 1 in B_k but it is hard to describe the image nicely.

Example 2.5.7. Let p be prime and $\Gamma = \Gamma_0(p)$. Then $C(\Gamma) = \{0, \infty\}$ and Γ is even. So the case k odd is trivial. For $k \geq 4$ even there are two Eistenstein series $G_{k,\Gamma,\infty}$ and $G_{k,\Gamma,0}$. For the first one we have by definition of $\Gamma_0(p)$ that

$$G_{k,\Gamma,\infty} = \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} 1|_k\gamma = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p|c}} \frac{1}{(cz+d)^k}.$$

Now consider the second one. We have $g.\infty = 0$ for $g = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and

$$g^{-1}\Gamma g = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : p \text{ didivdes } b \right\} =: \Gamma^0(p).$$

Put $\Gamma' = \Gamma^0(p)$. Then

$$G_{k,\Gamma,0} = (G_{k,\Gamma',\infty})\,|_k(g^{-1}) = \sum_{\gamma \in (\Gamma')_\infty^+ \backslash \Gamma'} 1|_k(\gamma g^{-1}) = \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in (\Gamma')_\infty^+ \backslash \Gamma'} (-dz+c)^{-k}.$$

Now note that $\gamma \in (\Gamma')_\infty^+ \backslash \Gamma'$ if and only if c, d are coprime and p does not divide d. Hence we get

$$G_{k,\Gamma,0} = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p\nmid d}} \frac{1}{(-dz+c)^k} = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p\nmid c}} \frac{1}{(cz+d)^k}.$$

Thus we have $G_{k,\Gamma,\infty} + G_{k,\Gamma,0} = G_{k,\mathrm{SL}_2(\mathbb{Z}),\infty}$. Recall that $G_{k,\mathrm{SL}_2(\mathbb{Z}),\infty}(\infty) = 2$ as k is even and $\mathrm{SL}_2(\mathbb{Z})$ is even. Therefore $G_{k,\mathrm{SL}_2(\mathbb{Z}),\infty} = 2E_k$ where E_k denotes the normalised Eisenstein series of level 1. Finally consider

$$2E_k(pz) = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1}} \frac{1}{(c(pz)+d)^k}.$$

Note that if $(c,d) \in \mathbb{Z}^2$ with $\gcd(c,d) = 1$, then $\gcd(pc,d) = 1$ unless p divides d. So

$$2E_k(pz) = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p|c}} \frac{1}{(cz+d)^k} + \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p|d}} \frac{1}{(pcz+d)^k}.$$

We can check that

$$\{(pc,d)\colon \gcd(c,d)=1, p|d\} = \{(pc,pd)\colon \gcd(c,d)=1, p\nmid c\},$$

which gives us

$$2E_k(pz) = G_{k,\Gamma,\infty} + \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p\nmid c}} \frac{1}{(pcz+pd)^k} = G_{k,\Gamma,\infty} + p^{-k}G_{k,\Gamma,0}.$$

Hence $\mathcal{E}_k(\Gamma)$ is spanned by $E_k(z)$ and $E_k(pz)$. Note that we have also shown that $E_k(pz)$ is 1 at the cusp ∞ and p^{-k} at the cusp 0.

2.6 The Petersson product

Lemma 2.6.1. *Let $U \subseteq \mathcal{H}$ be closed and bounded, $f\colon U \to \mathbb{C}$ a continuous function and $g \in \mathrm{PSL}_2(\mathbb{R})$. Then*

$$\int_U f(x+iy)\frac{d(x,y)}{y^2} = \int_{g^{-1}U} f(g.(x+iy))\frac{d(x,y)}{y^2}.$$

Proof. Consider $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ as a map between open subsets of $\mathbb{R}^2$ and let J_g denote the Jacobian matrix of this map. Then the Cauchy-Riemann equations yield

$$|J_g| = \left|\begin{pmatrix} \frac{\partial g_1}{\partial x} & \frac{\partial g_1}{\partial y} \\ \frac{\partial g_2}{\partial x} & \frac{\partial g_2}{\partial y} \end{pmatrix}\right| = |g'(z)|^2.$$

Recall that $\mathrm{Im}(g.z) = \frac{\mathrm{Im}(z)}{|j(g,z)|^2}$. Hence

$$|g'(z)|^2 = \left|\frac{a(cz+d) - c(az+b)}{(cz+d)^2}\right|^2 = \frac{1}{|cz+d|^4} = \left(\frac{\mathrm{Im}(g.z)}{\mathrm{Im}(z)}\right)^2.$$

Therefore we have

$$\begin{aligned} \int_U f(x+iy)\frac{d(x,y)}{y^2} &= \int_{g^{-1}U} f(g.(x+iy))\ |J_g|\ \frac{d(x,y)}{\mathrm{Im}(g(x+iy))^2} \\ &= \int_{g^{-1}U} f(g.(x+iy))\frac{d(x,y)}{y^2} \end{aligned}$$

as claimed. □

In fancy language the previous lemma states that the differential 2-form $y^{-2}d(x,y)$ is $\mathrm{PSL}_2(\mathbb{R})$-invariant. In the following we will write $dA(z)$ for $y^{-2}d(x,y)$. Lemma 2.6.1 can thus be read as

$$\int_U f(z)dA(z) = \int_{g^{-1}U} f(g.z)dA(z).$$

In particular, we have shown that $dA(g.z) = dA(z)$ for all $g \in \mathrm{PSL}_2(\mathbb{Z})$. Let now $g_1, \dots, g_{d_\Gamma}$ be coset representatives for $\overline{\Gamma}\backslash \mathrm{PSL}_2(\mathbb{Z})$ and let D be the fundamental domain as defined in Theorem 1.2.2. We define the fundamental domain of a finite index subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ by $D_\Gamma = \bigcup_{i=1}^{d_\Gamma} g_i D$. Clearly D_Γ has similiar properties in relation to Γ as D has in relation to $\mathrm{SL}_2(\mathbb{Z})$. In particular, every Γ-orbit in $\mathcal{H}$ has a representative in D_Γ and if this representative lies in the interior of D_Γ then it is unique.

Consider a function $F\colon \mathcal{H} \to \mathbb{C}$ being Γ-invariant of weight 0 for some $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index. Lemma 2.6.1 implies that if the integral

$$\int_{D_\Gamma} F(z)dA(z) \tag{2.6.1}$$

converges for one set of coset representatives $g_1, \dots, g_{d_\Gamma}$ of $\overline{\Gamma}\backslash \mathrm{PSL}_2(\mathbb{Z})$, then it converges for any such choice and the value of the integral is independent of this choice. Therefore we have defined a good notion of integration for functions on $\Gamma\backslash\mathcal{H}$.

Corollary 2.6.2. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a finite index subgroup, $g_1, \ldots, g_{d_\Gamma}$ be coset representatives for $\mathrm{PSL}_2(\mathbb{Z})/\overline{\Gamma}$ and let $F\colon \mathcal{H} \to \mathbb{C}$ be a continuous function such that*

$$(F|_0\gamma)(z) = O\left(|\operatorname{Im}(z)|^{-1-\varepsilon}\right) \quad \text{for all } \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

Then the integral in (2.6.1) converges. In addition the integral is independent of the choice of the g_i's if F is Γ-invariant of weight 0.

Proof. It can be checked that the condition on growth of F yields the convergence of the integral. Therefore the statement is clear by the previous observations. □

Proposition 2.6.3. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index, $k \geq 1$ and $f, g \in M_k(\Gamma)$. Define $F\colon \mathcal{H} \to \mathbb{C}$ by*

$$F(z) = f(z)\overline{g(z)}\operatorname{Im}(z)^k.$$

Then F is Γ-invariant of weight 0, and if at least one of f and g vanishes at each cusp, then F tends exponentially to 0 at each cusp and hence the integral in (2.6.1) with the given functon F converges.

Proof. F as defined is Γ-invariant of weight 0 since f and g are Γ-invariant of weight k and $\operatorname{Im}(g.z) = \operatorname{Im}(z)|j(g,z)|^{-2}$, so for any $\gamma \in \Gamma$

$$(F|_0\gamma)(z) = \left(j(\gamma,z)^k f(z)\right)\left(\overline{j(\gamma,z)^k g(z)}\right)\left(\frac{\operatorname{Im}(z)}{j(\gamma,z)\overline{j(\gamma,z)}}\right)^k = F(z).$$

Moreover, the decay at the cusps can easily be shown by considering the q-expansion of F at the corresponding cusps. □

Definition 2.6.4. Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index, $k \geq 1$ and $f, g \in M_k(\Gamma)$, at least one vanishing at every cusp of Γ. Then we define the **Petersson product** as

$$\langle f, g\rangle_\Gamma = \int_{D_\Gamma} f(z)\overline{g(z)}\operatorname{Im}(z)^k dA(z).$$

Note that the Petersson product is well-defined by the previous proposition.

Proposition 2.6.5. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index, $k \geq 3$ and c a cusp of Γ. In addition, let Γ be regular at c if k is odd. Then $\langle f, G_{k,\Gamma,c}\rangle = 0$ for all $f \in S_k(\Gamma)$.*

Proof. It can easily be checked that $\langle f, g\rangle_\Gamma = \langle f|_k\gamma, g|_k\gamma\rangle_{\gamma^{-1}\Gamma\gamma}$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. So we can assume that $c = \infty$ without loss of generality. Let $f \in S_k(\Gamma)$. By definition we have

$$\langle f, G_{k,\Gamma,\infty}\rangle_\Gamma = \int_{D_\Gamma} f(z)\overline{\left(\sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma}(1|_k\gamma)(z)\right)}\operatorname{Im}(z)^k dA(z).$$

Now we interchange integral and sum and afterwards apply Lemma 2.6.1:

$$\begin{aligned}\langle f, G_{k,\Gamma,\infty}\rangle_\Gamma &= \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma}\int_{D_\Gamma} f(z)\ \overline{(1|_k\gamma)(z)}\ \operatorname{Im}(z)^k\ dA(z)\\ &= \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma}\int_{\gamma D_\Gamma} f(\gamma^{-1}.z)\ \overline{(1|_k\gamma)(\gamma^{-1}.z)}\ \operatorname{Im}(\gamma^{-1}.z)^k\ dA(z)\\ &= \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma}\int_{\gamma D_\Gamma} j(\gamma^{-1},z)^k f(z)\ \overline{j(\gamma^{-1},z)^k\,1(z)}\ \frac{\operatorname{Im}(z)^k}{|j(\gamma^{-1},z)|^{2k}}\ dA(z)\\ &= \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma}\int_{\gamma D_\Gamma} f(z)\ \operatorname{Im}(z)^k\ dA(z)\\ &= \big|\Gamma\cap\{\pm 1\}\big|\cdot\int_{\Gamma_\infty^+\backslash\mathcal{H}} f(z)\ \operatorname{Im}(z)^k\ dA(z)\end{aligned}$$

Note that the last expression is well-defined since the integrand is Γ_∞^+-invariant. A fundamental domain for $\Gamma_\infty^+ = \left(\begin{smallmatrix}1 & h\mathbb{Z}\\ 0 & 1\end{smallmatrix}\right)$ in $\mathcal{H}$ is given by $\{z\in\mathcal{H}\colon 0\le \operatorname{Re}(z)\le h\}$. Note that $h = h_\Gamma(\infty)$ if Γ is even or regular at ∞ and $h = 2h_\Gamma(\infty)$ if Γ is irregular at ∞. However,

$$\int_{\Gamma_\infty^+\backslash\mathcal{H}} f(z)\ \operatorname{Im}(z)^k\ dA(z) = \int_{\substack{0<y<\infty\\ 0\le x\le h}} f(x+iy)\ y^{k-2}\ d(x,y).$$

We will now use the q-expansion of f and then again change the order of summation and integration. Note that $a_0(f)=0$ and $a_n(f) = O(n^{k/2})$ since f is a cusp form. Thus

$$\begin{aligned}\int_{\substack{0<y<\infty\\ 0\le x\le h}} f(x+iy)\ y^{k-2}d(x,y) &= \int_{\substack{0<y<\infty\\ 0\le x\le h}}\left(\sum_{n=1}^\infty a_n(f)e^{2\pi i n(x+iy)/h_\Gamma(\infty)}\right)\ y^{k-2}d(x,y)\\ &= \sum_{n=1}^\infty a_n(f)\int_0^h e^{2\pi i n x/h_\Gamma(\infty)}dx\int_0^\infty e^{-2\pi y n/h_\Gamma(\infty)}y^{k-2}dy.\end{aligned}$$

Finally we see for the first integral and $h = h_\Gamma(\infty)$ or $h = 2h_\Gamma(\infty)$ that for any $n\ge 1$

$$\int_0^h e^{2\pi i n x/h_\Gamma(\infty)}dx = \frac{h_\Gamma(\infty)}{2\pi i n}\left(e^{2\pi i n h/h_\Gamma(\infty)} - 1\right) = 0.$$

Therefore the product above is 0 and so $\langle f, G_{k,\Gamma,\infty}\rangle_\Gamma = 0$ as claimed. □

Remark. If c and d are distinct cusps of Γ then $\langle G_{k,\Gamma,c}, G_{k,\Gamma,d}\rangle$ is well-defined, but it is not generally 0. Moreover, it can be shown that for $k\ge 3$, $\mathcal{E}_k(\Gamma)$, the subspace of $M_k(\Gamma)$ spanned by the $G_{k,\Gamma,c}$'s, is exactly given by the set

$$\{f\in M_k(\Gamma)\colon \langle f,g\rangle = 0 \text{ for all } g\in S_k(\Gamma)\}.$$

In an abuse of notation we say $\mathcal{E}_k(\Gamma)$ is "the orthogonal complement of $S_k(\Gamma)$", which is not correct since $\langle\cdot,\cdot\rangle$ is not well-defined on all elements of $M_k(\Gamma)$. However, $\langle\cdot,\cdot\rangle$ certainly defines a positive definite inner product on $S_k(\Gamma)$. Finally note that we can take the above set as the definition of $\mathcal{E}_k(\Gamma)$ for $k = 1,2$.

2.7 Hecke operators

In this section we will try to generalise the concept of Hecke operators. Therefore we have to start with some pure algebra.

Definition 2.7.1. Let Γ_1, Γ_2 be subgroups of a group G. We say Γ_1 and Γ_2 are **commensurable** if the intersection $\Gamma_1 \cap \Gamma_2$ has finite index in both Γ_1 and Γ_2.

Proposition 2.7.2. *Being commensurable defines an equivalence relation on the set of subgroups of a group G.*

Proof. The relation is clearly reflexive and symmetric. To show transitivity let Γ_1, Γ_2 and Γ_3 be subgroups of G and suppose that Γ_1 and Γ_2 are commensurable, and that Γ_2 and Γ_3 are commensurable. Note that $[\Gamma_1 \cap \Gamma_2 : \Gamma_1 \cap \Gamma_2 \cap \Gamma_3] \leq [\Gamma_2 : \Gamma_2 \cap \Gamma_3] < \infty$. Hence

$$[\Gamma_1 : \Gamma_1 \cap \Gamma_3] \leq [\Gamma_1 : \Gamma_1 \cap \Gamma_2 \cap \Gamma_3] = [\Gamma_1 : \Gamma_1 \cap \Gamma_2] \cdot [\Gamma_1 \cap \Gamma_2 : \Gamma_1 \cap \Gamma_2 \cap \Gamma_3] < \infty.$$

As this argument is symmetric in Γ_1 and Γ_3 we are done. □

Recall that $\mathrm{GL}_2^+(\mathbb{Q})$ is the set of invertible 2×2 matrices over $\mathbb{Q}$ with positive determinant.

Proposition 2.7.3. *Let $g \in \mathrm{GL}_2^+(\mathbb{Q})$. Then for any $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index the groups Γ and $g^{-1}\Gamma g$ are commensurable.*

Proof. First let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Choose $N \in \mathbb{N}$ such that $h := Ng$ has integer entries, and pick $M \in \mathbb{N}$ such that $f := Mh^{-1}$ has integer entries, too. Then

$$g^{-1}\Gamma g = (Nh^{-1})\Gamma\left(\frac{1}{N}h\right) = \frac{1}{M}f\Gamma h.$$

Note that $f\gamma h = fh$ modulo M for $\gamma \in \Gamma(M)$. But $fh = Mh^{-1}h = M\,\mathrm{id}$, so $fh = 0$ modulo M. Hence we have $f\gamma h = 0$ modulo M, and thus M divides all entries of $f\gamma h$, so $1/M \cdot f\gamma h$ has integer entries, and therefore we see

$$g^{-1}\Gamma(M)g = \frac{1}{M}f\Gamma(M)h \subseteq \mathrm{SL}_2(\mathbb{Z}) = \Gamma$$

since the determinant of elements in $g^{-1}\Gamma g$ is clearly 1. Hence we have

$$\left[\Gamma : \Gamma \cap (g^{-1}\Gamma g)\right] \leq \left[\Gamma : \Gamma \cap (g^{-1}\Gamma(M)g)\right] = \left[\Gamma : g^{-1}\Gamma(M)g\right] < \infty.$$

So $\mathrm{SL}_2(\mathbb{Z})$ and $g^{-1}\,\mathrm{SL}_2(\mathbb{Z})g$ are commensurable.

Let now Γ be an arbitrary finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, then Γ and $\mathrm{SL}_2(\mathbb{Z})$ are commensurable, $\mathrm{SL}_2(\mathbb{Z})$ and $g^{-1}\,\mathrm{SL}_2(\mathbb{Z})g$ are commensurable as shown before, and $g^{-1}\,\mathrm{SL}_2(\mathbb{Z})g$ and $g^{-1}\Gamma g$ are commensurable as $\mathrm{SL}_2(\mathbb{Z})$ and Γ are. So Γ and $g^{-1}\Gamma g$ are commensurable by transitivity of the relation. □

Exercise. Let $g \in \mathrm{GL}_2^+(\mathbb{R})$ such that $g^{-1}\,\mathrm{SL}_2(\mathbb{Z})g$ is commensurable with $\mathrm{SL}_2(\mathbb{Z})$. Does this force g to be in $\mathrm{GL}_2^+(\mathbb{Q})$?

Proposition 2.7.4. *Let $\Gamma_1, \Gamma_2 \le \mathrm{SL}_2(\mathbb{Z})$ be of finite index, $g \in \mathrm{GL}_2^+(\mathbb{Q})$ and let $\Gamma_1 g \Gamma_2$ denote the double coset $\{xgy \colon x \in \Gamma_1, y \in \Gamma_2\}$. Then there are finite sets $\{\alpha_1, \dots, \alpha_r\}$ and $\{\beta_1, \dots, \beta_s\}$ such that*

$$\Gamma_1 g \Gamma_2 = \bigsqcup_{i=1}^{r} \Gamma_1 \alpha_i = \bigsqcup_{i=1}^{s} \beta_i \Gamma_2.$$

Proof. First note that Γ_1 and Γ_2 are commensurable since they are of finite index in $\mathrm{SL}_2(\mathbb{Z})$, and that Γ_1 and $g^{-1}\Gamma_1 g$ are commensurable by Proposition 2.7.3. Hence the quotient $(\Gamma_2 \cap (g^{-1}\Gamma_1 g)) \backslash \Gamma_2$ is finite. Let $\tau_1, \dots, \tau_r \in \Gamma_2$ be representatives for this quotient, so

$$\Gamma_2 = \bigsqcup_{i=1}^{r} \left(\Gamma_2 \cap (g^{-1}\Gamma_1 g)\right) \tau_i.$$

Then $g\Gamma_2 = \bigsqcup_{i=1}^{r} \left((g\Gamma_2) \cap (\Gamma_1 g)\right) \tau_i$. Now let $\alpha_i = g\tau_i$. Then

$$\Gamma_1 g \Gamma_2 = \bigcup_{i=1}^{r} \left((\Gamma_1 g \Gamma_2) \cap (\Gamma_1 g)\right) \tau_i = \bigcup_{i=1}^{r} (\Gamma_1 g)\tau_i = \bigcup_{i=1}^{r} \Gamma_1 \alpha_i.$$

We claim that this union is disjoint, so $\Gamma_1\alpha_i \cap \Gamma_1\alpha_j = \emptyset$ for all $i \ne j$. To prove this suppose $\Gamma_1\alpha_i \cap \Gamma_1\alpha_j \ne \emptyset$ for some $i \ne j$. Then $g\tau_i \in \Gamma_1 g \tau_j$, so $\tau_i \in (g^{-1}\Gamma_1 g)\tau_j$. But we also have $\tau_l \in \Gamma_2$ for all l, so $\tau_i \in \Gamma_2 \tau_j$ and thus $\tau_i \in (\Gamma_2 \cap g^{-1}\Gamma_1 g)\tau_j$ which contradicts the choice of the τ_l's. So the above union is disjoint as claimed.

Similarly we can construct β_i's using coset representatives for $\Gamma_1 / (\Gamma_1 \cap (g\Gamma_2 g^{-1}))$. Therefore everything is shown. ☐

Note that the action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathcal{H}$ extends naturally to $\mathrm{GL}_2^+(\mathbb{R})$. Using this we can extend the weight k action of $\mathrm{SL}_2(\mathbb{R})$ on functions $f \colon \mathcal{H} \to \mathbb{C}$ to $\mathrm{GL}_2^+(\mathbb{R})$ as well.

Definition 2.7.5. (a) Let $k \in \mathbb{Z}$. For a function $f \colon \mathcal{H} \to \mathbb{C}$ and $g \in \mathrm{GL}_2^+(\mathbb{R})$ we define

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

(b) Let $\Gamma_1, \Gamma_2 \le \mathrm{SL}_2(\mathbb{Z})$ of finite index, $g \in \mathrm{GL}_2^+(\mathbb{Q})$ and $\alpha_1, \dots, \alpha_r$ as in Proposition 2.7.4, so $\Gamma_1 g \Gamma_2 = \bigsqcup_{i=1}^{r} \Gamma_1 \alpha_i$. For f weakly modular of weight k and level Γ_1 we define

$$f|_k [\Gamma_1 g \Gamma_2] = \sum_{i=1}^{r} f|_k \alpha_i.$$

We will later see that the fudge factor $\det(g)^{k-1}$ in part (i) of the definition corresponds to the factor n^{k-1} in the definition of T_n in chapter 1.

Proposition 2.7.6. *In the situation of Definition 2.7.5 (b) $f|_k[\Gamma_1 g \Gamma_2]$ is independent of the choice of the α_i's and weakly modular of weight k and level Γ_2.*

Proof. If $\alpha'_1, \dots, \alpha'_s$ is another set of coset representatives then we see that $s = r$. So we can reorder such that $\alpha_i = \gamma_i \alpha'_i$ for some $\gamma_i \in \Gamma_1$. Hence $f|_k\alpha_i = f|_k\alpha'_i$.

In particular, if $\alpha_1, \dots, \alpha_r$ is one such choice then so is $\alpha_1\gamma, \dots, \alpha_r\gamma$ for some $\gamma \in \Gamma_2$. Hence the sum $\sum_{i=1}^r f|_k\alpha_i$ is independent of the choice of the α_i's and is Γ_2-invariant. □

Note that acting on the right of $f|_k[\Gamma_1 g \Gamma_2]$ by Γ_2 is effectively permuting summands.

Proposition 2.7.7. *If f is a modular function, a modular form or a cusp form of level Γ_1 then so is $f|_k[\Gamma_1 g \Gamma_2]$ of level Γ_2.*

Proof. We already know that $f|_k[\Gamma_1 g \Gamma_2]$ is Γ_2-invariant by Proposition 2.7.6. So we only need to consider the behaviour of $f|_k[\Gamma_1 g \Gamma_2]$ at its cusps.

If f is a modular function, a modular form or a cusp form of level Γ_1 then so is each term $f|_k\alpha_i$ of level $\alpha_i^{-1}\Gamma_1\alpha_i \cap \mathrm{SL}_2(\mathbb{Z})$. (This stays to be checked as an exercise.) Hence all the $f|_k\alpha_i$ are of the same type of level

$$\Gamma'_2 = \left(\bigcap_{i=1}^r \alpha_i^{-1}\Gamma_1\alpha_i \right) \cap \Gamma_2$$

and thus so is $f|_k[\Gamma_1 g \Gamma_2]$. Finally note that given a function f that is Γ-invariant all of the properties for f being a modular function, a modular form or a cusp form of level Γ are satisfied if and only if these properties are already satisfied at any smaller level $\Gamma' \subseteq \Gamma$ of finite index. As Γ'_2 is by construction contained in Γ_2, we only need to check that Γ'_2 is of finite index. But this is clear as Γ_1 and $\alpha_i^{-1}\Gamma_1\alpha_i$ are commensurable by Proposition 2.7.3, and Γ_1 and Γ_2 are commensurable as they are both finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$. Therefore we can ascend from Γ'_2 to Γ_2. □

Remark. We thus have a map

$$M_k(\Gamma_1) \xrightarrow{[\Gamma_1 g \Gamma_2]} M_k(\Gamma_2).$$

This map preserves cusp forms and hence induces a map

$$M_k(\Gamma_1)/S_k(\Gamma_1) \to M_k(\Gamma_2)/S_k(\Gamma_2).$$

If $k \geq 3$ this is the map $B_k(\Gamma_1) \to B_k(\Gamma_2)$. It can be explicitly described by considering Eisenstein series since these form a basis in $B_k(\Gamma_1)$. So it suffices to consider the images $f_c := G_{k,\Gamma_1,c}|_k[\Gamma_1 g \Gamma_2]$ of the Eisenstein series for all (regular) cusps c of Γ_1. More precise, we are only interested in the values at the cusps of f_c.

Examples.

(1) If $g^{-1}\Gamma_1 g = \Gamma_2$ then $\Gamma_1 g \Gamma_2 = \Gamma_1 g$. So the map $f \mapsto f|_k[\Gamma_1 g \Gamma_2]$ is just $f \mapsto f|_k g$. Since $f \mapsto f|_k g^{-1}$ is clearly the invers of this map, $f \mapsto f|_k g$ gives an isomorphism of the spaces $M_k(\Gamma_1)$ and $M_k(\Gamma_2)$.

(2) More generally, if $g^{-1}\Gamma_1 g \supseteq \Gamma_2$ then the quotient $(\Gamma_2 \cap (g^{-1}\Gamma_1 g))\backslash\Gamma_2$ is still trivial. Hence the map $f \mapsto f|_k[\Gamma_1 g \Gamma_2]$ is as in the first example just $f \mapsto f|_k g$, but it is not an isomorphism anymore. Its image is $M_k(g^{-1}\Gamma_1 g) \subseteq M_k(\Gamma_2)$.

(3) Suppose $\Gamma_1 \subseteq \Gamma_2$ and $g = 1$. Then the quotient $(\Gamma_2 \cap (g^{-1}\Gamma_1 g))\backslash\Gamma_2$ simplifies to $\Gamma_1\backslash\Gamma_2$. So the α_i's are just coset representatives for $\Gamma_1\backslash\Gamma_2$ and we are mapping

$$f \mapsto \sum_{\gamma \in \Gamma_1\backslash\Gamma_2} f|_k\gamma.$$

Since $f|_k\gamma = f$ for all $\gamma \in \Gamma_2$ if $f \in M_k(\Gamma_2)$, the restriction of this map to $M_k(\Gamma_2)$ is just the multiplication by the index $[\Gamma_2 : \Gamma_1]$. Hence the map $M_k(\Gamma_1) \to M_k(\Gamma_2)$ is surjective. It is called the "trace map" from level Γ_1 to level Γ_2.

(4) The last example is a much more subtle one. Let $\Gamma = \Gamma_1 = \Gamma_2 = \mathrm{SL}_2(\mathbb{Z})$ and $g = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ for some prime p. Then

$$\Gamma \cap \left(g^{-1}\Gamma g\right) = \Gamma^0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : p \text{ didivdes } b \right\}.$$

One can check that $\Gamma^0(p)\backslash\Gamma$ is given by the coset representatives $\left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right)_{j=0,\dots,p-1}$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. So for $f \in M_k(\Gamma)$ we have

$$\begin{aligned} f|_k[\Gamma g\Gamma] &= \sum_{j=0}^{p-1} f|_k \left[\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}\right] + f|_k \left[\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right] \\ &= \sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} + f|_k \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} \\ &= \sum_{j=0}^{p-1} p^{k-1}p^{-k} f\left(\frac{z+j}{p}\right) + p^{k-1}(pz)^{-k} f\left(-\frac{1}{pz}\right). \end{aligned}$$

But f is a modular form of level $\mathrm{SL}_2(\mathbb{Z})$, so

$$(pz)^{-k} f\left(-\frac{1}{pz}\right) = \left(f|_k \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right)(pz) = f(pz).$$

Therefore we get

$$f|_k[\Gamma g\Gamma] = \frac{1}{p}\sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) + p^{k-1} f(pz) = T_p(f)(z).$$

So these double coset operators indeed generate the level 1 Hecke operators T_n introduced in Section 1.6.

Definition 2.7.8. (a) Let $\Gamma_1, \Gamma_2 \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index. We define $\mathcal{R}(\Gamma_1, \Gamma_2)$ to be the $\mathbb{C}$-vector space with basis the symbols $[\Gamma_1 g \Gamma_2]$ for each $g \in \Gamma_1\backslash \mathrm{GL}_2^+(\mathbb{Q})/\Gamma_2$. Further, we define $\mathcal{R}(\Gamma) = \mathcal{R}(\Gamma, \Gamma)$.

(b) Let $\Gamma_1, \Gamma_2, \Gamma_3 \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index. We define a multiplication

$$\mathcal{R}(\Gamma_1, \Gamma_2) \times \mathcal{R}(\Gamma_2, \Gamma_3) \to \mathcal{R}(\Gamma_1, \Gamma_3).$$

For $[\Gamma_1 g \Gamma_2] \in \mathcal{R}(\Gamma_1, \Gamma_2)$ and $[\Gamma_2 h \Gamma_3] \in \mathcal{R}(\Gamma_2, \Gamma_3)$ write

$$\Gamma_1 g \Gamma_2 = \bigsqcup_{i=1}^{s} \Gamma_1 \lambda_i \quad \text{and} \quad \Gamma_2 h \Gamma_3 = \bigsqcup_{j=1}^{t} \Gamma_2 \mu_j.$$

We define

$$[\Gamma_1 g \Gamma_2] \times [\Gamma_2 h \Gamma_3] := \sum_{\gamma \in \Gamma_1 \backslash \mathrm{GL}_2^+(\mathbb{Q}) / \Gamma_3} c_\gamma \cdot [\Gamma_1 \gamma \Gamma_3]$$

where

$$c_\gamma := |\{(i,j) \in \{1, \dots, s\} \times \{1, \dots, t\} \colon \lambda_i \mu_j \in \Gamma_1 \gamma\}|\,.$$

It is tedious to check that this definition is indeed well-defined, so independent of the choice of λ_i and μ_j, and that this multiplication is associative, so

$$[\Gamma_1 g \Gamma_2] \times \Big([\Gamma_2 h \Gamma_3] \times [\Gamma_3 j \Gamma_4]\Big) = \Big([\Gamma_1 g \Gamma_2] \times [\Gamma_2 h \Gamma_3]\Big) \times [\Gamma_3 j \Gamma_4].$$

We omit the proof here. Moreover, it can be checked that the introduced multiplication satisfies

$$f|_k\Big([\Gamma_1 g \Gamma_2] \times [\Gamma_2 h \Gamma_3]\Big) = \Big(f|_k[\Gamma_1 g \Gamma_2]\Big)|_k[\Gamma_2 h \Gamma_3].$$

In particular, $\mathcal{R}(\Gamma)$ is a ring and $M_k(\Gamma)$ and $S_k(\Gamma)$ are right modules over this ring.

2.8 The Hecke algebras of $\Gamma_0(N)$ and $\Gamma_1(N)$

In this chapter we want to generalise the operators T_n introduced in Section 1.6. We noticed in the previous section that for p prime T_p agrees with the action of the double coset operator $\mathrm{SL}_2(\mathbb{Z}) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \mathrm{SL}_2(\mathbb{Z})$ on $M_k(\mathrm{SL}_2(\mathbb{Z}))$. As it is difficult to generalise this for arbitrary finite index subgroups Γ we are going to focus on the groups $\Gamma_0(N)$ and $\Gamma_1(N)$ in this section.

Proposition 2.8.1. *Let p be prime, $N \geq 1$ and $\Gamma = \Gamma_0(N)$ or $\Gamma = \Gamma_1(N)$.*

(i) If p divides N then

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma = \bigsqcup_{i=0}^{p-1} \Gamma \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix}.$$

(ii) If p does not divide N then

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma = \bigsqcup_{i=0}^{p-1} \Gamma \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} \sqcup \Gamma \gamma \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

where $\gamma = 1$ in the case of $\Gamma_0(N)$ and $\gamma = \left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)$ in the case of $\Gamma_1(N)$ with m, n being any integers such that $mp - nN = 1$.

Proof. Let $g = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. Recall that $\mathrm{SL}_2(\mathbb{Z}) \cap (g^{-1} \mathrm{SL}_2(\mathbb{Z}) g) = \Gamma^0(p)$ and

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i=0}^{p-1} \Gamma^0(p) \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \sqcup \Gamma^0(p) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Put $\tau_i = \left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right)$ for $i = 0, \ldots, p-1$ and $\tau_p = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Now let $\Gamma = \Gamma_1(N)$. We can easily check that $\Gamma \cap (g^{-1}\Gamma g) = \Gamma \cap \Gamma^0(p)$. Hence intersecting the above equality from the left with Γ yields

$$\Gamma = \Gamma \cap \left(\bigsqcup_{i=0}^{p} \Gamma^0(p)\tau_i \right) = \bigsqcup_{i=0}^{p-1} \left(\Gamma \cap \Gamma^0(p)\right) \tau_i \sqcup \left(\Gamma \cap \left(\Gamma^0(p)\tau_p\right)\right).$$

Here the first $p-1$ terms are easy to handle as $\tau_i \in \Gamma$ for $i = 0, \ldots, p-1$. To write the last term in the form $(\Gamma \cap \Gamma^0(p))\tau_p'$ we need to find a representive of the coset $\Gamma^0(p)\tau_p$ that lies in Γ, so $\tau_p' \in \Gamma \cap \Gamma^0(p)\tau_p$. Suppose such an element exists and write $\tau_p' = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then $\left(\begin{smallmatrix} -b & a \\ -d & c \end{smallmatrix}\right) = \tau_p'\tau_p^{-1} \in \Gamma^0(p)$, so p divides a. But $a = 1$ modulo N as $\tau_p' \in \Gamma$. So if p divides N we have a contradiction, meaning that the intersection is empty in this case. So the last term in the above disjoint union vanishes and we have $\Gamma g \Gamma = \bigsqcup_{i=0}^{p-1} \Gamma\alpha_i$ with $\alpha_i = g\tau_i = \left(\begin{smallmatrix} 1 & i \\ 0 & p \end{smallmatrix}\right)$ as claimed.

Suppose p does not divide N. Then we can find an element of the form $\left(\begin{smallmatrix} pa & b \\ Nc & d \end{smallmatrix}\right)$ such that $pad - Nbc = 1$ and $pa = d = 1$ modulo N. Let this be τ_p'. Then $\tau_p' \in \Gamma$ and $\tau_p' \in \Gamma^0(p)\tau_p$. Therefore we have $\Gamma g \Gamma = \bigsqcup_{i=0}^{p-1} \Gamma\alpha_i$ with $\alpha_i = g\tau_i = \left(\begin{smallmatrix} 1 & i \\ 0 & p \end{smallmatrix}\right)$ for $i = 0, \ldots, p-1$ and $\alpha_p = g\tau_p'$. Note that

$$\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} pa & b \\ Nc & d \end{pmatrix} = \begin{pmatrix} a & b \\ Nc & pd \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

So this matrix works as a final piece of our double coset for any a, b, c, d such that $pa = d = 1$ modular N and $pad - Nbc = 1$. In particular, we can take $c = d = 1$ as this always gives a solution for a, b. So we have

$$\Gamma g \Gamma = \bigsqcup_{i=0}^{p-1} \Gamma\alpha_i \sqcup \Gamma \begin{pmatrix} a & b \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

Finally note that everything works the same for $\Gamma = \Gamma_0(N)$. Moreover, the latter matrix $\left(\begin{smallmatrix} a & b \\ N & p \end{smallmatrix}\right)$ will be in $\Gamma_0(N)$, so we can ignore the whole matrix in this case. □

Hence we have for $\Gamma = \Gamma_0(N)$ or $\Gamma = \Gamma_1(N)$ and any $f \in M_k(\Gamma)$ for p dividing N that

$$\left[\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma\right](f) = \frac{1}{p} \sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right)$$

and for p not dividing N that

$$\left[\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma\right](f) = \frac{1}{p} \sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right) + p^{k-1}\left(f|_k \begin{pmatrix} m & n \\ N & p \end{pmatrix}\right)(pz).$$

Moreover, in the case $\Gamma = \Gamma_0(N)$ the term $f|_k\left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)$ reduces to f.

2.8.1 Interlude: Dirichlet characters

Definition 2.8.2. Let $N \geq 1$. A **Dirichlet charachter mod** N is a homomorphism of the multiplicative groups $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$.

Example. The map

$$(\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}^\times,\ 1 \mapsto 1,\ 3 \mapsto -1$$

is a Dirichlet character mod 4. In particular, it is the only non-trivial character mod 4. An example of a character mod 13 is the map

$$(\mathbb{Z}/13\mathbb{Z})^\times \to \mathbb{C}^\times,\ 2 \mapsto e^{2\pi i/12},$$

which is well-defined since 2 generates $(\mathbb{Z}/13\mathbb{Z})^\times$.

If M divides N any Dirichlet character mod M induces a character mod N. We say a character χ is **primitve** if it does not arise in this way from any M dividing N, $M < N$. The two examples above are primitive characters but for example

$$(\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{C}^\times,\ 1, 5 \mapsto 1,\ 3, 7 \mapsto -1$$

is not primitve since it comes from the above character mod 4.

To see how Dirichlet characters relate to modular forms first note that $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$. This is clear since $\Gamma_1(N)$ is the kernel of the group homomorphism between $\Gamma_0(N)$ and $(\mathbb{Z}/N\mathbb{Z})^\times$ sending a matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to a modulo N. This map is well-defined as $\gamma \in \Gamma_0(N)$ implies c being divisble by N, so N and a have to be coprime. Now consider $g \in \Gamma_0(N)$. Then

$$\Gamma_1(N) g \Gamma_1(N) = \Gamma_1(N) g = g\Gamma_1(N).$$

Let $g_1, \ldots, g_r \in \Gamma_0(N)$ be coset representatives for $\Gamma_1(N)\backslash\Gamma_0(N)$. Then $\Gamma_1(N)g$ is one of these cosets, so g gives an element of $\mathcal{R}(\Gamma_1(N))$ which only depends on the coset of g modular $\Gamma_1(N)$. Therefore the image of $g = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right)$ in $\mathcal{R}(\Gamma_1(N))$ depends only on d mod N since this uniquely determines a mod N. Thus we get a group homomorphism

$$(\mathbb{Z}/N\mathbb{Z})^\times \to \mathcal{R}(\Gamma_1(N)),\ d \mapsto \Gamma_1(N) \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \Gamma_1(N)$$

and hence an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ by linear operators on $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$. (Such an action is called a representation of $(\mathbb{Z}/N\mathbb{Z})^\times$.)

Proposition 2.8.3. *Let V be any complex vector space with an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ by linear operators. Then*

$$V = \bigoplus_{\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} V^\chi$$

where

$$V^\chi = \left\{ v \in V : g.v = \chi(g) \cdot v \text{ for all } g \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

The proof is omitted.

Definition 2.8.4. Let χ be a Dirichlet character. We define $M_k(\Gamma_1(N), \chi)$ as the χ-eigenspace $M_k(\Gamma_1(N))^\chi$ for the action of $(\mathbb{Z}/N\mathbb{Z})^\times$. This is called **the space of modular forms of level N and character χ**.

If $\mathbb{1}_N$ is the trivial character mod N then

$$M_k(\Gamma_1(N), \mathbb{1}_N) = M_k(\Gamma_0(N)).$$

To see this consider $f \in M_k(\Gamma_1(N), \mathbb{1}_N)$. Then $f = g.f$ for all $g \in (\mathbb{Z}/N\mathbb{Z})^\times$ and thus $f = f|_k\tilde{g}$ for all $\tilde{g} \in \Gamma_0(N)$ where $\tilde{g}$ denotes the element in $\Gamma_0(N)$ associated to $g \in (\mathbb{Z}/N\mathbb{Z})^\times$. Moreover, note that $M_k(\Gamma_1(N), \chi)$ is trivial unless $\chi(-1) = (-1)^k$. This is clear by definition.

Proposition 2.8.5. *If $f \in M_k(\Gamma_1(N), \chi)$ then*

$$\left[\Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(N)\right](f) = \sum_{n=0}^{\infty} a_{np}(f)q^n + \chi(p)\,p^{k-1}\sum_{n=0}^{\infty} a_n(f)q^{np}.$$

Proof. We have shown in Proposition 2.8.1 that

$$\left[\Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(N)\right](f) = \frac{1}{p}\sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right) + p^{k-1}\left(f|_k\begin{pmatrix}m & n\\ N & p\end{pmatrix}\right)(pz).$$

But since we have $\left(\begin{smallmatrix}m & n\\ N & p\end{smallmatrix}\right) \in \Gamma_0(N)$ it acts as $\chi(p)$ on $M_k(\Gamma_1(N), \chi)$. Hence the statement can be shown following the proof of Proposition 1.6.9 (a). □

Note that the previous proposition only makes sense if p does not divide N, since $\chi(p)$ would not be defined otherwise. But we can formally extend it to all p by defining $\chi(p) = 0$ in the case of p dividing N.

Definition 2.8.6. We use the following notations for elements of $\mathcal{R}(\Gamma_1(N))$:

- For p prime the element $\Gamma_1(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma_1(N)$ is denoted by T_p. (For p dividing N this is sometimes also denoted by U_p.)
- For $\lambda \in \mathbb{Q}^\times$ the element $\Gamma_1(N)\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right)\Gamma_1(N)$ is denoted by R_λ.
- For $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ the element $\Gamma_1(N)\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\Gamma_1(N)$ is called the **diamond operator**, denoted by $\langle d\rangle$, where a, b, c are any integers such that $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma_0(N)$.

Moreover, we define $\mathcal{T}(\Gamma_1(N))$ as the subalgebra of $\mathcal{R}(\Gamma_1(N))$ generated by the operators T_p, R_λ and $\langle d\rangle$ for all primes p, $\lambda \in \mathbb{Q}^\times$ and $d \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Proposition 2.8.7. *The algebra $\mathcal{T}(\Gamma_1(N))$ is commutative.*

We will only sketch the proof:

Proof. The R_λ's commute with everything since $\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right)$ is central in $\mathrm{GL}_2^+(\mathbb{Q})$ and the $\langle d\rangle$'s commute with each other since

$$\langle d\rangle\langle d'\rangle = (\Gamma g\Gamma)(\Gamma g'\Gamma) = \Gamma g g'\Gamma = \langle dd'\rangle = \langle d'd\rangle = \Gamma g' g\Gamma = (\Gamma g'\Gamma)(\Gamma g\Gamma) = \langle d'\rangle\langle d\rangle .$$

Here we used that $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ and that $(\mathbb{Z}/N\mathbb{Z})^\times$ is abelian. It remains to show that the T_p's commute with each other and with the $\langle d\rangle$'s.

We will first show that the T_p's commute among themselves. Let p, q be distinct primes. We claim that

$$T_pT_q = \Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & pq\end{pmatrix}\Gamma_1(N).$$

Moreover, we claim

$$\alpha\beta \in \Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & pq\end{pmatrix}\Gamma_1(N)$$

for any $\alpha \in \Gamma_1(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma_1(N)$, $\beta \in \Gamma_1(N)\left(\begin{smallmatrix}1 & 0\\ 0 & q\end{smallmatrix}\right)\Gamma_1(N)$. This works as $\alpha\beta$ has determinant pq, so by the Smith normal form we have $\alpha\beta \in \mathrm{SL}_2(\mathbb{Z})\left(\begin{smallmatrix}1 & 0\\ 0 & pq\end{smallmatrix}\right)\mathrm{SL}_2(\mathbb{Z})$. One can show that since $\alpha\beta = \left(\begin{smallmatrix}1 & *\\ 0 & pq\end{smallmatrix}\right)$ mod N we in fact have

$$\alpha\beta \in \Gamma_1(N)\begin{pmatrix}1 & *\\ 0 & pq\end{pmatrix}\Gamma_1(N).$$

This proves that the product T_pT_q is a constant multiple of $\Gamma_1(N)\left(\begin{smallmatrix}1 & 0\\ 0 & pq\end{smallmatrix}\right)\Gamma_1(N)$ and one can check that this constant is indeed one. So the first step is done.

For the second part let $g = \left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)$ and $\gamma = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ as in the definition of $\langle d\rangle$. Since $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ we have

$$\langle d\rangle T_p = (\Gamma\gamma\Gamma)(\Gamma g\Gamma) = \Gamma\gamma g\Gamma\gamma^{-1}\gamma\Gamma = (\Gamma\gamma g\gamma^{-1}\Gamma)(\Gamma\gamma\Gamma) = \left[\Gamma_1(N)(\gamma g\gamma^{-1})\Gamma_1(N)\right]\langle d\rangle .$$

But $\gamma\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\gamma^{-1}$ has determinant p and is $\left(\begin{smallmatrix}1 & *\\ 0 & p\end{smallmatrix}\right)$ mod N. By multiplying on the right by some power of $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \in \Gamma_1(N)$ we can make this be $\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)$ mod N. So it is in $\Gamma_1(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma_1(N)$ and thus $T_p\langle d\rangle = \langle d\rangle T_p$. □

Exercise. Let $N > 1$. Find an element of $\mathcal{R}(\Gamma_1(N))$ that is not in $\mathcal{T}(\Gamma_1(N))$.

Definition 2.8.8. For a prime power $n = p^r$, $r \geq 2$, we define T_n by

$$T_{p^r} = \begin{cases}(T_p)^r, & \text{if } p \text{ divides } N,\\ T_pT_{p^{r-1}} - p\,R_pT_{p^{r-2}}\langle p\rangle, & \text{if } p \text{ does not divide } N.\end{cases}$$

For general $n = p_1^{r_1}\dots p_k^{r_k}$ we define $T_n = T_{p_1^{r_1}}\dots T_{p_k^{r_k}}$.

Note that $T_n \in \mathcal{T}(\Gamma_1(N))$ for all $n \in \mathbb{N}$ by definition. In particular all T_n's commute.

Proposition 2.8.9. *Let $f \in M_k(\Gamma_1(N))$. Then $a_1(T_nf) = a_n(f)$.*

Proof. As in the level 1 case we will actually prove a stronger statement: For m, n coprime we have $a_m(T_n f) = a_{mn}(f)$. To see this consider first a prime power $n = p^r$. By induction and using Proposition 2.8.5 we get

$$\begin{aligned} T_{p^r}(f) = \sum_{n=0}^{\infty} a_{np^r}(f) q^n \; &+ \; p^{k-1} \sum_{n=0}^{\infty} a_{np^{r-1}} \left(\langle p \rangle f \right) q^{np} \\ &+ \; p^{2(k-1)} \sum_{n=0}^{\infty} a_{np^{r-2}} \left(\langle p \rangle^2 f \right) q^{np^2} \\ &+ \; \ldots \; + \; p^{r(k-1)} \sum_{n=0}^{\infty} a_n \left(\langle p \rangle^r f \right) q^{np^r}. \end{aligned}$$

Therefore the general case follows as in Section 1.6. □

Proposition 2.8.10. *(a) For all χ mod N the operators T_n preserve the subspaces $M_k(\Gamma_1(N), \chi)$ and $S_k(\Gamma_1(N), \chi)$ of $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$.*

(b) For p prime the action of T_p on $M_k(\Gamma_1(N), \mathbb{1}_N)$ coincides with $\Gamma_0(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_0(N)$.

Proof. For part (a) let $f \in M_k(\Gamma_1(N), \chi)$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Then

$$(T_n(f))|_k \gamma = \langle d \rangle \left(T_n(f)\right) = T_n(\langle d \rangle (f)) = T_n(\chi(d) \cdot f) = \chi(d) \cdot T_n(f).$$

Hence $T_n(f)$ is in $M_k(\Gamma_1(N), \chi)$. Clearly the same holds for $S_k(\Gamma_1(N), \chi)$.

For part (b) recall that $M_k(\Gamma_1(N), \mathbb{1}_N) = M_k(\Gamma_0(N))$. Then the statement is clear by Proposition 2.8.1 as we can choose a set of left coset representatives for $\Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_1(N)$ which are also left $\Gamma_0(N)$-coset representatives for $\Gamma_0(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_0(N)$ since $\left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)$ acts trivial on $M_k(\Gamma_1(N), \mathbb{1}_N)$ in the case of p not dividing N. So the corresponding operators coincide. □

Part (b) of the propositon allows us to identify $M_k(\Gamma_0(N))$ with $M_k(\Gamma_1(N), \mathbb{1}_N)$. Hence we don't have to consider $\Gamma_0(N)$ any more.

Definition 2.8.11. We say $f \in M_k(\Gamma_1(N))$ is an **eigenform** if it is a simultaneous eigenvector for all the T_n's and $\langle d \rangle$'s.

Remarks. (a) Since the $\langle d \rangle$'s can be resolved from the T_n's (which is not trivial and stays to be checked) it sufficies to define an eingenform as a simultaneous eigenvector for all the T_n's.

(b) Any eigenform f lies in $M_k(\Gamma_1(N), \chi)$ for some character χ. To see this let f in $M_k(\Gamma_1(N))$ be an eigenform. Then there are λ_d such that $\langle d \rangle f = \lambda_d f$ for all d coprime to N, and $\chi \colon d \mapsto \lambda_d$ defines a character such that $f \in M_k(\Gamma_1(N), \chi)$.

(c) As in the level 1 case we have $a_1(f) \neq 0$ unless f is constant. So we can scale such that $a_1(f) = 1$. In this case we say that f is **normalised**.

(d) If f is a normalised eigenform then we have

$$a_{mn}(f) = a_m(f)a_n(f)$$

for m, n coprime and

$$a_{p^r}(f) = a_p(f)a_{p^{r-1}}(f) - p^{k-1}\chi(p)a_{p^{r-2}}(f)$$

for p prime and $r \geq 2$. (Again we interpret $\chi(p)$ as 0 if p divides N.)

2.9 Hecke operators and the Petersson product

Let Γ be any finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Recall that we defined the Petersson product for $f_1, f_2 \in M_k(\Gamma)$, at least one vanishing at every cusp, by

$$\langle f_1, f_2\rangle_\Gamma = \int_{\Gamma\backslash\mathcal{H}} f_1(z)\overline{f_2(z)}(\mathrm{Im}(z))^k dA(z).$$

This is clearly positive definite, linear in the first argument and conjugate symmetric, so an inner product on the space of cusp forms of weight k and level Γ. Recall that if V is a finite-dimensional $\mathbb{C}$-vector space equipped with an inner product and $T\colon V \to V$ is a linear operator then there is $T^*\colon V \to V$ such that $\langle Tx, y\rangle = \langle x, T^*y\rangle$ for all $x, y \in V$. T^* is called the adjoint of T. The matrix of T^* is given by the conjugate transpose of T with respect to an orthonormal basis.

Theorem 2.9.1. *Let $f_1, f_2 \in M_k(\Gamma)$ for some $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index such that at least one of f_1, f_2 is a cusp form and let $g \in \mathrm{GL}_2^+(\mathbb{Q})$. Then*

$$\langle f_1|_k[\Gamma g\Gamma],\ f_2\rangle_\Gamma = \langle f_1,\ f_2|_k[\Gamma g'\Gamma]\rangle_\Gamma$$

where $g' = \det(g)\cdot g^{-1}$. So $\Gamma g'\Gamma$ is the adjoint of $\Gamma g\Gamma$.

To prove this theorem we first need some technical results. The first one generalises Lemma 2.6.1 for matrices in $\mathrm{GL}_2^+(\mathbb{Z})$:

Lemma 2.9.2. *Let $U \subseteq \mathcal{H}$ be closed and bounded, $f\colon U \to \mathbb{C}$ a continuous function and $g \in \mathrm{GL}_2^+(\mathbb{R})$. Then*

$$\int_U f(z)dA(z) = \int_{g^{-1}U} f(g.z)dA(z).$$

Proof. Let J_g denote the Jacobian matrix of the map g seen as a map between subsets of $\mathbb{R}^2$. We can easily check that

$$|J_g| = |g'(z)|^2 = \frac{\det(g)^2}{|j(g,z)|^4} \quad \text{and} \quad \mathrm{Im}(g.z) = \frac{\det(g)\,\mathrm{Im}(z)}{|j(g,z)|^2}.$$

Hence

$$\int_U f(z)dA(z) = \int_{g^{-1}U} f(g.z)|J_g|\frac{dz}{\mathrm{Im}(g.z)^2} = \int_{g^{-1}U} f(g.z)dA(z).$$

□

Lemma 2.9.3. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be of finite index and let $g \in \mathrm{GL}_2^+(\mathbb{Q})$ such that $g^{-1}\Gamma g$ is contained in $\mathrm{SL}_2(\mathbb{Z})$. Then for any $f_1 \in M_k(\Gamma)$ and $f_2 \in M_k(g^{-1}\Gamma g)$ we have*

$$\langle f_1|_k g, f_2\rangle_{g^{-1}\Gamma g} = \langle f_1, f_2|_k g'\rangle_\Gamma ,$$

where $g' = \det(g) \cdot g^{-1}$ and f_1, f_2 are such that both sides are defined.

Proof. It can be checked as an exercise that if one of these sides is defined, so is the other. Further, an explicit calculation shows that for any compact $U \subseteq \mathcal{H}$ and for any continuous functions $f_1, f_2 \colon \mathcal{H} \to \mathbb{C}$

$$\int_U (f_1|_k g)(z)\overline{f_2(z)}(\mathrm{Im}(z))^k dA(z) = \int_{gU} f_1(z)\overline{(f_2|_k g')(z)}(\mathrm{Im}(z))^k dA(z).$$

Finally note that $[z] = [w]$ in $g^{-1}\Gamma g\backslash\mathcal{H}$ if and only if there is $\gamma \in \Gamma$ such that $g^{-1}\gamma g.z = w$, so if and only if $[g.z] = [g.w]$ in $\Gamma\backslash\mathcal{H}$. Hence D' is a fundamental domain of the quotient $g^{-1}\Gamma g\backslash\mathcal{H}$ if and only if gD' is a fundamental domain of $\Gamma\backslash\mathcal{H}$, and if we let U grow into D' then gU grows into gD'. Thus we are done. □

The following lemma specifies Proposition 2.7.4 in the case of $\Gamma_1 = \Gamma_2$.

Lemma 2.9.4. *For any $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index and any $g \in \mathrm{GL}_2^+(\mathbb{Q})$ we have that $[\Gamma : \Gamma \cap g^{-1}\Gamma g] = [\Gamma : \Gamma \cap g\Gamma g^{-1}]$. Moreover, there are elements $g_1, \ldots, g_r$ such that*

$$\Gamma g\Gamma = \bigsqcup_{i=1}^r \Gamma g_i = \bigsqcup_{i=1}^r g_i\Gamma.$$

Proof. We first check the index. Let $\Gamma' = \Gamma \cap g\Gamma g^{-1}$. Then $g^{-1}\Gamma' g = \Gamma \cap g^{-1}\Gamma g$. Note that these are both contained in $\mathrm{SL}_2(\mathbb{Z})$, and recall that gD' is a fundamental domain of $\Gamma'\backslash\mathcal{H}$ if and only if D' is a fundamental domain of $g^{-1}\Gamma' g\backslash\mathcal{H}$. Thus Lemma 2.9.2 gives

$$\int_{g^{-1}\Gamma' g\backslash\mathcal{H}} dA = \int_{D'} dA = \int_{gD'} dA = \int_{\Gamma'\backslash\mathcal{H}} dA.$$

Therefore we see $d_{\Gamma'} = d_{g^{-1}\Gamma' g}$ since

$$d_{\Gamma'} \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} dA = \int_{\Gamma'\backslash\mathcal{H}} dA = \int_{g^{-1}\Gamma' g\backslash\mathcal{H}} dA = d_{g^{-1}\Gamma' g} \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} dA,$$

and thus $[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}][\overline{\Gamma} : \overline{\Gamma'}] = [\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}][\overline{\Gamma} : \overline{g^{-1}\Gamma' g}]$, so $[\Gamma : \Gamma'] = [\Gamma : g^{-1}\Gamma' g]$ as claimed.

Now recall that we can choose $\tau_1, \ldots, \tau_r \in \Gamma$ and $\sigma_1, \ldots, \sigma_r \in \Gamma$ as in the proof of Proposition 2.7.4 such that $\Gamma g\Gamma = \bigsqcup_{i=1}^r \Gamma g\tau_i = \bigsqcup_{i=1}^r \sigma_i g\Gamma$. Put $g_i := \sigma_i g\tau_i$ for $1 \leq i \leq r$. Then $g_i \in \Gamma g\tau_i$ and $g_i \in \sigma_i g\Gamma$ by construction and hence the g_i's are simultaneous right and left coset representatives as claimed. □

Remark. It can be checked by a direct computation that $\int_D dA = 4\pi/3$ where D is the fundamental domain of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$. Hence we have for any finite index subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ that

$$\int_{\Gamma\backslash\mathcal{H}} dA = d_\Gamma \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} dA = d_\Gamma \cdot \frac{4\pi}{3}.$$

We are now able to prove the above theorem.

Proof of Theorem 2.9.1. Choose $g_1, \ldots, g_r$ such that $\Gamma g\Gamma = \bigsqcup_{i=1}^r \Gamma g_i = \bigsqcup_{i=1}^r g_i\Gamma$ as in Lemma 2.9.4, so $g_i := \sigma_i g\tau_i$ for some $\tau_1, \ldots, \tau_r, \sigma_1, \ldots, \sigma_r \in \Gamma$ with $\Gamma g\Gamma = \bigsqcup_{i=1}^r \Gamma g\tau_i$ and $\Gamma g\Gamma = \bigsqcup_{i=1}^r \sigma_i g\Gamma$. Now put $\Gamma' = \Gamma \cap (g^{-1}\Gamma g)$ and fix an $i \in \{1, \ldots, r\}$. We can check that

$$\Gamma \cap (g_i^{-1}\Gamma g_i) = \Gamma \cap (\tau_i^{-1}g^{-1}\Gamma g\tau_i) = \Gamma \cap (g^{-1}\Gamma g) = \Gamma',$$

and similarly that $g_i\Gamma' g_i^{-1} = (g_i\Gamma g_i^{-1}) \cap \Gamma = \Gamma'$. In particular, we see that $g_i\Gamma' g_i^{-1}$ is a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ as Γ' clearly is, and that $f_1 \in M_k(g_i\Gamma' g_i^{-1})$ since $g_i\Gamma' g_i^{-1} \le \Gamma$. Moreover, we have $f_2 \in M_k(\Gamma')$ since $\Gamma' \le \Gamma$, and thus we can use Lemma 2.9.3 which yields

$$\langle f_1|_k g_i, f_2\rangle_{\Gamma'} = \langle f_1, f_2|_k g_i'\rangle_{g_i\Gamma' g_i} = \langle f_1, f_2|_k g_i'\rangle_{\Gamma'},$$

where $g_i' = \det(g_i) \cdot g_i^{-1}$. Therefore we get

$$\langle f_1|_k[\Gamma g\Gamma], f_2\rangle_\Gamma = \frac{d_\Gamma}{d_{\Gamma'}}\langle f_1|_k[\Gamma g\Gamma], f_2\rangle_{\Gamma'} = \frac{d_\Gamma}{d_{\Gamma'}}\sum_{i=1}^r \langle f_1|_k g_i, f_2\rangle_{\Gamma'} = \frac{d_\Gamma}{d_{\Gamma'}}\sum_{i=1}^r \langle f_1, f_2|_k g_i'\rangle_{\Gamma'}.$$

Now consider $\Gamma g\Gamma = \bigsqcup_{i=1}^r g_i\Gamma$. Inverting yields $\Gamma g^{-1}\Gamma = \bigsqcup_{i=1}^r \Gamma g_i^{-1}$, and as the determinant of g and all g_i's are clearly equal we see $\Gamma g'\Gamma = \bigsqcup_{i=1}^r \Gamma g_i'$ where $g' = \det(g) \cdot g^{-1}$. Hence $\sum_{i=1}^r f_2|_k g_i' = f_2|_k[\Gamma g'\Gamma]$ and thus

$$\langle f_1|_k[\Gamma g\Gamma], f_2\rangle_\Gamma = \frac{d_\Gamma}{d_{\Gamma'}}\sum_{i=1}^r \langle f_1, f_2|_k g_i'\rangle_{\Gamma'} = \frac{d_\Gamma}{d_{\Gamma'}}\langle f_1, f_2|_k[\Gamma g'\Gamma]\rangle_{\Gamma'} = \langle f_1, f_2|_k[\Gamma g'\Gamma]\rangle_\Gamma$$

as claimed. □

Corollary 2.9.5. *The operators $\Gamma g\Gamma$ for $g \in \mathrm{GL}_2^+(\mathbb{Q})$ preserve $\mathcal{E}_k(\Gamma) \subseteq M_k(\Gamma)$.*

Proof. The operator $\Gamma g'\Gamma$ preserves the cusp forms. Using Theorem 2.9.1 we can pass to the orthogonal complement: We have for any $f_1 \in \mathcal{E}_k(\Gamma)$ and for any $f_2 \in S_k(\Gamma)$ that

$$\langle f_1|_k[\Gamma g\Gamma], f_2\rangle_\Gamma = \langle f_1, f_2|_k[\Gamma g'\Gamma]\rangle_\Gamma = 0$$

by Proposition 2.6.5 since f_1 is a linear combination of Eisenstein series and $f_2|_k[\Gamma g'\Gamma]$ is in $S_k(\Gamma)$. Thus $f_1|_k[\Gamma g\Gamma]$ is orthogonal to every cusp form and therefore in $\mathcal{E}_k(\Gamma)$ by a remark following Proposition 2.6.5. □

Corollary 2.9.6. *(a) For p prime not dividing N, the adjoint of T_p with respect to $\langle\cdot,\cdot\rangle_{\Gamma_1(N)}$ is given by $\langle p\rangle^{-1}T_p$. Furthermore, T_p is normal, so $T_p^*T_p = T_pT_p^*$.*

(b) *The diamond operators are orthogonal, so $\langle d\rangle^* = \langle d\rangle^{-1}$ for all $d \in (\mathbb{Z}/N\mathbb{Z})^\times$.*

(c) *The space $S_k(\Gamma_1(N))$ has an orthonormal bases consisting of simultaneous eigenvectors for the diamond operators and the T_p's, p not dividing N.*

Proof. Let $\Gamma = \Gamma_1(N)$ and let $g = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ for part (a). By Theorem 2.9.1 the adjoint of $\Gamma g \Gamma$ is given by $\Gamma g' \Gamma$ with $g' = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$. As p does not divide N by assumption, Proposition 2.8.1 gives that $\gamma g' \in \Gamma g \Gamma$ with $\gamma = \left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right) \in \Gamma_0(N)$. So there are $\gamma_1, \gamma_2 \in \Gamma$ such that $g' = \gamma^{-1}\gamma_1 g \gamma_2$. Finally recall that Γ is normal in $\Gamma_0(N)$. Therefore we see

$$\Gamma g' \Gamma = \Gamma(\gamma^{-1}\gamma_1 g \gamma_2)\Gamma = \Gamma(\gamma^{-1}\Gamma)\gamma_1 g \Gamma = (\Gamma\gamma\Gamma)^{-1}(\Gamma g \Gamma).$$

So we have shown that $T_p^* = [\Gamma g' \Gamma] = \langle p\rangle^{-1} T_p$ since $[\Gamma\gamma\Gamma] = \langle p\rangle$. This implies directly that T_p is normal as

$$T_p^* T_p = \langle p\rangle^{-1} T_p T_p = T_p \langle p\rangle^{-1} T_p = T_p T_p^*.$$

Part (b) is clear since we see for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ that $\gamma' = \gamma^{-1}$, so

$$\langle d\rangle^* = \Gamma\gamma'\Gamma = \Gamma\gamma^{-1}\Gamma = (\Gamma\gamma\Gamma)^{-1} = \langle d\rangle^{-1}.$$

So the operator $\langle d\rangle$ is orhtogonal.

For part (c) recall from first year linear algebra that a normal matrix is diagonalisable. If we take any orthonormal basis of $S_k(\Gamma)$ with respect to the Petersson product then the matrix of $\Gamma g' \Gamma$ is the conjugate transpose of the matrix $\Gamma g \Gamma$. Part (a) of this corollary shows that all T_p with p not dividing N are normal and hence diagonalisable, part (b) gives that the diamond operators are orthogonal, so also diagonalisable. Finally we recall that the diamond operators and the T_p's commute. Therefore they are simultaneously diagonalisable. □

Remark. Considering $\Gamma_0(N)$ instead of $\Gamma_1(N)$ the same logic applies, but as the $\langle d\rangle$ operators are trivial in this case the T_p are self-adjoint. Hence their eigenvalues are real. Therefore $S_k(\Gamma_0(N))$ has a basis of modular forms with real eigenvalues for the T_p's. In particular this applies to $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

The following example shows that the T_p, p dividing N, can indeed fail to be diagonalisable.

Example. Let $f \in S_k(\Gamma_1(N))$ and p prime not dividing N. Assume f is an eigenvector for T_p with eigenvalue λ and assume that f has character χ. Now look at the space $S_k(\Gamma_1(Np))$. It contains $f_1(z) := f(z)$ and $f_2(z) := f(pz)$. We can compute

$$\begin{aligned} \lambda f_1 &= \left[\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)\right](f) \\ &= \sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} + f|_k \left(\begin{pmatrix} m & n \\ N & p \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right) \\ &= \left[\Gamma_1(Np) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(Np)\right](f_1) + p^{k-1}\chi(p) f_2. \end{aligned}$$

Moreover, note that $f_2((z+j)/p) = f(z+j) = f(z)$ as $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ is in $\Gamma_1(N)$. Thus

$$\left[\Gamma_1(Np)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma_1(Np)\right](f_2) = \sum_{j=0}^{p-1} f_2|_k \begin{pmatrix}1&j\\0&p\end{pmatrix} = \sum_{j=0}^{p-1} \frac{1}{p} f_2\left(\frac{z+j}{p}\right) = f_1.$$

Therefore we have shown that $T_p f_1 = \lambda f_1 - p^{k-1}\chi(p) f_2$ and that $T_p f_2 = f_1$ for T_p being the operator with respect to $\Gamma_1(Np)$, so $T_p = [\Gamma_1(Np)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(Np)]$.

More generally at level $p^j N$, the space spanned by $f(z), f(pz), \ldots, f(p^j z)$ is T_p-stable and the matrix of T_p looks like

$$\begin{pmatrix} \lambda & 1 & 0 & 0 & \cdots & 0 \\ -p^{k-1}\chi(p) & 0 & 1 & 0 & & 0 \\ 0 & 0 & 0 & 1 & & 0 \\ \vdots & \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & 0 & & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Exercise. This matrix is not diagonalisable for $j \geq 3$, independent of λ, χ and k.

So there is an obstruction to diagonalise T_p for p dividing N coming from forms of small level at p.

2.10 Old and new modular forms

Definition 2.10.1. Let $N \geq 1$. For a prime divisor p of N we define

$$S_k(\Gamma_1(N))_{p\text{-old}} = i_{1,p}\left(S_k(\Gamma_1(N/p))\right) + i_{2,p}\left(S_k(\Gamma_1(N/p))\right)$$

where $i_{1,p}$ is the natural inclusion $S_k(\Gamma_1(N/p)) \hookrightarrow S_k(\Gamma_1(N))$ and $i_{2,p}$ maps $f(z)$ to $f(pz)$. (Note that this sum is not generally a direct sum.) The space of all old modular forms is then given by

$$S_k(\Gamma_1(N))_{\text{old}} = \sum_{p \text{ prime},\, p|N} S_k(\Gamma_1(N))_{p\text{-old}}.$$

Moreover, we define $S_k(\Gamma_1(N))_{p\text{-new}}$ as the orthogonal complement of a p-old subspace and

$$S_k(\Gamma_1(N))_{\text{new}} = \bigcap_{p \text{ prime},\, p|N} S_k(\Gamma_1(N))_{p\text{-new}}.$$

This is precisely the orthogonal complement of $S_k(\Gamma_1(N))_{\text{old}}$.

Proposition 2.10.2. *All of these subspaces of $S_k(\Gamma_1(N))$ are stable under the operators T_n for all $n \geq 1$ and $\langle d \rangle$ for all $d \in (\mathbb{Z}/N\mathbb{Z})^\times$.*

Proof. It sufficies to show that the old subspaces are stable under the operators $\langle d\rangle$, T_p and their adjoints. We know that the adjoints of T_p for p not dividing N and of $\langle d\rangle$ for all $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ are in the subalgebra $\mathcal{T}(\Gamma_1(N))$, so we don't need to worry about them.

Firstly consider T_l for l not dividing N. Then the action of T_l on $S_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N/p))$ is given by some formula on q-expansions for all p dividing N. Hence $i_{1,p}(T_l f) = T_l(i_{1,p} f)$ is obvious for all $f \in S_k(\Gamma_1(N/p))$ and similarly we have

$$\begin{aligned} i_{2,p}(T_l f) &= i_{2,p}\left[\sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} + f|_k \left(\begin{pmatrix} m & n \\ N & p \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right)\right] \\ &= \sum_{j=0}^{p-1} (i_{2,p} f)|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} + (i_{2,p} f)|_k \left(\begin{pmatrix} m & n \\ N & p \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right) = T_l(i_{2,p} f). \end{aligned}$$

Hence T_l preserves $S_k(\Gamma_1(N))_{p\text{-old}}$ for all p.

Now consider $\langle d\rangle$ for some $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. Choose some $\gamma = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Then $\gamma \in \Gamma_0(N/p)$ also represents $\langle d\rangle \in \mathcal{R}(\Gamma_1(N/p))$. As functions on $\mathcal{H}$ we clearly have

$$i_{1,p}(\langle d\rangle f) = \langle d\rangle f = f|_k\gamma = (i_{1,p} f)|_k\gamma = \langle d\rangle (i_{1,p} f).$$

Furthermore

$$\langle d\rangle (i_{2,p} f) = \langle d\rangle \left(p^{1-k} f|_k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right) = p^{1-k}\left(f|_k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right)|_k \begin{pmatrix} a & b \\ Nc & d \end{pmatrix}.$$

Note that

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} = \begin{pmatrix} a & pb \\ Nc/p & d \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

Hence

$$\begin{aligned} \langle d\rangle (i_{2,p} f) &= p^{1-k}\left(f|_k \begin{pmatrix} a & pb \\ Nc/p & d \end{pmatrix}\right)|_k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \\ &= p^{1-k}(\langle d\rangle f)|_k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \\ &= i_{2,p}(\langle d\rangle f). \end{aligned}$$

So it remains to consider the T_q for q dividing N and the corresponding adjoints T_q^*. These cases are trickier. If q divides N but $q \neq p$, then T_q is given by the same formulae at level N and at level N/p. So we have

$$T_q \circ i_{1,p} = i_{1,p} \circ T_q, \quad T_q \circ i_{2,p} = i_{2,p} \circ T_q$$

as in the case of q not dividing N. So what about T_p, does it preserve p-old modular forms?

If p^2 is not dividing N, so p not dividing N/p, then we have for $f \in S_k(\Gamma_1(N/p))$ that $i_{1,p}f = \sum_{n=0}^{\infty} a_n(f)q^n$, so $T_p(i_{1,p}f) = \sum_{n=0}^{\infty} a_{np}(f)q^n$, and therefore

$$\begin{aligned} i_{1,p}(T_p f) = T_p f = T_p(i_{1,p}f) + p^{k-1}\sum_{i=0}^{\infty} a_n(\langle p\rangle\, f)q^{np} \\ = T_p(i_{1,p}f) + i_{2,p}(\langle p\rangle\, f) \; = T_p(i_{1,p}f) + \langle p\rangle\,(i_{2,p}f). \end{aligned}$$

Hence $T_p(i_{1,p}f) \in S_k(\Gamma_1(N))_{p\text{-old}}$. On the other hand we have

$$T_p(i_{2,p}f) = T_p\left(\sum_{n=0}^{\infty} a_n(f)q^{np}\right) = \sum_{n=0}^{\infty} a_n(f)q^n = i_{1,p}(f).$$

Hence T_p preserves $S_k(\Gamma_1(N))_{p\text{-old}}$ if p^2 does not divide N.

If p^2 divides N the formulae are the same for T_p at level N and at level N/p. So we have

$$T_p \circ i_{1,p} = i_{1,p} \circ T_p, \quad T_p \circ i_{2,p} = i_{1,p}.$$

So we have shown that T_q preserves $S_k(\Gamma_1(N))_{p\text{-old}}$ for all primes p, q. Hence T_q preserves $S_k(\Gamma_1(N))_{\text{old}}$ and similarly for $\langle d\rangle$.

Therefore we are left with the adjoints T_q^* for primes q dividing N. Do these preserve old modular forms? Let $w_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. This normalises $\Gamma_1(N)$, so $\Gamma_1(N)w_N\Gamma_1(N)$ is a single left or right coset (as for the diamond operators), and defines an element of $\mathcal{R}(\Gamma_1(N))$. (This is sometimes called the Atkin-Lehner involution.) We check that

$$T_p^* = \left[\Gamma_1(N)\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\Gamma_1(N)\right] = w_N T_p w_N^{-1}$$

since

$$\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}^{-1} = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

Note that $w_N^2 = -N \cdot \mathrm{id}$, so $w_N^{-1} = (-1)^k N^{-k+1} w_N$ as operators. Thus w_N is indeed nearly an involution and it stays to check that w_N preserves the p-old subspace for all primes p dividing N. This will imply that T_q preserves the p-new subspace for all primes p, q dividing N. As before, we compare w_N with the corresponding operator at level N/p, namely $w_{N/p}$.

$$\begin{aligned} w_N(i_{1,p}f)(z) &= N^{k-1}(Nz)^{-k} f\left(-\frac{1}{Nz}\right) \\ &= p^{k-1}\underbrace{\left(\frac{N}{p}\right)^{k-1}\left(\frac{N}{p}pz\right)^{-k} f\left(-\frac{1}{\frac{N}{p}pz}\right)}_{=w_{N/p}(f)(pz)} \\ &= p^{k-1} i_{2,p}(w_{N/p}f)(z). \end{aligned}$$

On the other hand

$$\begin{aligned} w_N(i_{2,p}f)(z) &= N^{k-1}(Nz)^{-k} f\left(-\frac{p}{Nz}\right) \\ &= p^{-1} \underbrace{\left(\frac{N}{p}\right)^{k-1} \left(\frac{N}{p}z\right)^{-k} f\left(-\frac{1}{\frac{N}{p}z}\right)}_{=w_{N/p}(f)(z)} \\ &= p^{-1} i_{1,p}(w_{N/p}f)(z). \end{aligned}$$

This finishes the proof. □

Remarks. (i) We have $w_N^* = -w_N$. So w_N^* preserves old subspaces and w_N preserves new ones.

(ii) See also proposition 5.6.2 in Diamond & Shurman for the above proof, but note that their $i_{2,p}$ is not defined as in this lecture. Theirs is given by $f \mapsto f|_k\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$, which is p^{k-1} times the $i_{2,p}$ defined in this course.

(iii) w_N does not preserve character subspaces: w_N maps $S_k(\Gamma_1(N), \chi)$ to $S_k(\Gamma_1(N), \overline{\chi})$. Moreover, note that $\overline{\chi} = \chi^{-1}$.

Proposition 2.10.3. *Let χ be a primitive character mod N. Then*

$$S_k(\Gamma_1(N), \chi) \subseteq S_k(\Gamma_1(N))_{new}.$$

Proof. The action of the $\langle d \rangle$'s on $S_k(\Gamma_1(N/p))$, p dividing N, must factor through $(\mathbb{Z}/(N/p)\mathbb{Z})^\times$. The maps $i_{1,p}$ and $i_{2,p}$ commute with the $\langle d \rangle$'s, so any $\langle d \rangle$ eigenvector in an old subspace must have a character factoring through $\mathbb{Z}/(N/p)\mathbb{Z}$ for some p. Thus it will not be primitive. □

The converse is not true: In general, it is not possible to tell from its character whether a modular form is new. For example the form in $S_8(\Gamma_0(2))$ from sheet 3 is oviously new. Note that the same example also shows that new and old subspaces aren't preserved by multiplication.

Proposition 2.10.4 (An alternative definition of the new subspace)**.** *For p being a prime dividing N we define maps*

$$\begin{aligned} \mathrm{tr}_{1,p} &\colon M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N/p)),\ f \mapsto \frac{1}{\delta}\sum_{i=1}^{\delta} f|_k\gamma_i, \\ \mathrm{tr}_{2,p} &\colon M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N/p)),\ f \mapsto p\ \left(w_{N/p}^{-1} \circ \mathrm{tr}_{1,p} \circ w_N\right)(f), \end{aligned}$$

where $\delta = [\Gamma_1(N/p) : \Gamma_1(N)]$ and $\gamma_1, \ldots, \gamma_\delta$ such that $\Gamma_1(N/p) = \bigsqcup_{i=1}^{\delta} \Gamma_1(N)\gamma_i$. We then have $\mathrm{tr}_{1,p} \circ i_{1,p} = \mathrm{id}$, $\mathrm{tr}_{2,p} \circ i_{2,p} = \mathrm{id}$ and

$$S_k(\Gamma_1(N))_{p\text{-}new} = \ker(\mathrm{tr}_{1,p}) \cap \ker(\mathrm{tr}_{2,p}).$$

Note that we can see $\delta \operatorname{tr}_{1,p}$ as the element $[\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\Gamma_1(N/p)]$ in $\mathcal{R}(\Gamma_1(N), \Gamma_1(N/p))$.

Proof. We have for $f \in S_k(\Gamma_1(N/p))$ and $g \in S_k(\Gamma_1(N))$ that

$$\langle i_{1,p}(f), g\rangle_{\Gamma_1(N)} = \delta\langle f, \operatorname{tr}_{1,p}(g)\rangle_{\Gamma_1(N/p)},$$

so the kernel of $\operatorname{tr}_{1,p}$ is the orthogonal complement of the image of $i_{1,p}$. Similarly

$$\begin{aligned}
\langle i_{2,p}(f), g\rangle_{\Gamma_1(N)} &= \langle p^{-1} w_N^{-1}(i_{1,p}(w_{N/p}f)), g\rangle_{\Gamma_1(N)} \\
&= p^{-1}\ \langle w_N^{*}(i_{1,p}(w_{N/p}f)), g\rangle_{\Gamma_1(N)} \\
&= p^{-1}\ \langle i_{1,p}(w_{N/p}f), w_N g\rangle_{\Gamma_1(N)} \\
&= p^{-1}\delta\ \langle w_{N/p}f, \operatorname{tr}_{1,p}(w_N g)\rangle_{\Gamma_1(N/p)} \\
&= p^{-1}\delta\ \langle f, w_{N/p}^{-1}(\operatorname{tr}_{1,p}(w_N g))\rangle_{\Gamma_1(N/p)} \\
&= p^{-2}\delta\ \langle f, \operatorname{tr}_{2,p}(g)\rangle_{\Gamma_1(N/p)}.
\end{aligned}$$

where λ is just a scalar. So the kernel of $\operatorname{tr}_{2,p}$ is the orthogonal complement of the image of $i_{2,p}$. Note that this proof needs minor modifications in the case of N/p being 1 or 2, since then $[\Gamma_1(N/p) : \Gamma_1(N)] \neq [\overline{\Gamma_1(N/p)} : \overline{\Gamma_1(N)}]$. In this case $\delta/2$ comes out rather than δ. □

It is an amusing fact, that this definition of "new" and "old" works also for Eisenstein series, but there is an Eisenstein series of level 6 which is new and old simultaneously.

Definition 2.10.5. A normalised eigenform in $S_k(\Gamma_1(N))_{\text{new}}$ is called a **primitive form**.

Example. Δ and the weight 8 modular form from sheet 3 are primitive forms.

Theorem 2.10.6 (Strong Multiplicity One)**.**

(a) For any $N \geq 1$, $S_k(\Gamma_1(N))_{new}$ has a basis of primitive forms.

(b) If $f \in S_k(\Gamma_1(N))_{new}$ is an eigenvector for all T_l with l not dividing N, then f is a scalar multiple of a primitive form.

(c) If $f \in S_k(\Gamma_1(N))$ and $g \in S_k(\Gamma_1(M))$ are primtive forms with $a_l(f) = a_l(g)$ for all but finitely many primes l, then $N = M$ and $f = g$.

We are not going to proof this theorem in the lecture. There is a nearly (but not quite) complete proof in Diamond & Shuman and a different one in Miyake. For a full proof see the paper of Atkin & Lehner, 1970.

Proposition 2.10.7. *For M dividing N and $f \in S_k(\Gamma_1(M))$ being a primitive form, define $S_k(\Gamma_1(N))[f]$ as the subspace of $S_k(\Gamma_1(M))$ spanned by all modular forms $f(dz)$ for some d dividing N/M. Then*

$$S_k(\Gamma_1(N)) = \bigoplus_{\substack{f \text{ primitive of} \\ \text{level dividing } N}} S_k(\Gamma_1(N))[f].$$

Moreover, a form $g \in S_k(\Gamma_1(N))$ is an eigenvalue for T_l for all l not dividing N if and only if it lies in one of the subspaces $S_k(\Gamma_1(N))[f]$.

Proof. We have seen that $S_k(\Gamma_1(N))_{\text{new}}$ has a basis of primitive forms. By induction on the number of divisors of N, the subspaces $S_K(\Gamma_1(N))[f]$ span $S_k(\Gamma_1(N))$.

Suppose the sum is not a direct sum. Then there is a nontrivial linear relation

$$\sum_{i,j} c_{i,j} f_i(d_{i,j} z) = 0$$

with scalars $c_{i,j}$, primitive forms f_i and factors $d_{i,j}$ dividing $N/\text{level}(f_i)$. We can suppose without loss of generality that this relation has the least possible number of nonzero $c_{i,j}$'s. Then all the f_i's such that $c_{i,j} \neq 0$ must have the same T_l eigenvalue for all l not dividing N, since otherwise apllying $T_l - \lambda$ for some λ would give a relation with fewer terms. Hence all the f_i's with $c_{i,j} \neq 0$ for some j have some T_l eigenvalue for all l not dividing N and thus they are equal by the Strong Multiplicity One theorem. So any linear relation between vectors in

$$\sum_{\substack{f \text{ primitive of} \\ \text{level dividing } N}} S_k(\Gamma_1(N))[f]$$

comes from a relation in $S_k(\Gamma_1(N))[f]$ for a single f. Hence the sum is direct.

Note that this also shows that the vectors $\{f(dz)\colon d \text{ dividing } N/\text{level}(f)\}$ are linearly independent. So the set

$$\{f(dz)\colon f \text{ primitive of level } N, d \text{ dividing } N/\text{level}(f)\}$$

is a basis. So it remains to show that any $g \in S_k(\Gamma_1(N))$ being an eigenvector for all T_l, l not dividing N, is in $S_k(\Gamma_1(N))[f]$ for some f. Suppose g is such an eigenvector for all T_l, l not dividing N. We can write $g = \sum_{i=1}^m \mu_i g_i$ with $g_i \in S_k(\Gamma_1(N))[f_i]$ for some f_i. If $T_l g = \alpha g$ then

$$0 = (T_l - \alpha)(g) = \sum_{i=1}^m \mu_i (T_l - \alpha)(g_i).$$

Since vectors in subspaces $S_k(\Gamma_1(N))[f]$ for distinct f's are linearly independent, all the vectors $(T_l - \alpha)(g_i)$ are zero. Since this holds for all l not dividing N, the Strong Multiplicity One theorem implies there is at most one nonzero μ_i, so $g = \mu_i g_i \in S_k(\Gamma_1(N))[f_i]$. Hence we are done. □

3 Miscellany

3.1 Riemann surfaces

A **Riemann surface** is a topological space X together with a countable open cover $(U_i)_{i\in I}$ of X and homeomorphisms $U_i \to V_i$ for all $i \in I$, where V_i are open subsets of $\mathbb{C}$ such that for all $U_i \cap U_j \neq \emptyset$ the map on the overlap is holomorphic. In this context the map on the overlap for $\varphi\colon U_\varphi \to V_\varphi$ and $\psi\colon U_\psi \to V_\psi$ with $U_\varphi \cap U_\psi \neq \emptyset$ is given by

$$\psi \circ \varphi^{-1}\colon \varphi(U_\varphi \cap U_\psi) \to \psi(U_\varphi \cap U_\psi).$$

The point of doing this is that we can make sense of the question when mappings $X \to Y$ between Riemann surfaces are holomorhpic: We just have to locally look at functions between coordinate charts in $\mathbb{C}$, and the overlap condition means this is independent of any choices.

Example. (i) Clearly $\mathbb{C}$ itselft is a Riemann surface.

(ii) The complex projective line $\mathbb{P}^1_{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, also called the **Riemann sphere**, is a Riemann surface. Here we have two coordinate charts, the natural inclusion $\mathbb{C} \hookrightarrow \mathbb{P}^1_{\mathbb{C}}$ and the map $\varphi\colon \mathbb{C} \to \mathbb{P}^1_{\mathbb{C}}$ with $\varphi(z) = 1/z$ for $z \neq 0$ and $\varphi(0) = \infty$. In this case the overlap map is $z \mapsto 1/z$ on $\mathbb{C} \setminus \{0\}$.

Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$. Then $Y(\Gamma) := \Gamma\backslash\mathcal{H}$ is naturally a Riemann surface. To see this consider $z \in \mathbb{C}$ such that $\mathrm{stab}_\Gamma(z) = \{1\}$. We can find a neighbourhood of z such that $U \to \Gamma\backslash\mathcal{H}$ is an injection and this gives a coordinate chart. Moreover, it can be shown that we can also deal with elliptic points. So $Y(\Gamma)$ is indeed a Riemann surface and $\mathcal{H} \to Y(\Gamma)$ is holomorphic.

Proposition. *If Γ is of finite index in $\mathrm{SL}_2(\mathbb{Z})$ we can define*

$$X(\Gamma) := Y(\Gamma) \cup C(\Gamma) = \Gamma\backslash(\mathcal{H} \cup \mathbb{P}^1_{\mathbb{Q}}).$$

This is a Riemann surface extending $Y(\Gamma)$. Moreover, $X(\Gamma)$ is compact.

Example. Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. The function $j = E_4^3/\Delta$ gives a bijection $Y(\Gamma) \to \mathbb{C}$, which can easily be extended to $X(\Gamma)$ mapping the cusp at ∞ to $\infty \in \mathbb{P}^1_{\mathbb{C}}$.Hence we have $X(\mathrm{SL}_2(\mathbb{Z})) \cong \mathbb{P}^1_{\mathbb{C}}$.

Note that, for general Γ of finite index, $X(\Gamma)$ has holes. The number of these holes is called the genius. The classical theory (Riemann-Roch) uses this to get exact formulae for the dimension of $S_k(\Gamma)$. For example the dimension of $S_2(\Gamma)$ is given by the genius of $X(\Gamma)$.

3.2 Modular forms and elliptic curves

There are two connections between modular forms and elliptic curves: An elementary one and a much harder one. We will briefly discuss both in the following.

An elementary approach

Points of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ have a one to one correspondance to lattices $\Lambda \subseteq \mathbb{C}$ up to homothety, which have a one to one correspondance to isomorphism classes of elliptic curves over $\mathbb{C}$. So weight 0 modular forms are functions on the set of elliptic curves. For example $j = E_4^3/\Delta$ is the j-invariant of elliptic curve theory.

More general, quotients $\Gamma\backslash\mathcal{H}$ have a one to one correspondance to elliptic curves with additional data. For example $\Gamma_1(N)\backslash\mathcal{H}$ corresponds to elliptic curves with a choice of a N-torsion point. One can show that $X_1(N)$, the Riemann surface attached to $\Gamma_1(N)$, is (in a canonical way) the set of $\mathbb{C}$-points of an algebraic curve over $\mathbb{Q}$.

Modular forms of weight k turn out to be functions on pairs

$$(E, \text{choice of Weierstrass equation for } E).$$

These modular forms scale by λ^k when we change the Weierstrass equation by λ, so when we replace $y^2 = x^3 + ax + b$ by $y^2 = x^3 + a\lambda^4 x + b\lambda^6$. For example $E \mapsto a$ is a modular form of weight 4. Hence it is E_4 up to a constant depending on normalization.

Similarly, modular forms of level k and level $\Gamma_1(N)$ are functions on triples

$$(E, P, \text{choice of Weierstrass equation for } E),$$

where P is the exact order of N. This purely algebraic approach allows us to define algebraically modular forms with coefficients in $\mathbb{Z}$.

A more advanced connection

Let E be an elliptic curve over $\mathbb{Q}$. We say E is **modular** if there is a non-constant holomorphic map $X_0(N) \to E(\mathbb{C})$ for some N.

Theorem (Weil, Marin)**.** *Let E be the elliptic curve given by $y^2 = x^3 + ax + b$. If E is modular, then there is a holomorphic differential on $X_0(N)$ which is the pullback of $\frac{dx}{y}$. This is the image $f(z)dz$ for some $f \in S_2(\Gamma_0(N))$. Moreover*

- *f is a scalar multiple of a primitive form,*
- *$a_p(f) = p + 1 - |E(\mathbb{F}_p)|$ for all p not dividing N, and*
- *every primitive form in $S_2(\Gamma_0(N))$ with rational q-expansion arises in this way.*

Theorem (Breuil, Conrad, Diamond and Taylor; 2001)**.** *Every elliptic curve over $\mathbb{Q}$ is modular.*

More precisely, this theorem is an extension of an earlier result due to Wiles which only apllied to elliptic curves whose bad primes weren't too bad.

These two theorems connect modular forms and elliptic curves in a new way, which can for example be used to efficiently compute elliptic curves since it is not too hard to compute modular forms. Morover, modularity gives powerful theoretical tools to attack for example the Birch and Swinnerton-Dyer conjecture.

3.3 Theta functions and quadratic forms

A **quadratic form** over $\mathbb{Z}$ in n variables is a homogeneous polynomial of degree 2 with coefficients in $\mathbb{Z}$, for example $x^2 + 3xy - z^2 + w^2$. We say a quadratic form Q is **even** if all its coefficients are even. Then we can write $Q(x) = x^T Ax$, where A is a symmetric integer matrix with even entries on the diagonal. Moreover, we say a quadratic form Q is positive definite if $Q(x) \geq 0$ and $Q(x) = 0$ if and only if $x = 0$.

Let Q be a quadratic form. If Q is positive definite then the number of vectors x such that $Q(x) = N$ is finite for all N, and we can define

$$\Theta_Q(z) = \sum_{x \in \mathbb{Z}^n} e^{2\pi i Q(x) z}.$$

This definition is independent of the choice of basis and Θ_Q is a power series in $e^{2\pi iz}$ if Q is even.

Theorem (Hecke)**.** *If n is even and Q is an even, positive definite quadratic form in n variables, then $\Theta_Q \in M_k(\Gamma_1(N))$ where $k = n/2$ and N is the determinant of the matrix corresponding to Q.*

We can use this theorem to understand quadratic forms. For instance J. H. Conway constructed a very large finite simple group by taking the automorphism group of a lattice constructed using modular forms.

In general, Θ-series don't tend to be Hecke eigenforms, but we can construct these using Θ-series: Let K be an imaginary quadratic field. Then $\mathcal{O}_k \cong \mathbb{Z}^2$ and $x \mapsto 2N_{K/\mathbb{Q}}(x)$ is an even, positive definite quadratic form. Similarly, any ideal in $\mathcal{O}_k$ gives a quadratic form. Hence we have a map from the ideal classes in K to modular forms of weight 1. If $\eta\colon \mathfrak{a}(K) \to \mathbb{C}^\times$, where $\mathfrak{a}$ is a character, then

$$\sum_{I \in \mathfrak{a}(K)} \eta(I)\Theta(I)$$

is a Hecke eigenform. Here $\Theta(I)$ represents the Θ-function which is attached to I.

3.4 Galois representations

Let K be a number field. For L being a finite normal extension of K we have a Galois group $\mathrm{Gal}(L/K)$. If we let L vary over all finite normal extensions of K, we can define the **absolute Galois group**

$$\mathrm{Gal}\left(\overline{K}/K\right) = \varprojlim_{L} \mathrm{Gal}(L/K).$$

This has a topology (the Krull topology) with respect to which open neighbourhoods of 1 are sets acting trivially on L for some finite extension L/K.

Galois representations are actions of $\mathrm{Gal}(\overline{K}/K)$ on finite-dimensional vector spaces over some field E by linear operators such that the resulting map $\mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(E)$ is continuous. If E is $\mathbb{C}$, the image of $\mathrm{Gal}(\overline{K}/K)$ must be finite, but if E is some $\mathbb{Q}_p$ there are a lot more representations. For instance, we can construct a 1-dimensional representation as follows:

Let $n \geq 0$ and ζ be a primitive p^n-th root of unity. Any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sends ζ to ζ^a for some $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and a is independent of the choice of ζ. These are compatible under reduction

$$(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times,$$

so we get elements of $(\mathbb{Z}/p\mathbb{Z})^\times$. Hence we have constructed a map

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{GL}_1(\mathbb{Q}_p).$$

It is called the cyclotomic character. Similarly, let E be an elliptic curve over $\mathbb{Q}$. Then $E[p^n] \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[p^n]$ by automorphisms. So we get a canonical map

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{Aut}_{\mathbb{Z}/p\mathbb{Z}}\left(E\left[p^n\right]\right).$$

Taking inverse limits we can define an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on

$$T_pE = \varprojlim_{n} E[p^n].$$

T_pE knows a lot about E. For example the order of $E(\mathbb{F}_l)$, l being any prime of good reduction different from p, is related to the trace of a special element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, namely the Frobenius at l.

Theorem. *Let f be a primitive eigenform in $S_k(\Gamma_1(N))$ for some N and k. For any prime p there are p-adic Galois representations*

$$\rho_{f,p}\colon\ \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{GL}_2\left(\overline{\mathbb{Q}_p}\right)$$

such that for all l not dividing Np

$$\mathrm{trace}\left(p_{f,p}(\mathit{Frob}_l)\right) = a_l(f).$$

Moreover, $\rho_{f,p}$ has the following properties:

- It is irreducible,
- complex conjugation acts as $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ in some basis (so $\rho_{f,p}$ is odd),

- the inertia subgroup $I_l \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts trivially for all but finitely many l (so $\rho_{f,p}$ is unramified almost everywhere), and
- $\rho_{f,p}$ is "potentially semistable" (technical to define).

Open conjecture (Fontaine-Mazur)**.** *All 2-dimensional p-adic Galois representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *satisfying these conditions arise from modular forms.*

This is known under very mild hypotheses by theorems of Kisin and Emerton. In particular, the conjecture implies the modularity theorem of Breuil, Conrad, Diamond and Taylor as stated in Section 3.2.