# Modular Forms

Robert Kurinczuk

Autumn 2017

# Contents


**1 Introduction** **4**

1.1 What are modular forms and why study them? . . . . . 4

1.2 Sources . . . . . 6

1.3 Acknowledgements . . . . . 6

**2 Modular forms of level one** **7**

2.1 Modular functions and forms . . . . . 7

2.1.1 The action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$ . . . . . 7

2.1.2 Modular functions and modular forms . . . . . 8

2.1.3 Lattice functions and modular forms . . . . . 10

2.1.4 Eisenstein series . . . . . 12

2.1.5 Eisenstein series in weight 2 and the product expansion of $\Delta$ . . . . . 17

2.2 How many modular forms are there? . . . . . 18

2.2.1 A fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ acting on $\mathbb{H}$ . . . . . 18

2.2.2 Zeroes of modular forms . . . . . 21

2.2.3 Dimensions of spaces of modular forms . . . . . 23

2.2.4 Modular functions and the $j$-invariant . . . . . 26

2.3 Hecke operators . . . . . 27

2.3.1 Motivation . . . . . 27

2.3.2 Correspondences on $\mathrm{Latt}_{\mathbb{C}}$ . . . . . 28

2.3.3 Lattice functions and Hecke operators . . . . . 31

2.3.4 Hecke operators . . . . . 32

2.3.5 Eigenforms . . . . . 33

2.4 The $L$-function of a modular form . . . . . 35

2.4.1 The Riemann zeta function and Dirichlet $L$-functions . . . 35
2.4.2 The $L$-function of a modular form . . . 37
2.5 Theta series and quadratic forms . . . 40
2.5.1 Quadratic forms . . . 40
2.5.2 Lattices and associated quadratic forms . . . 40
2.5.3 Theta series . . . 42

**3 Modular forms of higher level** **45**
3.1 Modular forms for congruence subgroups . . . 45
3.1.1 Congruence subgroups . . . 45
3.1.2 Modular forms for congruence subgroups . . . 47
3.1.3 Fundamental domains for congruence subgroups . . . 48
3.1.4 Finite dimensional spaces of modular forms . . . 51
3.2 Hecke operators in higher level . . . 53
3.2.1 Double coset operators and Hecke operators . . . 53
3.2.2 Diamond operators . . . 55
3.2.3 Hecke operators commute . . . 56
3.3 Bases of eigenforms . . . 58
3.3.1 The Petersson inner product . . . 58
3.3.2 Adjoints of Hecke operators and eigenforms . . . 61
3.4 Oldforms and newforms . . . 64

**A Complex Analysis** **66**
A.1 Holomorphic and meromorphic functions . . . 66
A.2 A trigonometric identity . . . 67

**B Group Theory** **68**
B.1 Structure of abelian groups . . . 68
B.2 Double cosets . . . 68

**C Spectral Theory** **69**
C.1 Hermitian inner products and the Spectral Theorem . . . 69

# Chapter 1

# Introduction

## 1.1 What are modular forms and why study them?

Let $\mathbb{H}$ denote the complex upper half plane

$$\mathbb{H} := \{z \in \mathbb{C} : \operatorname{Im}(z) > 0\}.$$

A *modular form* is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying a growth property and strong symmetrical properties. In particular, these imply that $f$ has a Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a_n q^n.$$

where $q = e^{2\pi i z}$. As we shall illustrate in the course, the sequence $a_n$ can encode deep arithmetic information.

As an example, it turns out that the function

$$\begin{aligned} f(z) &= q \prod_{n \geqslant 1} (1 - q^n)^2 (1 - q^{11n})^2 \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 + \cdots \\ &= \sum_{n=1}^{\infty} a_n(f) q^n \end{aligned}$$

is (non-obviously) a modular form, more precisely it is a *cusp form of weight 2 and level 11.*

On the other hand, let

$$E : y^2 + y = x^3 - x^2 - 10x - 20.$$

Then $E$ is an example of an elliptic curve over $\mathbb{Q}$. Let's count $\sharp E(\mathbb{Z}/p\mathbb{Z})$, noting we always include the *point at infinity* $0$, we have:

| $p$ | $E(\mathbb{Z}/p\mathbb{Z})$ | | | | | $\sharp E(\mathbb{Z}/p\mathbb{Z})$ |
|---|---|---|---|---|---|---|
| 2 | $(0,0)$, | $(0,1)$, | $(1,0)$, | $(1,1)$, | $0$ | 5 |
| 3 | $(1,0)$, | $(1,-1)$, | $(-1,0)$, | $(-1,-1)$, | $0$ | 5 |
| 5 | $(0,0)$, | $(0,-1)$, | $(1,0)$, | $(-1,-1)$, | $0$ | 5 |
| 7 | $(1,3)$, | $(2,2)$, | $(2,-3)$, | $(-1,1)$, | $(-1,-2)$, | 10 |
| | $(-2,1)$, | $(-2,-2)$, | $(-3,1)$, | $(-3,-2)$, | $0$ | |

**Amazing fact:** For $p \neq 11$ prime,

$$\sharp E(\mathbb{Z}/p\mathbb{Z}) = 1 + p - a_p(f).$$

For primes not equal to 11, the number of points in $E(\mathbb{Z}/p\mathbb{Z})$ is given by the Fourier coefficients of the modular form $f$, and we call the elliptic curve $E$ *modular*.

The following theorem is one of the triumphs of recent mathematics:

**The Modularity Theorem** (Wiles, Taylor, Diamond, Conrad, Breuil)**.** All elliptic curves over $\mathbb{Q}$ are modular.

Thanks to earlier work of Frey, Serre, Ribet, et al. this has a famous corollary:

**Fermat's Last Theorem** (Wiles)**.** Let $n \geqslant 3$ and $x, y, z \in \mathbb{Z}$, then

$$x^n + y^n = z^n$$

has no non-trivial solutions.

On the other hand, we can ask which modular forms are related to elliptic curves in this way. This was answered in the 1960's by Eichler–Shimura: these modular forms are the *newforms of weight* 2 *with integral Fourier coefficients.*

We finish this introduction with a quote, usually attributed to Eichler:

> *There are five fundamental operations of arithmetic: addition, subtraction, multiplication, division, and modular forms.*

**Exercise 1.1.1.** (i) Let $p$ be an odd prime. Show that the equation $ax^2 + bx + c = 0$, for $a, b, c \in \mathbb{Z}/p\mathbb{Z}$ with $a \not\equiv 0 \pmod{p}$, has

(a) exactly one solution in $\mathbb{Z}/p\mathbb{Z}$ if $b^2 - 4ac \equiv 0 \pmod{p}$.

(b) two solutions if $b^2 - 4ac$ is a nonzero square mod $p$.

(c) no solutions if $b^2 - 4ac$ is not a square mod $p$.

(ii) Let $P(x) \in \mathbb{Z}[x]$ be a polynomial with integral coefficients. Show that the equation $y^2+y = P(x)$ has exactly

$$p + \sum_{x=0}^{p-1} \left( \frac{1 + 4P(x)}{p} \right)$$

solutions $(x, y)$ in $(\mathbb{Z}/p\mathbb{Z})^2$, where, for $a \in \mathbb{Z}/p\mathbb{Z}$, we define

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p}; \\ 1 & \text{if } a \text{ is a nonzero square mod } p; \\ -1 & \text{if } a \text{ is not a square mod } p. \end{cases}$$

(iii) Let $E : y^2 + y = x^3 - x^2 - 10x - 20$ be the elliptic curve considered above. Compute $\sharp E(\mathbb{Z}/13\mathbb{Z})$ and compare this with the coefficient of $q^{13}$ of the modular form

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

(Working out the coefficient of $q^{13}$ in the series by hand is tricky, feel free to look this up, for example at the *L-functions and modular forms database* `http://www.lmfdb.org`.)

## 1.2 Sources

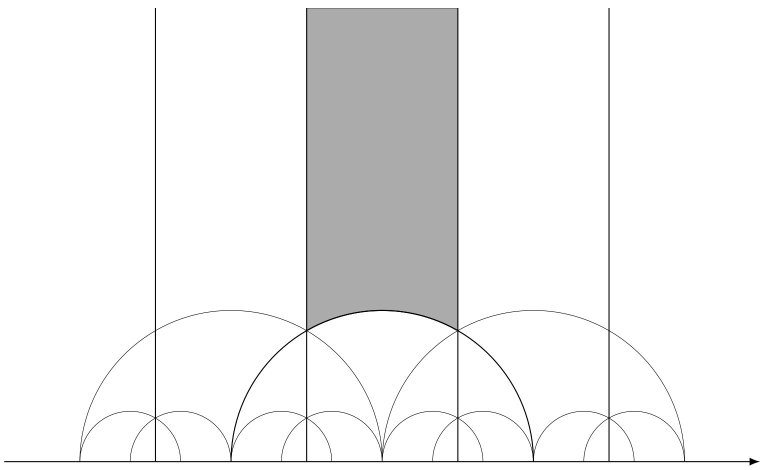
We follow the final chapter of Serre's *A course in arithmetic* [5] to develop modular forms in level one, and supplement this with material on modular forms in higher level, mostly taken from [2, Chapter 5] . We have also used various ideas from [3]. Other classic sources on modular forms are [4, 6].

A short introduction to modular forms aimed at a non-technical audience can be found in [1, Chapter 11 onwards], easy weekend reading!

## 1.3 Acknowledgements

The material covered in the course follows a syllabus carefully crafted by David Helm. I took much inspiration and ideas from handwritten notes taken in his course in the previous year, reused a lot of his exercises and reproduced most of his section on theta series verbatim. I thank David for many useful conversations on the material presented here.

I thank all attendees of the course for interesting suggestions and corrections during and after lectures, and on feedback forms. All of which I have tried to incorporate.



A fundamental domain for the modular group $\mathrm{SL}_2(\mathbb{Z})$ acting on the upper half plane $\mathbb{H}$.

# Chapter 2

# Modular forms of level one

## 2.1 Modular functions and forms

Modular forms are holomorphic functions which transform in a specified way under the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane $\mathbb{H}$, and satisfy a growth property. We begin by defining this action of $\mathrm{SL}_2(\mathbb{Z})$.

### 2.1.1 The action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$

The elements of $\mathrm{GL}_2(\mathbb{R})$ act as automorphisms of the extended complex plane $\mathbb{C} \cup \{\infty\}$ via, for $\gamma \in \mathrm{GL}_2(\mathbb{R})$ and $z \in \mathbb{C} \cup \{\infty\}$,

$$\gamma \cdot z = \frac{az+b}{cz+d}, \qquad \text{if } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where we interpret this definition if $c \neq 0$ as $\gamma \cdot (-d/c) = \infty$, $\gamma \cdot \infty = \frac{a}{c}$, and if $c = 0$ as $\gamma \cdot \infty = \infty$. Put

$$\mathrm{GL}_2(\mathbb{R})^+ := \{g \in \mathrm{GL}_2(\mathbb{R}) : \det(g) > 0\}.$$

**Lemma 2.1.1.** Let $\gamma \in \mathrm{GL}_2(\mathbb{R})$, then

$$\mathrm{Im}(\gamma \cdot z) = \det(\gamma) \frac{\mathrm{Im}(z)}{|cz+d|^2}.$$

and $\mathrm{GL}_2(\mathbb{R})^+$ preserves the upper half plane $\mathbb{H}$.

*Proof.* For $z \in \mathbb{C}$, we let $\overline{z}$ denote its complex conjugate. We have

$$\begin{aligned} 2i\mathrm{Im}(\gamma \cdot z) &= \gamma \cdot z - \overline{\gamma \cdot z} \\ &= \frac{az+b}{cz+d} - \frac{a\overline{z}+b}{c\overline{z}+d} \\ &= \frac{(az+b)(c\overline{z}+d) - (a\overline{z}+b)(cz+d)}{(cz+d)(c\overline{z}+d)} \\ &= \frac{ad(z-\overline{z}) - bc(z-\overline{z})}{|cz+d|^2} \\ &= \frac{2i\det(\gamma)\mathrm{Im}(z)}{|cz+d|^2}. \end{aligned}$$

Dividing by $2i$, we are done. □

In particular, $\mathrm{SL}_2(\mathbb{R})$ acts on the upper half plane $\mathbb{H}$. Notice that, $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ acts trivially on $\mathbb{H}$, so one can consider the action of $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ (which acts faithfully on $\mathbb{H}$). This is what Serre [5] does, however we stick with $\mathrm{SL}_2(\mathbb{R})$.

Given $z \in \mathbb{H}$, $z = x + iy$ we have

$$\begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & \sqrt{y}^{-1} \end{pmatrix} \cdot i = \frac{\sqrt{y}i + x/\sqrt{y}}{\sqrt{y}^{-1}} = x + iy = z,$$

hence $\mathrm{SL}_2(\mathbb{R})$ acts transitively on $\mathbb{H}$. The set of elements in $\mathrm{SL}_2(\mathbb{R})$ which fix $i$ is given by

$$\begin{aligned} \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{R})}(i) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) : \frac{ai+b}{ci+d} = i \right\}; \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) : ai + b = -c + di \right\}; \\ &= \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \right\} = \mathrm{SO}_2(\mathbb{R}). \end{aligned}$$

**Remark 2.1.2.** This shows that the map

$$\begin{aligned} \mathrm{SL}_2(\mathbb{R})/\,\mathrm{SO}_2(\mathbb{R}) &\to \mathbb{H} \\ \gamma &\mapsto \gamma \cdot i \end{aligned}$$

is a bijection.

### 2.1.2 Modular functions and modular forms

We now define modular forms together with the weaker notions of weakly modular functions and modular functions. Throughout $k$ will denote an integer.

**Definition 2.1.3.** A *weakly modular function of weight k and level one* is a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ such that for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $f$ satisfies the *modular transformation law*

$$f(\gamma \cdot z) = (cz + d)^k f(z). \tag{$\star$}$$

Let $f$ be a weakly modular function of weight $k$ and level one. Let's make some observations about $f$ implied by the modular transformation law. In particular, taking $\gamma = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ we have

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

Hence, if $f$ is not identically zero, then $k$ is even; and there are no non-zero weakly modular functions of level one and odd weight. Now set $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, for all $z \in \mathbb{H}$, we have

$$f(z + 1) = f(z), \tag{1}$$

and $f$ is periodic. Finally, set $\gamma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, for all $z \in \mathbb{H}$, we have

$$f(-z^{-1}) = z^k f(z). \tag{2}$$

We will see later that (1) and (2) together are equivalent for level one weakly modular functions to the modular transformation law ($\star$) for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

For $z \in \mathbb{C}$, put $q = e^{2\pi i z}$. Then $z \in \mathbb{H}$ if and only if $0 < |q| < 1$, as $|e^{2\pi i z}| = e^{\mathbf{Re}(2\pi i z)}$. Let

$$\mathbb{D}^* = \{z \in \mathbb{C} : 0 < |z| < 1\},$$

denote the punctured unit disc. The condition $f(z) = f(z+1)$ implies that there exists a meromorphic function $\widetilde{f} : \mathbb{D}^* \to \mathbb{C}$, with

$$\widetilde{f}(q) = f(z),$$

i.e. $\widetilde{f}(q) = f(\log(q)/2\pi i)$, which does not depend on the branch of the complex logarithm as $f(z) = f(z+1)$. We call $f$

(i) *meromorphic at* $\infty$ if $\widetilde{f}$ is meromorphic at 0;

(ii) *holomorphic at* $\infty$ if $\widetilde{f}$ is holomorphic at 0.

Case (i), implies that $\widetilde{f}$ has Laurent series expansion

$$\widetilde{f}(q) = \sum_{n=-N}^{\infty} a(n) q^n,$$

and in Case (ii) we can take $N = 0$.

**Definition 2.1.4.** A *modular function of weight $k$ and level one* is a weakly modular function of weight $k$ (and level 1) which is meromorphic at $\infty$.

A *modular form of weight $k$ and level one* is a modular function of weight $k$, which is holomorphic on $\mathbb{H} \cup \{\infty\}$:

**Definition 2.1.5** (Modular forms of level one)**.** A *modular form of weight $k$ and level one* is a function $f : \mathbb{H} \to \mathbb{C}$ satisfying the following properties:

(i) $f$ is holomorphic on $\mathbb{H}$;

(ii) $f(\gamma \cdot z) = (cz+d)^k f(z)$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ (*the modular transformation law*);

(iii) $f$ is holomorphic at $\infty$.

The *$q$-expansion* of a modular form $f : \mathbb{H} \to \mathbb{C}$ is, the power series expansion of $\widetilde{f}$,

$$f(z) = \sum_{n=0}^{\infty} a(n) q^n.$$

A modular form whose $q$-expansion starts with $a(0) = 0$ is called a *cusp form.*

We make the convention that we do not write the level of a (weakly) modular function/form if it is of level one. In this chapter, all modular functions considered will be level one.

**Example 2.1.6.** Let

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

Then $\Delta$ is (non-obviously) a cusp form of weight 12. This example is particularly important, and we will study it in detail later.

**Definition 2.1.7.** Define

$$M_k = \{\text{modular forms of weight } k\};$$
$$S_k = \{\text{cusp forms of weight } k\}.$$

Given $f, g \in M_k$, it is easy to see $f + g \in M_k$. Moreover, directly from the definitions, we have:

**Lemma 2.1.8.** Let $k, l \in \mathbb{Z}$.

(i) $M_k, S_k$ are $\mathbb{C}$-vector spaces.

(ii) If $f \in M_k$ and $g \in M_l$, then $fg \in M_{k+l}$.

### 2.1.3 Lattice functions and modular forms

We now reinterpret the modular transformation law in terms of *lattice functions*, this will lead to our first interesting examples of modular forms.

**Definition 2.1.9.** A lattice in $\mathbb{C}$ is a subgroup of the form

$$L_{v_1,v_2} = \mathbb{Z}v_1 + \mathbb{Z}v_2.$$

where $v_1, v_2 \in \mathbb{C}$ are $\mathbb{R}$-linearly independent vectors. Let

$$\mathrm{Latt}_{\mathbb{C}} = \{\text{lattices in } \mathbb{C}\} = \{L_{v_1,v_2} : v_1, v_2 \text{ are linearly independent}\}.$$

**Lemma 2.1.10.** We have $L_{v_1,v_2} = L_{v_1',v_2'}$ if and only if there exists $a, b, c, d \in \mathbb{Z}$ such that $v_1' = av_1 + bv_2$ and $v_2' = cv_1 + dv_2$ with $ad - bc = \pm 1$, i.e. $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$.

*Proof.* If $L_{v_1,v_2} = L_{v_1',v_2'}$, then we can find $a, b, c, d, a', b', c', d' \in \mathbb{Z}$ such that

$$\begin{pmatrix} v_1' \\ v_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$
$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} v_1' \\ v_2' \end{pmatrix}.$$

Hence

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix},$$

Hence $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ and $\det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \pm 1$.

If

$$\begin{pmatrix} v_1' \\ v_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

then $L_{v_1',v_2'} \subseteq L_{v_1,v_2}$. As $\det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \pm 1$, we can invert $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and use the new matrix to show that $L_{v_1,v_2} \subseteq L_{v_1',v_2'}$. □

Let $L_{v_1,v_2} \in \mathrm{Latt}_{\mathbb{C}}$. Then either $\mathrm{Im}(v_1/v_2) > 0$ or $\mathrm{Im}(v_2/v_1) > 0$, as $\{v_1, v_2\}$ form a $\mathbb{R}$-basis of $\mathbb{C}$. In the second case, $L_{v_2,v_1}$ defines the same lattice. Therefore, every lattice in $\mathrm{Latt}_{\mathbb{C}}$ can be written as $L_{v_1,v_2}$ with $\mathrm{Im}(v_1/v_2) > 0$. We assume until the end of the section that $\mathrm{Im}(v_1/v_2) > 0$.

If $L \in \mathrm{Latt}_{\mathbb{C}}$ and $\lambda \in \mathbb{C}^\times$, then

$$\lambda L = \{\lambda z : z \in L\} \in \mathrm{Latt}_{\mathbb{C}},$$

this is called *homothety.* We have

$$L_{v_1,v_2} = v_2 L_{v_1/v_2,1}.$$

Hence we have a map

$$\begin{aligned}\mathbb{H} &\to \mathrm{Latt}_{\mathbb{C}},\\ z &\mapsto L_{z,1}\end{aligned}$$

which induces a surjective map onto homothety classes of lattices.

**Lemma 2.1.11.** Let $z_1, z_2 \in \mathbb{H}$. Then $L_{z_1,1} = \lambda L_{z_2,1}$ for some $\lambda \in \mathbb{C}^\times$ if and only if there exists $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$z_1 = \gamma \cdot z_2 = \frac{az_2 + b}{cz_2 + d}.$$

Moreover, $L_{\gamma \cdot z,1} = (cz + d)^{-1} L_{z,1}$.

*Proof.* Suppose $L_{z_1,1} = \lambda L_{z_2,1}$ for some $\lambda \in \mathbb{C}^\times$. By Lemma 2.1.10, there exists $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z_1 \\ 1 \end{pmatrix} = \lambda \begin{pmatrix} z_2 \\ 1 \end{pmatrix}.$$

We have the equations

$$az_1 + b = \lambda z_2, \quad \text{and} \quad cz_1 + d = \lambda,$$

implying

$$z_2 = \frac{az_1 + b}{cz_1 + d}.$$

Put $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. We need to show $\det(\gamma) = 1$. By Lemma 2.1.1,

$$\det(\gamma) \frac{\mathrm{Im}(z_1)}{|cz_1 + d|^2} = \mathrm{Im}(\gamma \cdot z_1) = \mathrm{Im}(z_2).$$

However, $\mathrm{Im}(z_2) > 0$ and $\mathrm{Im}(z_2) > 0$, which implies $\det(\gamma) > 0$ and hence equal to 1.

Conversely, if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$z_1 = \gamma \cdot z_2 = \frac{az_2 + b}{cz_2 + d}.$$

Then

$$L_{z_1,1} = L_{\gamma \cdot z_2,1} = L_{\frac{az_2+b}{cz_2+d},1} = (cz_2 + d)^{-1} L_{az_2+b, cz_2+d} = (cz_2 + d)^{-1} L_{z_2,1},$$

the last equality by applying Lemma 2.1.10. □

All in all, Lemma 2.1.11 and the discussion preceding it show:

**Proposition 2.1.12.** The map $\mathbb{H} \to \mathrm{Latt}_{\mathbb{C}}$ given by $z \mapsto L_{z,1}$ induces a bijection between

$$\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H} \leftrightarrow \{\text{Lattices in } \mathbb{C} \text{ up to homothety}\} = \mathrm{Latt}_{\mathbb{C}} / \mathbb{C}^\times.$$

**Definition 2.1.13.** A *lattice function of weight* $k$ is a function $F : \mathrm{Latt}_{\mathbb{C}} \to \mathbb{C}$ such that for all $L \in \mathrm{Latt}_{\mathbb{C}}$, $\lambda \in \mathbb{C}^{\times}$ we have

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

**Lemma 2.1.14.** Let $F : \mathrm{Latt}_{\mathbb{C}} \to \mathbb{C}$ be a lattice function of weight $k$. Then the function $f : \mathbb{H} \to \mathbb{C}$ defined by

$$f(z) = F(L_{z,1}),$$

satisfies the modular transformation law

$$f(\gamma \cdot z) = (cz+d)^k f(z), \tag{$\star$}$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

*Proof.* We have

$$f(\gamma \cdot z) = F(L_{az+b/cz+d,1}) = F((cz+d)^{-1} L_{z,1}) = (cz+d)^k F(L_{z,1}) = (cz+d)^k f(z).$$

□

**Remark 2.1.15.** The map of lemma 2.1.14 taking lattice functions to functions on $\mathbb{H}$ satisfying the modular transformation law ($\star$) is bijective. Therefore, weakly modular functions of weight $k$ identify with certain lattice functions of weight $k$ (a strict subset as we didn't give an analogue of the meromorphy condition for lattice functions).

A general definition of a *lattice* in a $\mathbb{R}$-vector space $V$ is a discrete additive subgroup of $V$ that spans $V$ over $\mathbb{R}$. Recall, a *discrete subset* $L$ of a topological space $V$ is a subset such that for every $p \in L$ there exists an open set $U$ of $V$ such that $U \cap L = \{p\}$.

**Lemma 2.1.16.** Every lattice in a $\mathbb{R}$-vector space $V$ has the form

$$\mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_n$$

for some basis $\{v_1, \ldots, v_n\}$ of $V$.

**Exercise 2.1.17.** Using the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem B.1.2), prove lemma 2.1.16.

**Exercise 2.1.18.** A lattice in $\mathbb{C}$ is said to have *complex multiplication* if there is $\alpha \in \mathbb{C}\backslash\mathbb{Z}$ such that $\alpha L \subseteq L$. Show that the lattice $L_{z,1}$ has complex multiplication if and only if $z$ satisfies a quadratic polynomial with integral coefficients. Show further that if this is the case, then the set of all $\alpha \in \mathbb{C}$ with $\alpha L \subseteq L$ is a subring of the number field $\mathbb{Q}(z)$ that has finite rank as a $\mathbb{Z}$-module.

### 2.1.4 Eisenstein series

Thinking of the modular transformation law in terms of lattice functions, it turns out it is straightforward to write down candidates for modular forms: The function $G_k : \mathrm{Latt}_{\mathbb{C}} \to \mathbb{C}$ given by

$$G_k(L) = \sum_{\omega \in L\backslash\{0\}} \frac{1}{\omega^k}$$

satisfies

$$G_k(\lambda L) = \sum_{\omega \in \lambda L \setminus \{0\}} \frac{1}{\omega^k} = \sum_{\omega \in L \setminus \{0\}} \frac{1}{(\lambda^{-1}\omega)^k} = \lambda^{-k} G_k(L).$$

Hence if we can show the series converges, we will have an example of a lattice function of weight $k$. Notice that, by taking $\lambda = -1$, the function $G_k$ is identically 0 whenever $k$ is odd. We will prove that for $k \geqslant 4$ even, the function on $\mathbb{H}$ given by $G_k$ and Lemma 2.1.14 converges and defines a non-zero modular form. This function on $\mathbb{H}$, which we also denote $G_k$ by an abuse of notation, is defined by

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

and satisfies the modular transformation law ($\star$) by Lemma 2.1.14. The functions $G_k$ are called *Eisenstein series.*

**Theorem 2.1.19.** For $k \geqslant 3$, the series defining $G_k(z)$ converges absolutely to a holomorphic function on $\mathbb{H}$.

*Proof.* The idea is to compare $|mz+n|$ with $\max\{|m|,|n|\}$. There exist constants $C > c > 0$ such that

$$c \max\{|m|,|n|\} \leqslant |mz+n| \leqslant C \max\{|m|,|n|\}.$$

Therefore, $\sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{|mz+n|^k}$ converges if and only if $\sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{\max\{|m|,|n|\}^k}$ converges. For $N \geqslant 1$,

$$\sharp\{x \in \mathbb{Z}^2 : \max\{|m|,|n|\} = N\} = 8N$$

Therefore, $\sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{\max\{|m|,|n|\}^k}$ converges if and only if $\sum_{N \geqslant 1} \frac{8}{N^{k-1}}$ converges, i.e. if and only if $k \geqslant 3$. For $k \geqslant 3$, the series is uniformly convergent on compact subsets of $\mathbb{H}$ and we conclude by Lemma A.1.3. $\square$

To show that, for $k \geqslant 4$ even, $G_k$ is a modular form of weight $k$; it remains to show that $G_k$ is holomorphic at $\infty$. To show this we compute the $q$-expansion of $G_k$. But, first we need to recall some definitions:

(i) Let $\zeta$ denote *Riemann's zeta function*, defined for $s \in \mathbb{C}$ with real part greater than one by $\zeta(s) = \sum_{n \geqslant 1} n^{-s}$.

(ii) For a positive integer $n$, let $\sigma_l(n) = \sum_{0<d|n} d^l$, denote the *$l$-th divisor sum function.*

(iii) Let $B_k$ be the *$k$-th Bernouilli number*, defined by

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

**Example 2.1.20.** We explain how to compute the first Bernouilli numbers from their definition. Recall, $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$, therefore $\frac{e^x-1}{x} = \sum_{n=0}^{\infty} \frac{x^n}{(n+1)!}$. Now we find a multiplicative inverse by equating coefficients in

$$\left( \sum_{n=0}^{\infty} \frac{x^n}{(n+1)!} \right) \left( \sum_{k=0}^{\infty} B_k \frac{x^k}{k!} \right) = 1.$$

Comparing coefficients of $x^d$ we have $B_0 = 1$, and

$$0 = \sum_{k=0}^{d} \frac{B_k}{k!} \frac{1}{(d-k+1)!}.$$

And multiplying both sides by $(d+1)!$ we have

$$0 = \sum_{k=0}^{d} B_k \binom{d+1}{k}.$$

Hence

$$(d+1)B_d = -\sum_{k=0}^{d-1} B_k \binom{d+1}{k}.$$

And we can iteratively compute the Bernouilli numbers! We have

$$B_1 = -1/2,\ B_2 = 1/6,\ B_4 = -1/30,\ B_6 = 1/42 \ldots.$$

We also have $B_{2k+1} = 0$ for $k \geqslant 1$ which is straightforward to prove from the definition above, but we will not use it.

**Theorem 2.1.21.** For $k \geqslant 4$ even, the Eisenstein series $G_k$ is a modular form of weight $k$ and has $q$-expansion

$$G_k(z) = 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n\right).$$

*Proof.* We use the trigonometric identity of Lemma A.2.1

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

Recall,

$$\cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2}, \qquad \sin(\theta) = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

Plugging into the identity for cot we have

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

Hence

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

Differentiating $(k-1)$-times, we have

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

Moreover, as $k$ is even,

$$\begin{aligned} G_k(z) &= \sum_{\substack{m\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^k}, \\ &= 2\sum_{n=1}^{\infty}\frac{1}{n^k} + 2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^k} \\ &= 2\zeta(k) + 2\sum_{m=1}^{\infty}\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} n^{k-1}q^{mn} \end{aligned}$$

The coefficient of $q^d$ in the sum is:

$$2\frac{(2\pi i)^k}{(k-1)!}\sum_{n|d} n^{k-1} = 2\frac{(2\pi i)^k}{(k-1)!}\sigma_{k-1}(d),$$

giving

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

Finally, we use Euler's formula, for the Riemann zeta function at the even integers:

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

Putting this all together, we get

$$G_k(z) = 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{d=1}^{\infty}\sigma_{k-1}(d)q^d\right),$$

and hence $G_k$ is holomorphic at $\infty$. We had already observed that $G_k$ is holomorphic on $\mathbb{H}$ and satisfies the modular transformation property ($\star$), therefore $G_k$ defines a modular form. □

To complete the proof, we need to prove Euler's formula for the value of the Riemann zeta function at even integers.

**Lemma 2.1.22** (Euler's formula)**.** Let $k \geqslant 1$, then

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

*Proof.* We can use some of the same tricks we have already used. We have

$$\begin{aligned} \pi z\cot(\pi z) &= \pi z\frac{\cos(\pi z)}{\sin(\pi z)} = \pi i z\frac{e^{2\pi i z}+1}{e^{2\pi i z}-1} \\ &= \pi i z + \frac{2\pi i z}{e^{2\pi i z}-1} \\ &= \pi i z + \sum_{k=0}^{\infty}\frac{B_k}{k!}(2\pi i z)^k, \end{aligned} \tag{1}$$

by definition of the Bernoulli numbers. In the open unit disc, we also have

$$\begin{aligned}
\pi z \cot(\pi z) &= 1 + z \sum_{n=1}^{\infty} \left( \frac{1}{z+n} + \frac{1}{z-n} \right) \\
&= 1 + \sum_{n=1}^{\infty} \frac{-2z^2}{n^2 - z^2} \\
&= 1 + \sum_{n=1}^{\infty} \frac{-2z^2}{n^2} \frac{1}{1 - z^2/n^2} \\
&= 1 + \sum_{n=1}^{\infty} \frac{-2z^2}{n^2} \sum_{k=0}^{\infty} \frac{z^{2k}}{n^{2k}} \\
&= 1 + \sum_{k=0}^{\infty} -2z^{2(k+1)} \sum_{n=1}^{\infty} \frac{1}{n^{2(k+1)}} \\
&= 1 + \sum_{k=1}^{\infty} -2z^{2k} \sum_{n=1}^{\infty} \frac{1}{n^{2k}} \\
&= 1 - 2 \sum_{k=1}^{\infty} z^{2k} \zeta(2k). \qquad (2)
\end{aligned}$$

Comparing coefficients of $z^{2k}$ in (1) and (2) gives Euler's formula. □

**Definition 2.1.23.** For $k \geqslant 4$ even, we define the *normalized Eisenstein series* $E_k$ in $M_k$ by

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

In particular,

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n, \qquad E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n,$$

$$E_8(z) = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n, \qquad E_{10}(z) = 1 - 264 \sum_{n=1}^{\infty} \sigma_9(n) q^n,$$

$$E_{12}(z) = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n, \qquad E_{14}(z) = 1 - 24 \sum_{n=1}^{\infty} \sigma_{13}(n) q^n.$$

We saw that if we add modular forms of weight $k$ we get a modular form of weight $k$, and if we multiply modular forms of weight $k$ and $l$ we get a modular form of weight $k + l$. Let us use this to give an example of a *cusp form*:

**Example 2.1.24** (Discriminant modular form $\Delta$)**.** We have

$$E_4^3(z) - E_6^2(z) = 1728q + \text{higher order terms},$$

hence $E_4^3 - E_6^2$ defines a cusp form of weight 12. We normalize so that the coefficient of $q$ is 1 and define

$$\begin{aligned}
\Delta(z) &= \frac{E_4^3(z) - E_6^2(z)}{1728} \\
&= q - 24q^2 + 252q^3 + \cdots \\
&= \sum_{n=1}^{\infty} \tau(n) q^n.
\end{aligned}$$

In fact, it turns out that $\Delta$ has $q$-expansion equal to $q\prod_{n=1}^{\infty}(1-q^n)^{24}$ (our stated, but not proved, Example 2.1.6).

Ramanujan conjectured that $\tau$ is multiplicative: if $(m,n)=1$ then $\tau(mn)=\tau(m)\tau(n)$; and that for a prime $p$ and $r \geqslant 1$, $\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1})$. These conjectures were proved by Mordell (1917). We will prove these later.

### 2.1.5 Eisenstein series in weight 2 and the product expansion of $\Delta$

**Exercise 2.1.25.** Define, the *Eisenstein series in weight* 2, $G_2(z)$ to be the series

$$G_2(z) = \sum_{\substack{m\in\mathbb{Z}\\(m,n)\neq(0,0)}} \left(\sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^2}\right).$$

(The inner sum is over all integers, except when $m=0$ when it is over all non-zero integers). Note that as the sum is not absolutely convergent we need to fix an order. For this next question we set $\sum_{n\in\mathbb{Z}} f(n) = \lim_{N\to\infty}\sum_{n=-N}^{N} f(n)$. Similarly, we define $G_2'(z)$ to be the series:

$$G_2'(z) = \sum_{\substack{n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \left(\sum_{m\in\mathbb{Z}} \frac{1}{(mz+n)^2}\right).$$

Set

$$H(z) = \sum_{\substack{m\in\mathbb{Z}\\(m,n)\neq(0,0),(0,1)}} \left(\sum_{n\in\mathbb{Z}} \frac{1}{(mz+n-1)(mz+n)}\right),$$

$$H'(z) = \sum_{\substack{n\in\mathbb{Z}\\(m,n)\neq(0,0),(0,1)}} \left(\sum_{m\in\mathbb{Z}} \frac{1}{(mz+n-1)(mz+n)}\right).$$

(i) Show that $G_2(-z^{-1}) = z^2 G_2'(z)$.

(ii) Show that $H(z)=2$.
Hint: Write $\frac{1}{(mz+n-1)(mz+n)} = \frac{1}{mz+n-1} - \frac{1}{mz+n}$, there will be a lot of cancellation.

(iii) Show that $H'(z) = 2 - \frac{2\pi i}{z}$.
This is harder, we give some hints:

(a) Show that $H'(1/z) = z\sum_{\substack{n\in\mathbb{Z}\\(m,n)\neq(0,0),(0,1)}} \sum_{m\in\mathbb{Z}} \left(\frac{1}{(m+(n-1)z)} - \frac{1}{(m+nz)}\right)$;

(b) Use the series expansion for $\pi\cot\pi z$ to show that

$$\sum_{\substack{n\in\mathbb{Z}\\(m,n)\neq(0,0),(0,1)}} \sum_{m\in\mathbb{Z}} \frac{1}{(m+(n-1)z)} = \frac{1}{z} + \sum_{n\in\mathbb{Z},n\neq 1} \pi\cot(n-1)\pi z.$$

(c) Show that this sum is equal to $\frac{1}{z} + \lim_{N\to\infty}(\pi\cot(-N\pi z) + \pi\cot(-(N+1)\pi z))$.

(d) Use the expression for $\cot z$ in terms of $e^{iz}, e^{-iz}$ to show that this limit is $\frac{1}{z} - 2\pi i$.

(e) Perform a similar analysis to show that

$$\sum_{\substack{n\in\mathbb{Z} \\ (m,n)\neq(0,0),(0,1)}} \sum_{m\in\mathbb{Z}} \frac{1}{(m+nz)} = \frac{1}{z}.$$

(f) Conclude that $H'(z) = 2 - \frac{2\pi i}{z}$.

(iv) Show that $G_2$ is holomorphic on $\mathbb{H}$.
Hint: Show $(G_2 - H)$, $(G_2' - H')$ are absolutely convergent, uniformly on compact subsets of $\mathbb{H}$ and rearrangements of each other. Show that it follows that $G_2$ is uniformly convergent on compact subsets of $\mathbb{H}$ and hence holomorphic.

(v) Show that

$$G_2(-z^{-1}) - z^2 G_2(z) = -2\pi i z.$$

Is $G_2$ a modular form?

(vi) Find the $q$-expansion of $G_2$.

**Exercise 2.1.26.** Let $\eta$ denote the function $\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n)$, where as usual $q = e^{2\pi i z}$. Let $E_2(z)$ be the unique scalar multiple of $G_2(z)$ whose $q$-expansion begins with 1.

(i) Show that $\eta(z+1) = e^{\frac{\pi i}{12}}\eta(z)$.

(ii) Show that

$$\frac{d}{dz}(\log(\eta(z))) = \frac{\pi i}{12} E_2(z).$$

(iii) Show that, for $\sqrt{\ }$ the branch of the square root having nonnegative real part, we have

$$\eta\left(-1/z\right) = \sqrt{z/i}\,\eta(z).$$

(iv) Show that $\eta^{24} = \Delta$. Deduce that $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$.

## 2.2 How many modular forms are there?

Having defined modular forms and given a family of interesting examples, the next natural question is:

> How many modular forms are there?
> More precisely, what are the dimensions of the complex vector spaces $M_k$?

To answer this question we first need a better understanding of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$.

### 2.2.1 A fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ acting on $\mathbb{H}$

**Definition 2.2.1.** Suppose a group $G$ acts on $\mathbb{H}$. A closed subset $\mathcal{D}$ of $\mathbb{H}$ is called a *fundamental domain* for the action of $G$ if

(i) given $z \in \mathbb{H}$ there exists $\gamma \in G$ such that $\gamma \cdot z \in \mathcal{D}$;

(ii) if $z, z' \in \mathcal{D}$ are distinct $z \neq z'$ and there exists $\gamma \in G$ such that $\gamma \cdot z = z'$ then $z, z'$ both lie on the boundary of $\mathcal{D}$ and this boundary has measure zero.

For example, the set $\mathcal{T} = \{z \in \mathbb{H} : |\mathbf{Re}(z)| \leqslant 1/2\}$ is a fundamental domain for the (additive) group $\mathbb{Z}$ acting on $\mathbb{H}$ by translations, $x \cdot z = z + x$ for $x \in \mathbb{Z}$, $z \in \mathbb{H}$. It is immediately clear that fundamental domains are non-unique; in our example, any translate of $\mathcal{T}$ by any element of $\mathbb{R}$ is also a fundamental domain for the given action of $\mathbb{Z}$ on $\mathbb{H}$!

Two elements of $\mathrm{SL}_2(\mathbb{Z})$ which will be particularly important are

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

These act on $\mathbb{H}$ in the following way:

$$S \cdot z = -\frac{1}{z} \quad T \cdot z = z + 1.$$

Moreover, as noticed earlier $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ acts trivially on $\mathbb{H}$. We also observe that $\langle T \rangle \simeq \mathbb{Z}$, and $T^a$ is acting on $\mathbb{H}$ via the translation $z \mapsto z + a$.

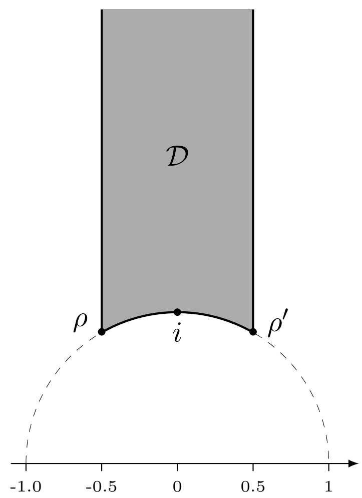
The rough idea to construct a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ acting on $\mathbb{H}$ is that using powers of $T$ every $z \in \mathbb{H}$ is in the same orbit as some $p \in \mathbb{H}$ with $|\mathbf{Re}(p)| \leqslant 1/2$, Moreover, noticing that, $S \cdot z = -\frac{\overline{z}}{|z|^2}$, we see that if $|p| < 1$ we can apply $S$ and move it to a point of larger absolute value. Then one can apply a power of $T$ again and continue.

**Theorem 2.2.2.** (i) The set

$$\mathcal{D} := \{z \in \mathbb{H} : -\frac{1}{2} < \mathbf{Re}(z) \leqslant \frac{1}{2}, |z| \geqslant 1\}$$

is a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$.

(ii) The elements $S, T$ generate $\mathrm{SL}_2(\mathbb{Z})$.




*Proof.* Let $\Gamma = \langle S, T \rangle$ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by $S, T$. Let $z \in \mathbb{H}$ be fixed. Choose $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ such that $|cz + d|$ is minimal amongst $|c'z + d'|$ with $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma$. By Lemma 2.1.1,

$$\mathrm{Im}(\gamma \cdot z) = \mathrm{Im}(z)/|cz + d|^2$$

is then maximal amongst $\mathrm{Im}(\gamma' \cdot z)$, $\gamma' \in \Gamma$. Let $n \in \mathbb{Z}$ such that

$$|\mathbf{Re}(T^n \gamma \cdot z)| \leq 1/2.$$

Suppopse $T^n \gamma \cdot z \notin \mathcal{D}$, i.e. $|T^n \gamma \cdot z| < 1$. Then

$$\begin{aligned} \mathrm{Im}(ST^n \gamma \cdot z) = \frac{\mathrm{Im}(T^n \gamma \cdot z)}{|T^n \gamma \cdot z|} &> \mathrm{Im}(T^n \gamma \cdot z) \\ &= \mathrm{Im}(\gamma \cdot z), \end{aligned}$$

contradicting the maximality of $\mathrm{Im}(\gamma \cdot z)$. Hence $T^n \gamma \cdot z \in \mathcal{D}$.

Suppose $z, z' \in \mathcal{D}$, we want to understand when they are in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit, and in particular show that if they are distinct and in the same orbit then they lie on the boundary of $\mathcal{D}$. Without loss of generality assume $\mathrm{Im}(z') \geqslant \mathrm{Im}(z)$. There is $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma \cdot z = z'$. Then

$$\mathrm{Im}(z) \leqslant \mathrm{Im}(z') = \mathrm{Im}(\gamma \cdot z) = \frac{\mathrm{Im}(z)}{|cz + d|^2},$$

the first inequality by our assumption. Therefore $|cz+d| \leqslant 1$. This implies $cz+d$ has imaginary part less than or equal to 1 in absolute value, and we have

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

as $z \in \mathcal{D}$. Therefore, $|c| \leqslant 1$, and we have three possibilities $c = 0, 1, -1$.

(i) ($c = 0$): Then as $\det(\gamma) = 1$ we have $\gamma = \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ for some $b \in \mathbb{Z}$, and it suffices to take $\gamma = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ as $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ acts trivially on $\mathcal{D}$. Then $z' = \gamma \cdot z = z + b$, and as $z, z' \in \mathcal{D}$ either

  (a) $b = 0$ and $z = z'$, or

  (b) $b = \pm 1$ and $z, z'$ lie on the boundary of $\mathcal{D}$.

(ii) ($c = 1$): Then our condition $|cz + d| \leq 1$ reads $|z + d| \leq 1$, and $z \in \mathcal{D}$ hence either $d = 0, 1, -1$.

  (a) ($d = 0$): this implies $|z| = 1$ and as $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma = \pm \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} = \pm T^a S$. Hence $z' = \gamma \cdot z = -\frac{1}{z} + a$, and as $|S \cdot z| = |z| = 1$, so we have two points on the unit circle $z$ and $S \cdot z$ and $\mathcal{D}$ which are translates under $a \in \mathbb{Z}$, implying $a = 0, 1, -1$. If $a = 0$ then $z' = S \cdot z = -\overline{z}$, and if $a = \pm 1$ then $S \cdot z = \rho$ or $\rho'$ and $z' = z = \rho$ or $\rho'$.

  (b) (d=1): We have $|z + 1| \leqslant 1$, $|z| \leqslant 1$, $|\mathbf{Re}(z)| \leqslant 1/2$ implying $z = \rho$. We have $\gamma = \begin{pmatrix} a & a-1 \\ 1 & 1 \end{pmatrix}$ and

$$\gamma \cdot \rho = a - \frac{1}{\rho + 1} = a + \rho = \begin{cases} \rho & \text{if } a = 0; \\ \rho' & \text{if } a = 1. \end{cases}$$

  (c) ($d = -1$): similar to the case $d = 1$ (omitted).

(iii) $(c = -1)$: multiply by $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and get back to case 2.

We have shown that no two distinct points in the interior of $\mathcal{D}$ are in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit, completing the proof that $\mathcal{D}$ is a fundamental domain.

Tracing back through the proof so far, we have computed the stabilizers in $\mathrm{SL}_2(\mathbb{Z})$ of all points in $\mathcal{D}$, for $z \in \mathcal{D}$ put

$$\Gamma_z := \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(z) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \cdot z = z\}.$$

We record these as a lemma:

**Lemma 2.2.3.** Putting $z' \in \mathcal{D}$ any point outside $\{i, \rho, \rho'\}$ we have

$$\begin{aligned} \Gamma_i &= \pm\{1, S\} \\ \Gamma_\rho &= \pm\{1, TS, (TS)^2\} \\ \Gamma_{\rho'} &= \pm\{1, ST, (ST)^2\} \\ \Gamma_{z'} &= \pm\{1\}. \end{aligned}$$

Finally we show that $\mathrm{SL}_2(\mathbb{Z}) = \Gamma$. Pick $z \in \mathcal{D}$ which is not in the boundary. At the start of the proof, we showed: for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ there exists $\gamma' \in \Gamma$ such that

$$\gamma' \cdot (\gamma \cdot z) \in \mathcal{D}.$$

Hence $\gamma'\gamma \cdot z$ and $z$ are in the same $\mathrm{SL}_2(\mathbb{Z})$ orbit and both in $\mathcal{D}$. Hence

$$\gamma'\gamma = \pm 1.$$

As $-1 = S^2$ and $\gamma'$ are both in $\Gamma$ so too is $\gamma$. □

### 2.2.2 Zeroes of modular forms

Let $f : \mathbb{H} \to \mathbb{C}$ be a non-zero modular form. Let $\nu_\infty(f)$ denote the index of the first nonvanishing term in the $q$-expansion of $f$. As $f$ is holomorphic it has no poles on the fundamental domain $\mathcal{D}$.

**Lemma 2.2.4.** There are only finitely many zeroes of $f$ on $\mathcal{D}$.

*Proof.* Let $f(z) = \widetilde{f}(q)$, $q = e^{2\pi i z}$. Then as $f$ is a modular form, $\widetilde{f}$ is holomorphic on $\mathbb{D}$. Hence in a neighbourhood of 0 in $\mathbb{D}$, $\widetilde{f}$ has no zeroes except possibly at $\mathbb{D}$. So if $0 < |q| < \varepsilon$, we have $\widetilde{f}(q) \neq 0$. Hence $f$ has no zeroes with imaginary part greater than $N(\varepsilon)$. The remainder of the fundamental domain is compact, so $f$ has only finitely many zeroes on $\mathcal{D}$ by Lemma A.1.4. □

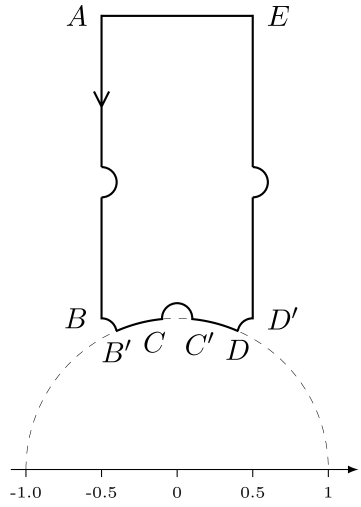
**Proposition 2.2.5** (The $(k/12)$-proposition)**.** We have

$$\nu_\infty(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_\rho(f) + \sum_{\substack{p \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \\ p \not\sim i, \rho}} \nu_p(f) = \frac{k}{12}.$$

If we set $e_p = |\Gamma_p|/2$, another way to write the $(k/12)$-formula is

$$\nu_\infty(f) + \sum_{p \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}} \frac{\nu_p(f)}{e_p} = \frac{k}{12}.$$

*Proof.* The idea of the proof is to integrate $f'/f$ close to the fundamental domain and use Cauchy's argument principle.




Our contour $EABB'CC'DD'$ follows the boundary of $\mathcal{D}$ cutting across at imaginary part $N$ where there are no zeroes with imaginary part greater than or equal to $N$. On the boundary if the zero is not at $i, \rho, \rho'$ the contour avoids it by going around a ball of radius $\varepsilon$, including it on one side of the line $\mathrm{Im}(z) = 0$ and excluding it on the other side as illustrated above, so that every zero of $f$ on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is counted precisely once inside the contour, except possibly zeroes at $i, \rho, \rho'$; if there are zeroes at these points they are kept outside the contour.

By Cauchy's argument principle

$$\frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)}dz = 2\pi i \sum_{\substack{p\in\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \\ p\not\sim i,\rho}} \nu_p(f).$$

We now compute the integral on the LHS.

The horizontal integral along the path EA: We change variables $q = e^{2\pi i z}$ and have

$$\frac{1}{2\pi i}\int_{EA}\frac{f'(z)}{f(z)}dz = \frac{1}{2\pi i}\int_{\substack{B(0,e^{-2\pi N}) \\ \text{oriented clockwise}}} \frac{\widetilde{f}'(q)}{\widetilde{f}(q)}dq = -\nu_0(\widetilde{f}) = -\nu_\infty(f).$$

The vertical integrals $AB$ and $D'E$ cancel.

To evaluate the integral on the arcs $BB'$, $CC'$, $DD'$ around $\rho, i, \rho'$ respectively, we note that the proof of Cauchy's argument principle applies more generally to show that

$$\frac{1}{i\theta}\int_{A_\varepsilon}\frac{f'(z)}{f(z)}dz = \nu_p(f),$$

for a sufficiently small arc of angle $\theta$ and radius $\varepsilon$ around $p$. (The usual argument principle for the full closed circle would have $\theta = 2\pi$). Hence, around $\rho$ we have

$$\frac{1}{2\pi i}\int_{BB'}\frac{f'(z)}{f(z)}dz = -\frac{1}{2\pi i}i\frac{\pi}{3}\nu_\rho(f) = -\frac{\pi}{6}\nu_\rho(f).$$

The sign appearing as the arc is oriented clockwise. Similarly, the integral around $\rho'$ gives $-\frac{\pi}{6}\nu_\rho(f)$ and around $i$ gives $-\frac{\pi}{2}\nu_i(f)$.

Collecting terms, to prove the proposition it remains to show for $\varepsilon$ sufficiently small

$$\frac{1}{2\pi i}\left(\int_{B'C}\frac{f'(z)}{f(z)}dz+\int_{C'D}\frac{f'(z)}{f(z)}dz\right)=\frac{k}{12}.$$

We notice first that $S\cdot z=-1/z=-\overline{z}$ on the unit circle and sends $B'C$ to $DC'$. Hence the integral we wish to compute is

$$\frac{1}{2\pi i}\left(\int_{B'C}\frac{f'(z)}{f(z)}dz-\int_{S(B'C)}\frac{f'(z)}{f(z)}dz\right).$$

Now $f(S\cdot z)=z^k f(z)$ as $f$ is a modular form of weight $k$, and differentiating both sides with respect to $z$ we get

$$f'(S\cdot z)\frac{d(S\cdot z)}{dz}=kz^{k-1}f(z)+z^kf'(z).$$

Dividing this by $f(S\cdot z)=z^kf(z)$ we have

$$\frac{f'(S\cdot z)}{f(S\cdot z)}\frac{d(S\cdot z)}{dz}=\frac{k}{z}+\frac{f'(z)}{f(z)}.$$

Therefore,

$$\frac{1}{2\pi i}\left(\int_{B'C}\frac{f'(z)}{f(z)}dz-\int_{B'C}\frac{f'(S\cdot z)}{f(S\cdot z)}d(S\cdot z)\right)=-\frac{1}{2\pi i}\int_{B'C}\frac{k}{z}dz.$$

As $\varepsilon\to 0$, the final integral is along an arc of angle $\pi/6$ oriented clockwise around 0, hence

$$-\frac{1}{2\pi i}\int_{B'C}\frac{k}{z}dz=-\frac{k}{2\pi i}\cdot-\frac{\pi i}{6}=\frac{k}{12},$$

which is what we needed to show. □

**Remark 2.2.6.** This section can be generalized easily to modular functions counting poles and their orders as well as zeroes.

### 2.2.3 Dimensions of spaces of modular forms

We now use our understanding of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ and, in particular, the $(k/12)$-proposition to prove dimension formulae of spaces of modular forms.

**Proposition 2.2.7.** (i) For $k<0$, $k$ odd, or $k=2$,

$$M_k=0;$$

In other words, there are no nonzero modular forms of odd weight, negative weight or weight 2.

(ii) The only modular forms of weight zero are the constant functions

$$M_0=\mathbb{C}.$$

(iii) If $k=4,6,8,10,14$, then

$$M_k=\mathbb{C}E_k$$

is one-dimensional generated by Eisenstein series.

(iv) The discriminant form $\Delta$ is non-vanishing on $\mathbb{H}$, and multiplication by $\Delta$ defines an isomorphism

$$S_k = M_{k-12}\Delta.$$

(v) We have a decomposition

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

*Proof.* (i) We have already seen there are no nonzero modular forms of odd weight, by applying the modular transformation law ($\star$) with $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, so we do not reprove it here. By Proposition 2.2.5, all terms on LHS are non-negative, hence $k$ is non-negative and there are no nonzero modular forms of negative weight. Moreover, there is no way to make $2/12 = 1/6$ on the LHS by positive integral combinations of $1, 1/2, 1/3$ hence there are no modular forms of weight 2.

(ii) First note that constant functions are modular forms of weight zero. Let $f \in M_0$, and pick any $p \in \mathbb{H}$. Suppose that $f$ is not constant. Let $c$ denote the constant function taking value $f(p)$ on the entire half plane. Then $(f - c) \in M_0$ and has a zero at $p$, implying that the LHS of Proposition 2.2.5 is nonzero, however the RHS is, a contradiction. Hence $f - c = 0$, and $f$ is constant.

(iii) Let $f \in M_k$. In all the cases $k = 4, 6, 8, 10, 14$ there is only one possibility for Proposition 2.2.5 to hold:

$$\begin{aligned} k = 4 &\Rightarrow \nu_\rho(f) = 1 \text{ and everywhere else } f \text{ is nonzero;} \\ k = 6 &\Rightarrow \nu_i(f) = 1 \text{ and everywhere else } f \text{ is nonzero;} \\ k = 8 &\Rightarrow \nu_\rho(f) = 2 \text{ and everywhere else } f \text{ is nonzero;} \\ k = 10 &\Rightarrow \nu_\rho(f) = \nu_i(f) = 1 \text{ and everywhere else } f \text{ is nonzero;} \\ k = 14 &\Rightarrow \nu_\rho(f) = 2, \nu_i(f) = 1 \text{ and everywhere else } f \text{ is nonzero;} \end{aligned}$$

Let $f, f'$ be non-zero modular forms of weight $k$. As $f, f'$ have the same zeroes $f/f' \in M_0$ hence $f = cf'$ by part (ii) and we can take $f' = E_k$.

(iv) For $k = 12$, $\Delta \in S_k$ implies $\nu_\infty(f) = 1$ and $\Delta$ is nonvanishing on $\mathbb{H}$. Hence for $f, f' \in M_{k-12}$, the equation $f\Delta = f'\Delta$ implies that $f = f'$ and the map is injective. For $k \geqslant 12$, if $g \in S_k$ then $g/\Delta$ is holomorphic on $\mathbb{H}$ and $\nu_\infty(g/\Delta) = \nu_\infty(g) - \nu_\infty(\Delta) \geqslant 0$. Hence $g/\Delta \in M_{k-12}$, and the multiplication by $\Delta$ map is bijective.

(v) As $E_k$ does not vanish at $\infty$, given $f \in M_k$ we can subtract a multiple $mE_k$ of $E_k$ so that $f - mE_k \in S_k$.

□

**Example 2.2.8.** For $k = 8, 10, 14$, as $\dim M_k = 1$, by comparing the leading coefficients in their $q$-expansions we see that

$$\begin{aligned} E_8 &= E_4^2 \\ E_4E_6 &= E_{10} \\ E_4^2E_6 &= E_{14}. \end{aligned}$$

**Theorem 2.2.9.** (i) We have

$$\dim M_k = \begin{cases} 0 & \text{if } k < 0, k \text{ odd;} \\ \lfloor k/12 \rfloor & \text{if } k \equiv 2 \pmod{12}, k > 0; \\ \lfloor k/12 \rfloor + 1 & \text{if } k \not\equiv 2 \pmod{12}, k \text{ even}, k > 0; \end{cases}$$

(ii) Any $f \in M_k$ can be written as a polynomial in $E_4$ and $E_6$.

*Proof.* (i) The dimension formula is true for $k < 12$ by Corollary 2.2.7 (i),(iii). By Corollary 2.2.7 (iv), (v) we have for $k \geqslant 12$

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

hence the formula holds for all $k$.

(ii) By Example 2.2.8 all modular forms of weight $k < 12$ and $k = 14$ can be written as polynomials in $E_4, E_6$. Suppose $k \geqslant 4$ is even, then we can $a, b \in \mathbb{Z}^{\geqslant 0}$ such that

$$4a + 6b = k,$$

and so $E_4^a E_6^b \in M_k$. Hence, for all $f \in M_k$ there exists $\lambda \in \mathbb{C}$ such that

$$f - \lambda E_4^a E_6^b \in S_k.$$

Hence by Corollary 2.2.7 (iv)

$$f = cE_4^a E_6^b + \Delta f_1,$$

with $f_1 \in M_{k-12}$. Hence Part (ii) follows by induction on $k$.

□

**Remark 2.2.10.** Let $M_\bullet = \bigoplus_{k=0}^\infty M_k$, this is a graded ring, i.e. $M_k M_l \subseteq M_{k+l}$. Moreover, the map $\mathbb{C}[X, Y] \to M_\bullet$ taking $X$ to $E_4$ and $Y$ to $E_6$ is an isomorphism of rings. Setting degree $X = 4$ and degree $Y = 6$, this is an isomorphism of graded rings where the grading on $\mathbb{C}[X, Y]$ is $\mathbb{C}[X, Y] = \bigoplus_{k=0}^\infty$ homogeneous polynomials of degree $k$.

**Exercise 2.2.11.** Use the identity $E_8 = E_4^2$ to show that

$$\sigma_7(n) = 480\sigma_3(n) + 240^2 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m).$$

Use the identity $E_{10} = E_4 E_6$ to write $\sigma_9(n)$ in terms of $\sigma_3(n)$ and $\sigma_5(n)$.

**Exercise 2.2.12** (Ramanujan's congruence)**.** Show that there exist and find constants such that $E_4^3 = c_1 E_{12} + c_2 \Delta$. Conclude that $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$.

**Exercise 2.2.13.** Using the $q$-expansions of $E_4, E_6$ and the identity $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$, show that the $q$-expansion of $\Delta$ has integral coefficients.

**Exercise 2.2.14.** (i) Let $d = \dim M_k$. Show that there is a unique basis for $M_k$ of the form $g_1, ..., g_d$, where for all $i$ the $q$-expansion of $g_i$ has the form $q^{i-1} + \sum_{n=d}^\infty c_n q^n$.

(ii) Show further that any element of $M_k$ whose $q$-expansion has integer coefficients is an integral linear combination of the $g_i$.

**Exercise 2.2.15.** Let $M_k(\mathbb{Z})$ be the space of modular forms of weight $k$ with integral $q$-expansions. Show that the (graded) ring $M_\bullet(\mathbb{Z}) = \bigoplus_{k \geqslant 0} M_k(\mathbb{Z})$ is generated over $\mathbb{Z}$ by $E_4$, $E_6$, and $\Delta$.

### 2.2.4 Modular functions and the $j$-invariant

The quotient of modular forms is a modular function: Let $f \in M_k$, $f' \in M_l$ be modular forms, then $f/f'$ is a modular function of weight $k-l$. There is a particularly important modular function of weight 0. Define

$$j(z) = \frac{E_4^3(z)}{\Delta(z)},$$

a modular function of weight 0 called the *$j$-invariant*. The $j$-invariant is holomorphic on $\mathbb{H}$ as $\Delta$ is non-vanishing on $\mathbb{H}$, and has a simple pole at $\infty$.

**Remark 2.2.16** (Monstrous Moonshine)**.** The $q$-expansion of $j$ is given by

$$j(z) = \frac{1}{q} + 744 + 196884q + 2149360q^2 + \cdots .$$

It was noticed in the 1970's that these coefficients are very close to the dimensions of the irreducible representations of the *Monster group* (the largest *sporadic* simple group) which has order approx $8 \times 10^{53}$! This phenomenon was coined *monstrous moonshine* by Conway and Norton!

**Theorem 2.2.17.** The function $j$ induces a bijection

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}.$$

*Proof.* Let $\lambda \in \mathbb{C}$, and put

$$f(z) = E_4^3(z) - \lambda\Delta(z)$$

a modular form of weight 12. The $(k/12)$-proposition 2.2.5, implies

$$1 = \frac{\nu_i(f)}{2} + \frac{\nu_\rho(f)}{3} + \sum_{\substack{p \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \\ p \neq i,\rho}} \nu_p(f),$$

as $\nu_\infty(f) = 0$. Hence $f$ vanishes at exactly one point $z_0 \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. Dividing by $\Delta$, this implies

$$j(z_0) - \lambda = 0,$$

for precisely one $z_0 \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. Hence $j$ defines a bijection $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$. □

**Remark 2.2.18.** (i) Following the theorem there is a unique topology and complex structure on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ that makes $j : \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$ an isomorphism of Riemann surfaces (one dimensional complex manifolds).

(ii) Combining with the bijection of Proposition 12, we also have a bijection $j : \mathrm{Latt}_{\mathbb{C}} / \mathbb{C}^\times \to \mathbb{C}$ by $j(L_{z,1}) = j(z)$. An elliptic curve over $\mathbb{C}$ is isomorphic to $\mathbb{C}/L$ for some $L \in \mathrm{Latt}_{\mathbb{C}}$, this is called the *Uniformization Theorem*, and $L, L' \in \mathrm{Latt}_{\mathbb{C}}$ define isomorphic elliptic curves if and only if the lattices are homothetic, that is $L = \lambda L'$, for some $\lambda \in \mathbb{C}^\times$. Hence the $j$-invariant is an invariant for isomorphism classes of elliptic curves over $\mathbb{C}$.

**Theorem 2.2.19.** Let $f$ be a merormorphic function on $\mathbb{H}$. The following are equivalent:

(i) $f$ is a modular function of weight zero;

(ii) $f$ is a quotient of two modular forms of the same weight;

(iii) $f$ is a rational function of $j$.

Recall, the definition of a *rational function* of $j$: In other words, Property (iii) says that there are polynomials $P, Q \in \mathbb{C}[X]$ such that $P(j)/Q(j) = f$.

*Proof.* The implications (iii)⇒(ii)⇒(i) are straightforward from the definitions. We show (i)⇒(iii). Let $f$ be a modular function of weight zero. Let $z_i$ denote the poles of $f$ in $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$, and let $a_i$ denote the order of $z_i$ (there are only finitely many poles - argument completely analogous to Lemma 2.2.4). Then

$$f(z)\prod_i (j(z) - j(z_0))^{a_i}$$

is a modular function of weight zero with no poles in $\mathbb{H}$. Choose $k \in \mathbb{Z}$ such that

$$\Delta^k(z) f(z) \prod_i (j(z) - j(z_0))^{a_i}$$

is holomorphic at $\infty$. Hence is a modular form of weight $12k$. By Theorem 2.2.9 (ii)

$$\Delta^k(z) f(z) \prod_i (j(z) - j(z_0))^{a_i} = \sum_{4c+6d=12k} b_{c,d} E_4^c(z) E_6^d(z).$$

Hence it suffices to show that

$$\sum_{4c+6d=12k} b_{c,d} E_4^c E_6^d / \Delta^k$$

is a rational function in $j$. As $4c+6d = 12k$, we must have $c = 3c'$ and $d = 2d'$ for integers $c', d'$. Hence

$$\frac{E_4^c E_6^d}{\Delta^k} = \left(\frac{E_4^3}{\Delta}\right)^{c'} \left(\frac{E_6^2}{\Delta}\right)^{d'},$$

and we just need to check $E_4^3/\Delta$ and $E_6^2/\Delta$ are rational functions in $j$. The first is by definition, as $E_4^3/\Delta = j$. For the second, note that

$$\begin{aligned} \frac{E_6^2}{\Delta} - j &= \frac{E_6^2}{\Delta} - \frac{E_4^3}{\Delta} \\ &= 1728 \left( \frac{E_6^2}{E_4^3 - E_6^2} - \frac{E_4^3}{E_4^3 - E_6^2} \right) \\ &= -1728. \end{aligned}$$

Hence $\frac{E_6^2}{\Delta} = j - 1728$, and we are done. □

**Corollary 2.2.20.** For $k \geqslant 4$. Every modular function of weight $k$ is the product of a rational function in $j$ with $E_k$.

## 2.3 Hecke operators

### 2.3.1 Motivation

In Example 2.1.24, we remarked, without proof, some nice arithmetic properties of the coefficients in the $q$-expansion of $\Delta = \sum_{n=1}^{\infty} \tau(n) q^n$ conjectured by Ramanujan:

(i) If $(m,n)=1$ then
$$\tau(mn)=\tau(m)\tau(n);$$

(ii) for a prime $p$ and $r\geqslant 1$,
$$\tau(p^{r+1})=\tau(p)\tau(p^r)-p^{11}\tau(p^{r-1}).$$

Notice that, also in the $q$-expansion of the Eisenstein series
$$E_k(z)=1-\frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n,$$
the functions $\sigma_{k-1}(n)=\sum_{d|n}d^k$ satisfy

(i) If $(m,n)=1$ then
$$\sigma_{k-1}(mn)=\sigma_{k-1}(m)\sigma_{k-1}(n);$$

(ii) for a prime $p$ and $r\geqslant 1$,
$$\sigma_{k-1}(p^{r+1})=\sigma_{k-1}(p)\sigma_{k-1}(p^r)-p^{k-1}\sigma_{k-1}(p^{r-1}).$$

In the next sections we introduce operators on the vector spaces of modular forms of weight $k$, and will prove these identities. The underlying philosophy is that the modular forms which are eigenvectors for these operators are those with arithmetic content such as $\Delta$ and $E_k$.

### 2.3.2 Correspondences on $\mathrm{Latt}_{\mathbb{C}}$

Let $S$ be a set, and $\mathbb{Z}[S]$ be the free abelian group on symbols $[s]$ for $s\in S$, i.e.
$$\mathbb{Z}[S]=\{a_1[s_1]+\cdots+a_r[s_r]:a_i\in\mathbb{Z},s_i\in S\},$$
considered as an abelian group under addition. A *correspondence* $T$ on a set $S$ is a $\mathbb{Z}$-linear map
$$T:\mathbb{Z}[S]\to\mathbb{Z}[S].$$
By $\mathbb{Z}$-linearity, we can define $T$ by its values on the elements of $S$,
$$T[s]=\sum_{y\in S}n_y(s)[y],$$
with $n_y(s)\in\mathbb{Z}$. The key examples for us are:

**Definition 2.3.1.** For $\lambda\in\mathbb{C}^{\times}$, we define a correspondence $R_\lambda$ on $\mathrm{Latt}_{\mathbb{C}}$ by our rescaling operator, for $L\in\mathrm{Latt}_{\mathbb{C}}$,
$$R_\lambda[L]=[\lambda L].$$
For $n\in\mathbb{Z}^+$, we define a correspondence $T_n$ on $\mathrm{Latt}_{\mathbb{C}}$ by summing over all sublattices of index $n$, for $L\in\mathrm{Latt}_{\mathbb{C}}$,
$$T_n[L]=\sum_{[L:L']=n}[L'].$$

**Proposition 2.3.2.** For all $\lambda, \lambda' \in \mathbb{C}^\times$, $n, m \in \mathbb{Z}^+$

(i) $R_\lambda R_{\lambda'} = R_{\lambda\lambda'} = R_{\lambda'} R_\lambda$;

(ii) $R_\lambda T_n = T_n R_\lambda$;

(iii) if $(n, m) = 1$ then $T_m T_n = T_{mn}$;

(iv) for $p$ prime, $T_{p^n} T_p = T_{p^{n+1}} + p T_{p^{n-1}} R_p$.

*Proof.* (i) This is clear: $R_\lambda R_{\lambda'}[L] = [\lambda\lambda' L] = R_{\lambda\lambda'}[L] = R_{\lambda'} R_\lambda [L]$.

(ii) We have $R_\lambda T_n(L) = \sum_{[L:L']=n} R_\lambda [L'] = \sum_{[L:L']=n} [\lambda L]$ and $T_n R_\lambda [L] = \sum_{[\lambda L : L'] = n} [L']$. But multiplication by $\lambda$ defines a bijection $\{L' \subseteq L : [L : L'] = n\}$ and $\{L'' \subseteq \lambda L : [\lambda L : L''] = n\}$, hence the two sums are the same.

(iii) Suppose $(n, m) = 1$. By definition

$$\begin{aligned} T_n T_m [L] &= T_n \sum_{[L:L']=n} [L'] \\ &= \sum_{[L:L']=m} T_n([L']) \\ &= \sum_{[L:L']=m} \sum_{[L':L'']=n} [L''] \\ &= \sum_{[L:L'']=mn} \alpha(L/L'')[L''], \end{aligned}$$

where $\alpha(L/L'')$ is the number of lattices $L'$ such that $L'' \subseteq L' \subseteq L$ with $[L : L'] = m$ and $[L' : L''] = n$. It suffices to show that whenever $(m, n) = 1$ we have $\alpha(L/L'') = 1$, then clearly

$$T_n T_m [L] = \sum_{[L:L'']=mn} L'' = T_{nm}[L],$$

and hence $T_n T_m [L] = T_m T_n [L]$. In other words, it suffices to show that for each $L'' \subseteq L$ of index $mn$ there is a unique $L' \subseteq L$ such that $[L : L'] = m$ and $[L' : L''] = n$. For such a lattice, $L'/L''$ is an order $n$ subgroup of $L/L''$ a finite abelian group of order $mn$. By Lemma B.1.1, $L/L''$ has a unique subgroup of order $n$ namely $m(L/L'')$. Its preimage under the map $L \to L/L''$ gives the unique lattice $L'$ satisfying the conditions. Hence $\alpha(L/L'') = 1$ for all coprime $m, n$, and $T_n T_m = T_{mn} = T_m T_n$.

(iv) By definition,

$$\begin{aligned} T_{p^n} T_p [L] &= \sum_{[L:L']=p} T_{p^n}[L'] \\ &= \sum_{[L:L']=p} \sum_{[L':L'']=p^n} [L''] \\ &= \sum_{[L:L'']=p^{n+1}} \beta(L/L'')[L'']. \end{aligned}$$

where

$$\begin{aligned} \beta(L/L'') &= \sharp\{L' \subseteq L : [L : L'] = p, [L' : L''] = p^n\} \\ &= \sharp\{H \leqslant L/L'' : |H| = p^n\}. \end{aligned}$$

This time however $\beta(L/L'')$ depends on $L/L''$. Let's first consider an example:

**Example 2.3.3.** Let $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$. Put $L_1'' = \mathbb{Z}p^2w_1 + \mathbb{Z}w_2$ and $L_2'' = \mathbb{Z}pw_1 + \mathbb{Z}pw_2$. Then $L/L_1'' = \mathbb{Z}/p^2\mathbb{Z}$, and $L/L_2'' = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. As $L/L_1''$ is cyclic

$$\beta(L/L_1'') = \sharp\{H \leqslant L/L_1'' : |H| = p\} = 1$$

whereas

$$\beta(L/L_2'') = \sharp\{H \leqslant L/L_2'' : |H| = p\} = p+1$$

as there are $p^2 - 1$ non-zero elements in $L/L_2''$, and $p-1$ elements generate the same subgroup.

Returning to the general case, as $L$ is generated by two elements so too is $L/L''$. By the Fundamental Theorem of Abelian Groups, a finite abelian group of order $p^{n+1}$ generated by two elements fits into one of two cases:

(a) $L/L'' = \mathbb{Z}/p^{n+1}\mathbb{Z}$ is cyclic;

(b) $L/L'' = \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}/p^b\mathbb{Z}$, $a, b \geqslant 1$

In case (a), $\beta(L/L'') = 1$ as $L/L''$ is cyclic and its subgroups of a given order are unique.

**Lemma 2.3.4.** We are in case (*b*), $L/L''$ is not cyclic, if and only if $L'' \subseteq pL$.

*Proof.* Suppose $L'' \subseteq pL \subseteq L$ then $L/pL$ is a quotient of $L/L''$. Hence as $L/pL \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ is not cyclic, neither is $L/L''$.

Suppose we are in the not cyclic case $L/L'' \simeq \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}/p^b\mathbb{Z}$ and let $H = p\mathbb{Z}/p^a\mathbb{Z} \oplus p\mathbb{Z}/p^b\mathbb{Z} \subseteq L/L''$. The preimage $L_H$ of $H$ in $L$ has index $p^2$ and is generated by the images of $w_1, w_2$, hence $L_H = pL \supseteq L''$. □

In case (b), as $[L : L'] = p$ the group $L/L'$ is killed by multiplication by $p$ and hence $pL \subseteq L'$. By Lemma 2.3.4, we thus have $L'' \subseteq pL \subseteq L' \subseteq L$, and

$$\begin{aligned}\beta(L/L'') &= \sharp\{L' \subseteq L : [L' : pL] = p\}\\ &= \sharp\{H \leqslant L/pL : |H| = p\}.\end{aligned}$$

counts the number subgroups of $L/pL = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ of order $p$ and as we have already explained this is $p+1$. Therefore

$$\begin{aligned}T_{p^n}T_p[L] &= \sum_{\substack{[L:L'']=p^{n+1}\\ L/L''\text{ cyclic}}} [L''] + (p+1) \sum_{\substack{[L:L'']=p^{n+1}\\ L/L''\text{ not cyclic}}} [L''];\\
&= \sum_{\substack{[L:L'']=p^{n+1}\\ L/L''\text{ cyclic}}} [L''] + (p+1) \sum_{\substack{[L:L'']=p^{n+1}\\ L/L''\subseteq pL}} [L'']\\
&= \sum_{[L:L'']=p^{n+1}} [L''] + p \sum_{\substack{[L:L'']=p^{n+1}\\ L/L''\subseteq pL}} [L'']\\
&= \sum_{[L:L'']=p^{n+1}} [L''] + p \sum_{[pL:L'']=p^{n-1}} [L'']\\
&= T_{p^{n+1}}[L] + pT_{p^{n-1}}R_p[L]\\
&= T_{p^{n+1}}[L] + pR_pT_{p^{n-1}}[L]\end{aligned}$$

the final equality by (ii).

□

By induction on $n$, Proposition 2.3.2 (iv), shows that $T_{p^n}$ is a polynomial in $T_p$ and $R_p$. Since, the operators $T_{p^n}$ are polynomials in $T_p, R_p$ they all commute with each other, and hence by (iii) we see that $T_n$ commutes with $T_m$ for all $m, n \in \mathbb{Z}^+$.

**Corollary 2.3.5.** (i) For $p$ prime the $T_{p^n}$ are polynomials in $T_p$ and $R_p$.

(ii) The algebra generated by $R_\lambda$ and $T_p$, $p$ prime, is commutative and contains all $T_n$.

**Exercise 2.3.6.** Let $m, n \in \mathbb{Z}^+$, show that

$$T_n T_m = \sum_{\substack{a|\mathrm{GCD}(m,n) \\ a \geqslant 1}} a R_a T_{mn/a^2}.$$

### 2.3.3 Lattice functions and Hecke operators

Let $F : \mathrm{Latt}_{\mathbb{C}} \to \mathbb{C}$ be a lattice function of weight $k$, that is

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

We define $R_\lambda F : \mathrm{Latt}_{\mathbb{C}} \to \mathbb{C}$ by

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

and we define $T_n F : \mathrm{Latt}_{\mathbb{C}} \to \mathbb{C}$ by

$$T_n F(L) = n^{k-1} \sum_{[L:L']=n} F(L').$$

The factor $n^{k-1}$ is just a convenient normalization. By Proposition 2.3.2, we have

$$R_\lambda T_n F = T_n R_\lambda F = \lambda^{-k} T_n F,$$

or in other words $T_n F$ is also a lattice function of weight $k$, i.e. $T_n$ acts on the space of lattice functions of weight $k$.

**Lemma 2.3.7.** We have

$$\begin{aligned} &T_m T_n F = T_{mn} F \quad \text{if } (m,n) = 1, \\ &T_{p^{n+1}} F = T_p T_{p^{n+1}} F - p^{k-1} T_{p^{n-1}} F \quad \text{if } p \text{ is prime and } n \geqslant 1. \end{aligned}$$

*Proof.* The first part follows from Part (iii) of Proposition 2.3.2 as $(nm)^{k-1} = n^{k-1} m^{k-1}$. Extending $F$ to $\mathbb{Z}[\mathrm{Latt}_{\mathbb{C}}]$ linearly, part (iv) of Proposition 2.3.2 gives

$$F(T_{p^n} T_p [L]) = F(T_{p^{n+1}}[L]) + p^{1-k} F(T_{p^{n-1}}[L]).$$

Hence

$$\frac{1}{(p^{n+1})^{k-1}} T_{p^n} T_p F([L]) = \frac{1}{(p^{n+1})^{k-1}} T_{p^{n+1}} F[L] + p^{1-k} \frac{1}{(p^{n-1})^{k-1}} T_{p^{n-1}} F[L],$$

and multiplying by $(p^{n+1})^{k-1}$ we get

$$T_{p^n} T_p F([L]) = T_{p^{n+1}} F[L] + p^{k-1} T_{p^{n-1}} F[L].$$

∎

We now want to transfer the action of $T_n$ on lattice functions to an action on modular functions. For that we need a lemma:

**Lemma 2.3.8.** Let $L = L_{z_1,z_2} \in \mathrm{Latt}_{\mathbb{C}}$. Let $S_n$ be the set of integer matrices $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $ad = n$, $a \geqslant 1$, $0 \leqslant b < d$. The map

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \to L_{az_1+bz_2,dz_2},$$

is a bijection from $S_n$ onto the set $L(n)$ of sublattices of index $n$ in $L$.

*Proof.* We have

$$L_{adz_1,dz_2} = L_{adz_1+bdz_2,dz_2} \subseteq L_{az_1+bz_2,dz_2} \subseteq L,$$

and $[L : L_{adz_1,dz_2}] = ad^2$ and $[L_{az_1+bz_2,dz_2} : L_{adz_1+bdz_2,dz_2}] = d$. Hence $[L : L_{az_1+bz_2,dz_2}] = ad = n$ so $L_{az_1+bz_2,dz_2} \in L(n)$. Another way to see this is that the index is equal to the determinant of the linear transformation $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$. Conversely let $L' \in L(n)$ and put

$$H_1 = L/(L' + \mathbb{Z}z_2), \quad \text{and} \quad H_2 = \mathbb{Z}z_2/(L' \cap \mathbb{Z}z_2).$$

These are cyclic groups generated by the images of $z_1$ and $z_2$ respectively. Let $a = |H_1|$ and $d = |H_2|$. The exact sequence

$$0 \to H_2 \to L/L' \to H_1 \to 0,$$

shows that $ad = n$. Moreover, $z_2 \in L' + \mathbb{Z}z_2$ and multiplication by $d$ kills $H_2$, hence $dz_2 \in L'$. On the other hand, multiplication by $a$ kills $H_1$, so $az_1 \in L' + \mathbb{Z}z_2$. Thus, there exists $b \in \mathbb{Z}$ such that $az_1 + bz_2 \in L'$ and as there is a unique $b$ satisfying $0 \leqslant b < d$. Hence $L_{az_1+bz_2,dz_2} \subseteq L' \subseteq L$ and as $[L : L_{az_1+bz_2,dz_2}] = n$ we must have $L' = L_{az_1+bz_2,dz_2}$. □

Notice that, if $p$ is prime then the elements of $S_p$ are the matrix $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and the $p$ matrices $\left(\begin{smallmatrix} 1 & b \\ 0 & p \end{smallmatrix}\right)$ for $0 \leqslant b < p$.

### 2.3.4 Hecke operators

Our connection between lattice functions and modular functions, see Remark 2.1.15, now allows us to define an action of $T_n$ on the space of weakly modular functions. Let $f$ be a modular function of weight $k$, and $F$ it associated lattice funtion, so that $f(z) = F(L_{z,1})$. We put

$$\begin{aligned}
T_n f(z) = T_n F(L_{z,1}) &= n^{k-1} \sum_{[L_{z,1}:L']=n} F(L) \\
&= n^{k-1} \sum_{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_n} F(L_{az+b,d}) \\
&= n^{k-1} \sum_{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_n} F(dL_{\frac{az+b}{d},1}) \\
&= n^{k-1} \sum_{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_n} R_d F(L_{\frac{az+b}{d},1}) \\
&= n^{k-1} \sum_{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_n} d^{-k} F(L_{\frac{az+b}{d},1}) \\
&= n^{k-1} \sum_{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_n} d^{-k} f\left(\frac{az+b}{d}\right) = n^{k-1} \sum_{\substack{a \geqslant 1,\ ad=n \\ 0 \leqslant b < d}} d^{-k} f\left(\frac{az+b}{d}\right),
\end{aligned}$$

and observe that if $f$ is meromorphic on $\mathbb{H}$ so too is $T_n f$, so indeed we have defined an action on the space of weakly modular functions. We now show that the $T_n$ act as linear operators on the vector spaces $M_k, S_k$. We call the $T_n$ *Hecke operators*.

**Theorem 2.3.9.** (i) $T_n$ preserves the spaces of modular functions of weight $k$, modular forms of weight $k$, cusp forms of weight $k$.

(ii) Suppose $f(z) = \sum_{m\in\mathbb{Z}} c(m)q^m$ is a modular function of weight $k$, then $T_n f(z) = \sum_{m\in\mathbb{Z}} \gamma(m)q^m$ with

$$\gamma(m) = \sum_{\substack{a|\mathrm{GCD}(m,n)\\ a\geqslant 1}} a^{k-1} c\left(\frac{mn}{a^2}\right).$$

*Proof.* Suppose $f$ is a modular function of weight $k$ with $q$-expansion $f(z) = \sum_{m\in\mathbb{Z}} a(m)q^m$. Then, by definition,

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

Now

$$\sum_{0\leqslant b<d} e^{2\pi i \frac{b}{d} m} = \begin{cases} d & \text{if } d \mid m;\\ 0 & \text{otherwise.}\end{cases}$$

Hence, putting $m' = m/d$, we have

$$\begin{aligned}
T_n f(z) &= n^{k-1} \sum_{m\in\mathbb{Z}} \sum_{\substack{a\geqslant 1\\ ad=n}} d^{-k+1} a(m) e^{2\pi i a z m'}\\
&= n^{k-1} \sum_{m\in\mathbb{Z}} \sum_{\substack{a\geqslant 1\\ ad=n}} n^{-k+1} a^{k-1} a(m) q^{am'}\\
&= \sum_{m\in\mathbb{Z}} \sum_{\substack{a\geqslant 1\\ ad=n}} a^{k-1} a(m) q^{am'}.
\end{aligned}$$

For the coefficient of $q^m$, we need $am' = m$ and $ad = n$, so $a \mid \mathrm{GCD}(m,n)$ and these $a$'s contribute:

$$\sum_{\substack{a|\mathrm{GCD}(m,n)\\ a\geqslant 1}} a^{k-1} c\left(\frac{mn}{a^2}\right).$$

It follows that $T_n$ preserves the properties of meromorphy, holomorphy and vanishing at $\infty$, and hence preserves the spaces of modular functions, modular forms, and cusp forms. □

### 2.3.5 Eigenforms

**Definition 2.3.10.** A modular form $f(z) = \sum_{n=0}^{\infty} c(n)q^n$ of weight $k$ is called a *(Hecke) eigenform* if there exist $\lambda_n \in \mathbb{C}$ such that, for all $n \in \mathbb{Z}^+$,

$$T_n f = \lambda_n f.$$

It is called a *normalized eigenform* if $c(1) = 1$.

**Example 2.3.11.** The space of cusp forms of weight 12 has dimension 1 and is generated by $\Delta$. As $T_n$ preserves $S_{12}$, we have

$$T_n\Delta = \lambda_n\Delta,$$

for some $\lambda_n \in \mathbb{C}$, and $\Delta$ is a normalized eigenform.

**Proposition 2.3.12.** If $f \in M_k$ is a normalized eigenform, then the $n$-th coefficient in the $q$-expansion of $f$ is its $T_n$-eigenvalue.

*Proof.* The coefficient of $q$ in the $q$-expansion of $T_n f$ is

$$\sum_{\substack{a|\mathrm{GCD}(n,1)\\ a\geqslant 1}} a^{k-1}c\left(\frac{n}{a^2}\right) = c(n).$$

On the other hand, $T_n f = \lambda_n f$ so $c(n) = \lambda_n c(1)$, and if $f$ is a normalized eigenform then $c(1) = 1$ so $c(n) = \lambda_n$. □

**Corollary 2.3.13.** If $f(z) = \sum_{n=0}^{\infty} c(n)q^n$ is a normalized eigenform of weight $k$ then

$$\begin{aligned} c(m)c(n) &= c(mn) \qquad \text{if } (m,n) = 1; \\ c(p)c(p^n) &= c(p^{n+1}) + p^{k-1}c(p^{n-1}). \end{aligned}$$

Applying Corollary 2.3.13 to the normalized eigenform $\Delta$ gives Ramanujan's conjecture proved by Mordell (see Example 2.1.24).

**Proposition 2.3.14.** For all even $k \geqslant 4$, $E_k$ is a (non-normalized) eigenform.

*Proof.* It suffices to show that $T_pE_k = \lambda_pE_k$ for all primes $p$. Recall, $E_k(z) = \frac{1}{2\zeta(k)}G_k(L_{z,1})$ where $G_k(L) = \sum_{\omega\in L\setminus\{0\}} \frac{1}{\omega^k}$. Consider

$$p^{1-k}T_nG_k(L) = \sum_{[L:L']=n}\sum_{\omega\in L'\setminus\{0\}} \frac{1}{\omega^k} = \sum_{\omega\in L\setminus\{0\}} n_p(\omega)\omega^{-k},$$

where

$$n_p(\omega) = \sharp\{L' : [L : L'] = p, \omega \in L'\}.$$

Now, for such an $L'$, multiplication by $p$ kills $L/L'$ so $pL \subset L' \subset L$. The sublattices of index $p$ in $L$ correspond to the subgroups of order $p$ in $L/pL \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ of which there are $p+1$. So if $\omega \in pL$ then $\omega$ is in all the $L'$ and $n_p(\omega) = p+1$. If $\omega \notin pL$ then $pL + \mathbb{Z}\omega$ is the unique lattice of index $p$ in $L$ containing $\omega$ so $n_p(\omega) = 1$. Hence

$$\begin{aligned} p^{1-k}T_nG_k(L) &= \sum_{\omega\in pL\setminus\{0\}} (p+1)\omega^{-k} + \sum_{\omega\in L\setminus pL} \omega^{-k} \\ &= \sum_{\omega\in pL\setminus\{0\}} p\omega^{-k} + \sum_{\omega\in L\setminus\{0\}} \omega^{-k} \\ &= \sum_{\omega\in L\setminus\{0\}} p(p\omega)^{-k} + \sum_{\omega\in L\setminus\{0\}} \omega^{-k} \\ &= (1 + p^{-k+1})G_k(L). \end{aligned}$$

This implies that $E_k$ is an eigenform with $\lambda_p = p^{k-1}(1 + p^{1-k}) = p^{k-1} + 1 = \sigma_{k-1}(p)$. □

The underlying philosophy is that eigenforms are the modular forms of arithmetic interest. In particular, we have:

**Lemma 2.3.15.** If $f$ is a normalized eigenform then the coefficients in its $q$-expansion are algebraic integers.

*Proof.* By Exercise 2.2.15, $M_k$ has a basis with integral coefficients. Therefore with respect to this basis $T_n$ can be viewed as a matrix with integral coefficients. The characteristic polynomial of $T_n$ with respect to this basis is monic and integral, and hence its eigenvalues are algebraic integers. As $f$ is a normalized eigenform the $n$-th coefficient in its $q$-expansion is the eigenvalue of $T_n$ on $f$. □

**Theorem 2.3.16.** The space $M_k$ has a basis of eigenforms.

We delay the proof of the theorem until the end of the notes when we have developed more machinery. We will prove $S_k$ has a basis of eigenforms by defining an inner product on $S_k$ and showing that the $T_n$ are normal operators with respect to this inner product, then apply the Spectral Theorem (see Appendix C). This implies $M_k$ has a basis of eigenforms as $E_k$ is an eigenform by Proposition 2.3.14.

For $4 \leqslant k \leqslant 10$ even and $k = 14$, $M_k = \mathbb{C}E_k$ and $\{E_k\}$ is a basis of eigenforms. For $k = 12$, $\{E_k, \Delta\}$ is a basis of eigenforms. However for the first interesting case when $\dim_{\mathbb{C}}(S_k) > 1$ namely $k = 24$. We have $\dim M_{24} = 3$ and $E_{24}$ is an eigenform, but neither $\Delta^2, E_{12}\Delta$ are eigenforms....

**Exercise 2.3.17.** Compute the matrix of the Hecke operator $T_2$ acting on $S_{24}$ with respect to the basis $E_4^3\Delta$,$\Delta^2$ of $S_{24}$, and show that its characteristic polynomial is irreducible. What does this mean about the eigenforms of level 24?

**Exercise 2.3.18.** Let $V$ be a three dimensional real vector space, and let $\mathrm{Latt}_V$ denote the space of lattices in $V$. For $a, b$ positive integers with $a$ dividing $b$, define a correspondence $T_{a,b}$ on $\mathrm{Latt}_V$

$$T_{a,b}[L] = \sum_{\substack{L' \subseteq L \\ L/L' \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}}} [L'],$$

i.e. the sum over the sublattices $L' \subset L$ such that $L/L'$ is isomorphic to $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

(i) Show that if $(b, b') = 1$,then $T_{a,b}T_{a',b'} = T_{aa',bb'}$.

(ii) Fix a prime p, and express $T_{1,p^2}$, $T_{1,p^3}$, and $T_{p,p^2}$ as polynomials in $T_{1,p}$, $T_{p,p}$, and the rescaling by $p$ operator $R_p$.

## 2.4 The $L$-function of a modular form

### 2.4.1 The Riemann zeta function and Dirichlet $L$-functions

Given a sequence $(a_n)_{n=1}^{\infty}$ of complex numbers we can consider the Dirichlet series

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

The primordial example is $a_n = 1$ for all $n$: the *Riemann zeta function*

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

It satisfies the following nice properties:

(i) For $\mathbf{Re}(s) > 1$ the series converges absolutely;

(ii) For $\mathbf{Re}(s) > 1$, we have the *Euler product*

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

(iii) The function $\zeta$ extends to a meromorphic function on $\mathbb{C}$ with a simple pole at $s = 1$ and putting $\Lambda = \pi^{-s/2} s(s-1)\Gamma\left(\frac{s}{2}\right)\zeta(s)$ it satisfies the functional equation

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

The second class of examples usually considered are the Dirichlet $L$-functions. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a *primitive homomorphism* (a homomorphism not coming from a homomorphism $(\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{C}^\times$ via reduction modulo $M$ for any divisor $M$ of $N$). Put $a_n = \chi(n)$ if $(n, N) = 1$ and 0 otherwise. Then we define

$$L(s, \chi) = \sum_{n \geqslant 1} \frac{a_n}{n^s}.$$

(i) For $\mathbf{Re}(s) > 1$ the series converges absolutely;

(ii) For $\mathbf{Re}(s) > 1$, we have the *Euler product*

$$L(s, \chi) = \prod_{\text{primes } p} \frac{1}{1 - \chi(p)p^{-s}};$$

(iii) The function $L(-, \chi)$ extends to a meromorphic function on $\mathbb{C}$ with a functional equation relating $L(s, \chi)$ and $L(1 - s, \chi)$.

Like modular forms, these *L-functions* encode arithmetical structure which can be otherwise difficult to study. Applications include:

(i) The prime number theorem: the number $\pi(x)$ of primes less than or equal to $x$ satisfies $\pi(x) \sim x/\log(x)$.

(ii) Dirichlet's theorem on arithmetic progressions: For all $a, d \in \mathbb{Z}$ coprime there are infinitely many primes in the sequence

$$a, a + d, a + 2d, a + 3d, \ldots.$$

Two problems related to $L$-functions: the *Riemann hypothesis* and the *BSD conjecture*, both have \$1 million dollar prizes for successful solutions, see:

`http://www.claymath.org/millennium-problems`

### 2.4.2 The $L$-function of a modular form

Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ be a modular form of weight $k$. The (Hecke) *$L$-function* of $f$ is:

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

**Theorem 2.4.1.** (i) $L(s,f)$ converges absolutely for $\mathbf{Re}(s) > k$. Moreover, if $f \in S_k$ the $L(s,f)$ converges absolutely for $\mathbf{Re}(s) > k/2+1$.

(ii) If $f$ is a normalized eigenform, then $L(s,f)$ has an Euler product

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

(iii) If $f \in S_k$, then $L(s,f)$ extends to entire function on $\mathbb{C}$ and, putting $\Lambda(s,f) = (2\pi)^{-s}\Gamma(s)L(s,f)$, satisfies the functional equation

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

We note that there are more general statements than (iii) which include any modular form $f$, but we content ourselves with the case of cusp forms.

**Example 2.4.2.** (i) We saw in Proposition 2.3.14 that $E_k$ is a non-normalized eigenform, and if we consider the normalized eigenform $f(z) = \frac{B_k}{2k}E_k(z) = \sum_{n=0}^{\infty} a(n)q^n$, we have $a(p) = 1 + p^{k-1}$ so that

$$\begin{aligned} L(s,f) &= \prod_{p \text{ prime}} \frac{1}{1 - (1+p^{k-1})p^{-s} + p^{k-1-2s}} \\ &= \prod_{p \text{ prime}} \frac{1}{(1-p^{-s})} \frac{1}{(1-p^{k-1}p^{-s})} = \zeta(s)\zeta(s-k+1). \end{aligned}$$

(ii) For $\Delta(z) = \sum_{n=1}^{\infty} \tau(n)q^n \in S_{12}$ we have

$$\begin{aligned} L(\Delta,s) &= \prod_{p \text{ prime}} \frac{1}{1 - \tau(p)p^{-s} + p^{11-2s}} \\ \Lambda(\Delta,s) &= \Lambda(\Delta, 12-s). \end{aligned}$$

*Proof of Theorem 46.* (i) We claim that for $f \in M_k$ there is a constant $c \in \mathbb{R}$ such that $|a(n)| < cn^{k-1}$. Then for $\mathbf{Re}(s) = k+\epsilon$ with $\epsilon$ positive we have $|n^{-s}| = n^{-k-\epsilon}$ and hence

$$|a_n n^{-s}| = cn^{-(1+\epsilon)},$$

so the series converges absolutely. We also claim that if $f \in S_k$ there is a constant $c \in \mathbb{R}$ such that $|a(n)| < cn^{k/2}$, and the $S_k$ statement follows similarly. We prove the claims after the proof of the Theorem.

(ii) As for $(m,n) = 1$ we have $a(m)a(n) = a(mn)$, in the region of the absolute convergence, we have

$$\sum_{n=1}^{\infty} a(n)n^{-s} = \prod_{\text{prime } p} \sum_{m=0}^{\infty} a(p^m)p^{-ms}.$$

Moreover

$$\begin{aligned}(1 - a(p)p^{-s} + &p^{k-1}p^{-2s})(1 + a(p)p^{-s} + a(p^2)p^{-2s} + \cdots) \\ &= 1 + \sum_{r\geqslant 2}(a(p^{r+1}) - a(p)a(p^r) + p^{k-1}a(p^{r-2}))p^{-rs} = 1,\end{aligned}$$

the final equality by Corollary 2.3.13. Hence

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

(iii) Let

$$\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt$$

denote Euler's Gamma function, integration by parts gives $\Gamma(s+1) = s\Gamma(s)$ and extends $\Gamma$ to a nowhere vanishing meromorphic function on the entire complex plane with poles at the negative integers. It is a special case of a Mellin transform. Given $h : \mathbb{C} \to \mathbb{C}$ define its Mellin transform

$$g(s) = \int_0^\infty h(t)t^{s-1}dt,$$

whenever the integral converges. The Gamma function is the Mellin transform of $e^{-t}$.

From now on $f \in S_k$ and $f(z) = \sum_{n=1}^\infty a(n)q^n$. Consider

$$\begin{aligned}\int_0^\infty f(iy)y^{s-1}dy &= \sum_{n=1}^\infty a_n \int_0^\infty e^{-2\pi ny}y^{s-1}dy \\ &= \sum_{n=1}^\infty a_n \left(\frac{1}{2\pi n}\right)^s \int_0^\infty e^{-t}t^{s-1}dt \\ &= (2\pi)^{-s}\Gamma(s)\sum_{n=1}^\infty a_n n^{-s}.\end{aligned}$$

interchanging the sum and integral is justified where the sum is absolutely convergent, and we change variables via $t = 2\pi ny$.

Now consider splitting the integral at 1 and change variables $y \to 1/y$ in the first integral, under which 1 is fixed:

$$\begin{aligned}\int_0^1 f(iy)y^{s-1}dy + \int_1^\infty f(iy)y^{s-1}dy &= -\int_1^\infty f\left(i/y\right)\left(1/y\right)^{s-1}d(1/y) + \int_1^\infty f(y)y^{s-1}dy \\ &= -\int_1^\infty f\left(i/y\right)\left(1/y\right)^{s-1}d(1/y) + \int_1^\infty f(iy)y^{s-1}dy \\ &= \int_1^\infty f\left(iy\right)\left(iy\right)^k y^{-1-s}dy + \int_1^\infty f(iy)y^{s-1}dy \\ &= i^k\int_1^\infty f\left(iy\right)y^{k-s-1}dy + \int_1^\infty f(iy)y^{s-1}dy \\ &= \int_1^\infty f(iy)(y^{s-1} + i^k y^{k-s-1})dy.\end{aligned}$$

(Noting where we used $f(-1/iz) = f(i/z) = (iz)^k f(iz)$, thanks to the modular transformation property applied with the matrix $S$.)

Now this integral converges to a holomorphic function because $f(iy)$ decreases exponentially as $y \to \infty$, its relation to $L(s, f)$ giving the analytic extension of the $L$-function. We put $\Lambda(s, f) = \int_1^\infty f(iy)(y^{s-1} + (-1)^{k/2} y^{k-s-1})dy$.

Finally, we have

$$\begin{aligned}\Lambda(k-s, f) &= \int_1^\infty f(iy)(y^{k-s-1} + (-1)^{k/2} y^{s-1})dy \\ &= (-1)^{k/2} \int_1^\infty f(iy)((-1)^{k/2} y^{k-s-1} + y^{s-1})dy \\ &= (-1)^{k/2} \Lambda(s, f).\end{aligned}$$

□

During the proof of (i) we used a claim we prove now:

**Lemma 2.4.3.** For $f(z) = \sum_{n=0}^\infty a(n)q^n$ a modular form of weight $k$ there is a constant $c \in \mathbb{R}$ such that $|a(n)| < cn^{k-1}$ and if $f$ is a cusp form there is a constant $c \in \mathbb{R}$ such that $|a(n)| < cn^{k/2}$.

*Proof.* As any $f \in M_k$ is a linear combination of an Eisenstein series with a cusp form and as Eisenstein series satisfy the first bound on their coefficients it remains to show for $f(z) = \sum_{n=1}^\infty a(n)q^n \in S_k$ we have $|a(n)| < cn^{k/2}$.

Let $\widetilde{f}(q) = f(z) = \sum_{n \geqslant 1} a(n)q^n$ be a cusp form of weight $k$. From the $q$-expansion, we see that $\widetilde{f}(q)/q$ is bounded as $q$ approaches 0 hence

$$\frac{|f(z)|}{e^{-2\pi \mathrm{Im}(z)}}$$

is bounded as $\mathrm{Im}(z) \to \infty$. That is, as $\mathrm{Im}(z) \to \infty$, $|f(z)|$ decreases exponentially quickly. Therefore so does

$$\Phi(z) = |f(z)|(\mathrm{Im}(z))^{k/2}.$$

For all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we have

$$\begin{aligned}\Phi(\gamma \cdot z) &= |f(\gamma \cdot z)| \mathrm{Im}(\gamma \cdot z)^{k/2} \\ &= \Phi(z),\end{aligned}$$

by modularity of $f$ (the modular transformation law $(\star)$) and Lemma 2.1.1. In particular, $\Phi$ is determined by its values on the fundamental domain $\mathcal{D}$. Since $\Phi(z) \to 0$ as $\mathrm{Im}(z) \to \infty$, $\Phi$ is bounded on $\mathcal{D}$ and hence on $\mathbb{H}$. Therefore, there exists a positive constant $M$ such that

$$|f(z)| \leqslant M(\mathrm{Im}(z))^{-k/2},$$

for all $z \in \mathbb{H}$. Now fix $y > 0$ and let $z$ range along the straight line $L_y$ from $-\frac{1}{2} + iy$ to $\frac{1}{2} + iy$ in $\mathcal{D}$. Then $q$ moves counterclockwise around a circle $C_y$ of radius $e^{-2\pi y}$ around 0. By Cauchy's formula for the meromorphic expansion at 0 of $\widetilde{f}$ we have

$$\begin{aligned}|a(n)| &= \left| \frac{1}{2\pi} \int_{C_y} q^{-n+1} \widetilde{f}(q) dq \right| \\ &= \left| \int_{-1/2}^{1/2} f(z) e^{-2\pi i n z} dz \right| \\ &\leqslant e^{-2\pi n y} \sup_{z \in L_y} |f(z)| \\ &\leqslant M y^{-k/2} e^{-2\pi n y}.\end{aligned}$$

Taking $y = 1/n$ gives the required bound. □

**Remark 2.4.4.** Hecke also proved a converse theorem: a Dirichlet series satisfying a functional equation of the type in Theorem 46, and satisfying some regularity and growth hypothesis comes from a modular form of weight $k$. Moreover, it has an Euler product if and only if the modular form is a normalized eigenform.

## 2.5 Theta series and quadratic forms

### 2.5.1 Quadratic forms

Recall, a quadratic form (over $\mathbb{Z}$) is a homogeneous polynomial of degree 2 with integral coefficients, e.g.

$$z_1^2 + 2z_1z_2 + 17z_3^2 + z_4^2 = 0.$$

Modular forms have applications to an interesting problem involving quadratic forms: how many different ways are there to represent an integer by a quadratic form? More precisely, given a quadratic form $Q(z_1, \ldots, z_n)$ and $m \in \mathbb{Z}$ what is

$$\sharp\{(x_1, \ldots, x_n) \in \mathbb{Z}^n : Q(x_1, \ldots, x_n) = m\}.$$

Using modular forms, one can recover classical results such as Lagrange's four square theorem: every non-negative integer is a sum of four squares. However, tackling general quadratic forms, for example $z_1^2 + \cdots + z_n^2$, would require *higher level* and *half-integral weight* modular forms so we restrict ourselves to special cases here. We do not consider half-integral weight modular forms in this course, the interested reader can consult [3, Chapter IV].

### 2.5.2 Lattices and associated quadratic forms

Let $\Lambda$ be a lattice in $\mathbb{R}^n$. By Lemma 2.1.16, there exists a basis $\{v_1, \ldots, v_n\}$ of $\mathbb{R}^n$ such that

$$\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n.$$

We put $B = (v_1 \cdots v_n)$ the matrix of (column) basis vectors and let $A$ be the symmetric $n$ by $n$ matrix

$$A = B^T B = (v_i \cdot v_j),$$

where the $\cdot$ indicates the standard dot product on $\mathbb{R}^n$.

The volume $v(\Lambda)$ of the lattice $\Lambda$ is defined to be the volume of the fundamental parallelogram in $\mathbb{R}^n$:

$$\begin{aligned} v(\Lambda) &= \mathrm{vol}\{c_1v_1 + \cdots + c_nv_n : c_i \in [0,1]\} \\ &= \det(B) = \sqrt{\det(A)}. \end{aligned}$$

Notice that $\det(A)$ is invertible and positive.

**Definition 2.5.1.** The *dual lattice* $\Lambda^\vee$ of $\Lambda$ is defined to be the set

$$\Lambda^\vee = \{x \in \mathbb{R}^n : x \cdot v \in \mathbb{Z}\}.$$

For example, $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$ is self dual whereas $(2\mathbb{Z}^n)^\vee = \frac{1}{2}\mathbb{Z}^n$.

Let $w_1, \dots, w_n$ be the dual basis of $v_1, \dots, v_n$, that is $w_i$ is the unique vector in $\mathbb{R}^n$ such that

$$w_i \cdot v_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwises.} \end{cases}$$

**Lemma 2.5.2.** We have $\Lambda^\vee = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n$ and in particular $\Lambda^\vee$ is a lattice.

*Proof.* Let $x \in \mathbb{R}^n$ and write $x$ in terms of the basis $w_1, \dots, w_n$

$$x = \sum_{i=1}^n a_i w_i.$$

Then $x \in \Lambda^\vee$ if and only if $x \cdot v \in \mathbb{Z}$ for all $v \in \Lambda$, which happens if and only if $x \cdot v_j \in \mathbb{Z}$ for all $1 \leqslant j \leqslant n$. But, for all $1 \leqslant j \leqslant n$,

$$\sum_{i=1}^n a_i w_i \cdot v_j \in \mathbb{Z},$$

if and only if $a_i \in \mathbb{Z}$ for all $1 \leqslant i \leqslant n$ which is what we needed to show. □

Notice that if we take $C = A^{-1}$, $C = (C_{ij})$ then $w_i = \sum_{j=1}^n C_{ij} v_j$ as

$$\sum_{j=1}^n C_{ij} v_j \cdot v_k = \sum_{j=1}^n C_{ij} A_{jk} = \begin{cases} 1 & \text{if } i = k \\ 0 & \text{otherwise.} \end{cases}$$

**Lemma 2.5.3.** We have $\Lambda = \Lambda^\vee$ if and only if $A \in \mathrm{SL}_n(\mathbb{Z})$.

*Proof.* Suppose $\Lambda = \Lambda^\vee$ then $\Lambda \subseteq \Lambda^\vee$ implies that $x \cdot y \in \mathbb{Z}$ for all $x, y \in \Lambda$ and hence $A \in M_n(\mathbb{Z})$. Similarly, $C \in M_n(\mathbb{Z})$ and hence $A \in \mathrm{GL}_n(\mathbb{Z})$ and $\det(A) = \pm 1$. However, we have already seen that $\det(A)$ is positive hence $A \in \mathrm{SL}_n(\mathbb{Z})$.

Conversely, if $A \in \mathrm{SL}_n(\mathbb{Z})$, then $C \in \mathrm{SL}_n(\mathbb{Z})$ has integral coeffients and as $w_i = \sum_{j=1}^n C_{ij} v_j$ we have $w_i \in \Lambda$ and hence $\Lambda^\vee \subseteq \Lambda$ by Lemma 2.5.2. Similarly, as $A \in \mathrm{SL}_n(\mathbb{Z})$ we have $v_i \in \Lambda^\vee$ and hence $\Lambda \subseteq \Lambda^\vee$. □

**Assumption 1:** $\Lambda$ is self dual, i.e. $\Lambda = \Lambda^\vee$.

Then $\Lambda$ gives rise to a quadratic form over $\mathbb{Z}$

$$\begin{aligned} Q_\Lambda(z_1, \dots, z_n) &= (z_1 v_1 + \cdots + z_n v_n) \cdot (z_1 v_1 + \cdots + z_n v_n) \\ &= \begin{pmatrix} z_1 & \cdots & z_n \end{pmatrix} A \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}. \end{aligned}$$

**Question:** For $m \in \mathbb{Z}$ how many times does $Q_\Lambda(z)$ represent $m$? In other words, for how many $z \in \mathbb{Z}^n$ are such that $Q_\Lambda(z) = m$.

The quadratic form $Q_\Lambda$ is positive definite, hence the answer is 0 if $m < 0$, 1 if $m = 0$, and finite if $m > 0$.

**Assumption 2:** For all $z \in \mathbb{Z}^n$, $Q_\Lambda(z) \in 2\mathbb{Z}$, i.e. is even.

This is not strictly speaking necessary, we make the assumption to avoid modular forms of higher level and half integral weight, but it does rule out interesting examples e.g. $z_1^2 + \cdots + z_n^2$. We now give an example that satisfies both assumptions:

**Example 2.5.4.** Let $e_1, \ldots, e_n$ be the standard basis of $\mathbb{R}^8$, i.e. $e_i$ is the vector is 1 in the $i$-th place and 0's in all other places. Let $\Lambda_8 = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ be the lattice in $\mathbb{R}^8$ be defined by

$$\begin{aligned} v_1 &= \frac{1}{2}(e_1 - e_2 - e_3 - e_4 - e_5 - e_6 - e_7 + e_8) & v_5 &= -e_3 + e_4 \\ v_2 &= e_1 + e_2 & v_6 &= -e_4 + e_5 \\ v_3 &= -e_1 + e_2 & v_7 &= -e_5 + e_6 \\ v_4 &= -e_2 + e_3 & v_8 &= -e_6 + e_7. \end{aligned}$$

The corresponding matrix is

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

which has determinant 1 so $\Lambda_8$ satisfies Assumption 1 by Lemma 2.5.3. Moreover,

$$Q_{\Lambda_8}(z_1, \ldots, z_8) = 2(z_1^2 + z_2^2 + z_3^2 + z_4^2 + z_5^2 + z_6^2 + z_7^2 + z_8^2 - z_1z_3 - z_2z_4 - z_3z_4 - z_4z_5 - z_6z_7 - z_7z_8),$$

so $\Lambda_8$ satisfies Assumption 2.

**Remark 2.5.5.** It is known that the densest possible packing of eight dimensional spheres of radius $\sqrt{2}$ in $\mathbb{R}^8$ is obtained by placing one sphere at each point in $\Lambda_8$!

**Lemma 2.5.6.** Assumptions 1 and 2 together imply that the rank of $\Lambda$ is divisible by 8.

*Proof.* Omitted, see [5, V.2.1, Corollary 2]. □

### 2.5.3 Theta series

Let $\Lambda$ be a lattice in $\mathbb{R}^n$ which satisfies Assumptions 1 and 2. Let

$$\begin{aligned} a_m(\Lambda) &= \sharp\{z \in \mathbb{Z}^n : Q_\Lambda(z) = 2m\}, \\ &= \sharp\{x \in \Lambda : x \cdot x = 2m\}. \end{aligned}$$

**Definition 2.5.7.** Define the theta series attached to $\Lambda$ to be

$$\theta_\Lambda(q) = \sum_{m=0}^{\infty} a_m(\Lambda) q^m = \sum_{x \in \Lambda} q^{\frac{1}{2}(x \cdot x)}.$$

Putting $q = e^{2\pi i z}$, we have:

**Theorem 2.5.8.** The theta series $\theta_\Lambda(z)$ is a modular form of weight $n/2$.

Before proving the theorem, we note some consequences:

We have $\theta_{\Lambda_8}$ is a modular form of weight 4 and its $q$-expansion begins $1 + \cdots$, hence $\theta_{\Lambda_8} = E_4$, and

$$a_m(\Lambda_8) = 240\sigma_3(m),$$

for $m \geqslant 1$. We have determined $a_m(\Lambda_8)$ for all $m$! In higher weight (hence higher rank lattices), more work is required in order to write $\theta_\Lambda$ in terms of our basis vectors with known $q$-expansions, but to obtain an exact formula we only need to work out finitely many $a_m(\Lambda)$ to compare $q$-expansions.

In fact, we also have a uniform result: As the coefficient in the $q$-expansion of $\theta_\Lambda$ is 1 we can write

$$\theta_\Lambda = E_k + g$$

with $g \in S_k$ a cusp form of weight $k = n/2$. Writing its $q$-expansion $g(z) = \sum_{m=1}^{\infty} c(m)q^m$ we have

$$a_m(\Lambda) = -\frac{4k}{B_k}\sigma_{k-1}(m) + c(m),$$

and on the right hand side only $c(m)$ depends on $\Lambda$. By Lemma 2.4.3, $c(m)$ grows more slowly that $\frac{4k}{B_k}\sigma_{k-1}(m)$ hence

$$a_m(\Lambda) \sim -\frac{4k}{B_k}\sigma_{k-1}(m).$$

It remains to prove Theorem 2.5.8:

*Proof of Theorem 2.5.8.* The $a_m(\Lambda)$ grow at most polynomially and the coefficients in the $q$-expansion decay exponentially, hence $\theta_\Lambda(q)$ converges on the unit disc, and $\theta_\Lambda(z)$ is holomorphic on $\mathbb{H}$ and at $\infty$.

It remains to show that for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ we have

$$\theta_\Lambda(\gamma \cdot z) = (cz + d)^{n/2}\theta_\Lambda(z).$$

It is sufficient to show this for $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, i.e. that

$$\theta_\Lambda(z + 1) = \theta_\Lambda(z), \qquad \theta_\Lambda(-1/z) = z^{n/2}\theta_\Lambda(z).$$

The first equality is clear from the definition of $\theta_\Lambda$ in terms of the $q$-expansion. So it remains to show $\theta_\Lambda(-1/z) = z^{n/2}\theta_\Lambda(z)$ and for this we will use Fourier analysis on $\mathbb{R}^n$. As Fourier Analysis is not a prerequisite we will black box the results we use:

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a smooth rapidly decreasing function (i.e. for all $m \in \mathbb{Z}^{\geqslant 0}$ we have $|x|^m|f(x)| \to 0$ as $|x| \to \infty$). The Fourier transform of $f$ is

$$\widehat{f}(y) = \int_{\mathbb{R}^n} e^{-2\pi i(x \cdot y)} f(x)dx.$$

We recall three facts:

(i) $\widehat{f}$ is smooth, rapidly decreasing.

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

(iii) (Poisson summation formula): Let $\Lambda$ be a lattice in $\mathbb{R}^n$ then

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

Now fix $\Lambda = \Lambda^\vee$ and let $\Lambda_t = t^{1/2}\Lambda$. Then $\Lambda_t^\vee = t^{-1/2}\Lambda^\vee = t^{-1/2}\Lambda = \Lambda_{t^{-1}}$. Hence $v(\Lambda_t) = t^{n/2}$ as $v(\Lambda) = 1$ by Lemma 2.5.3. We now apply the Poisson summation formula to $\Lambda_t$ and $f(x) = e^{-\pi(x\cdot x)}$, giving the identity:

$$\sum_{x\in\Lambda_t} e^{-\pi(x\cdot x)} = t^{n/2} \sum_{x\in\Lambda_{t^{-1}}} e^{-\pi(x\cdot x)}.$$

Rewriting this in terms of $\Lambda$ gives us

$$\sum_{x\in\Lambda} e^{-t\pi(x\cdot x)} = t^{n/2} \sum_{x\in\Lambda_{t^{-1}}} e^{-t^{-1}\pi(x\cdot x)}. \qquad (\dagger)$$

Now we return to showing $\theta_\Lambda(-1/z) = z^{n/2}\theta_\Lambda(z)$. As $\theta_\Lambda(-1/z) - z^{n/2}\theta_\Lambda(z)$ is analytic in $z$ if it is non-zero then its zeroes are isolated. So it suffices to show this equality on the line $z = it$ with $t > 0$, i.e. it suffices to show that $\theta_\Lambda(-1/it) = z^{n/2}\theta_\Lambda(it)$. However, by definition

$$\theta_\Lambda(-1/it) = \sum_{x\in\Lambda} e^{2\pi i(-1/it)\frac{1}{2}(x\cdot x)} = \sum_{x\in\Lambda} e^{-\frac{\pi}{t}(x\cdot x)};$$
$$(it)^{n/2}\theta_\Lambda(it) = t^{n/2} \sum_{x\in\Lambda} e^{-t\pi(x\cdot x)}.$$

the equality in the second line follows as $8 \mid n$ by Lemma 2.5.6. Hence $(\dagger)$ implies $\theta_\Lambda(-1/it) = z^{n/2}\theta_\Lambda(it)$ which is what we needed to show. □

**Remark 2.5.9.** Without Assumption 2, half integral powers of $q$ would have appeared in the $q$-expansion of $\theta_\Lambda$. In these cases, $\theta_\Lambda$ would not satisfy the modular transformation law $(\star)$ for $\mathrm{SL}_2(\mathbb{Z}) = \langle S, T\rangle$, but for the subgroup generated by $S$ and $T^2$.

# Chapter 3

# Modular forms of higher level

## 3.1 Modular forms for congruence subgroups

### 3.1.1 Congruence subgroups

Remark 2.5.9, suggests we should generalize our definition of modular forms to include functions satisfying the modular transformation law ($\star$) for certain subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

The group $\mathrm{SL}_2(\mathbb{Z})$ has an infinite family of normal subgroups: Let $N$ be a positive integer and define the principal congruence subgroup of level $N$ to be

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

it is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$ as it is the kernel of the reduction modulo $N$ homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

**Definition 3.1.1.** A congruence subgroup of $\mathrm{SL}_2(\mathbb{Q})$ of level $N$ is a subgroup $\Gamma$ such that

$$\Gamma(N) \leqslant \Gamma \leqslant \mathrm{SL}_2(\mathbb{Q})$$

with $[\Gamma : \Gamma(N)]$ finite.

Notice that:

(i) If $\Gamma$ is a congruence subgroup of level $N$ then it is a congruent subgroup of level $N'$ for all multiples $N'$ of $N$.

(ii) Congruence subgroups are closed under intersection as $\Gamma(NM) \subseteq \Gamma(N) \cap \Gamma(M)$.

**Example 3.1.2.** For example, we define

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

to be the subgroup of all matrices in $\Gamma$ which are upper triangular modulo $N$. And

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

the subgroup of all matrices in $\Gamma$ which are upper triangular unipotent modulo $N$.

**Lemma 3.1.3.** Let $\gamma \in \mathrm{GL}_2(\mathbb{Q})$ and $\Gamma$ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Q})$. Then $\gamma\Gamma\gamma^{-1}$ is a congruence subgroup.

*Proof.* As $\Gamma$ is a congruence subgroup there exists $N$ such that $\Gamma(N) \leqslant \Gamma$ with finite index. Hence $\gamma\Gamma(N)\gamma^{-1} \leqslant \gamma\Gamma\gamma^{-1}$ with finite index, so it suffices to show there exists $M$ such that $\Gamma(M) \leqslant \gamma\Gamma(N)\gamma^{-1}$ with finite index.

Notice that

$$\Gamma(N) = \mathrm{SL}_2(\mathbb{Q}) \cap \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + NM_2(\mathbb{Z}) \right\}.$$

Hence

$$\begin{aligned} \gamma\Gamma(N)\gamma^{-1} &= \gamma\,\mathrm{SL}_2(\mathbb{Q})\gamma^{-1} \cap \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + N\gamma M_2(\mathbb{Z})\gamma^{-1} \right\} \\ &= \mathrm{SL}_2(\mathbb{Q}) \cap \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + N\gamma M_2(\mathbb{Z})\gamma^{-1} \right\}. \end{aligned} \qquad (\dagger)$$

Choose $a \in \mathbb{Z}$ such that $a\gamma$ and $a\gamma^{-1}$ lie in $M_2(\mathbb{Z})$. Then

$$a\gamma^{-1}M_2(\mathbb{Z})a\gamma \subseteq M_2(\mathbb{Z}).$$

Hence, conjugating by $\gamma$ we have

$$a^2M_2(\mathbb{Z}) \subseteq \gamma M_2(\mathbb{Z})\gamma^{-1}.$$

Therefore, from ($\dagger$), we have

$$\Gamma(a^2N) \subseteq \gamma\Gamma(N)\gamma^{-1}.$$

Applying the same argument to $\gamma^{-1}\Gamma(a^2N)\gamma$ we get

$$\gamma\Gamma(a^4N)\gamma^{-1} \subseteq \Gamma(a^2N) \subseteq \gamma\Gamma(N)\gamma^{-1}.$$

As $\gamma\Gamma(a^4N)\gamma^{-1}, \gamma\Gamma(N)\gamma^{-1}$ are both finite index in $\gamma\,\mathrm{SL}_2(\mathbb{Z})\gamma^{-1}$, $\gamma\Gamma(a^4N)\gamma^{-1}$ is finite index in $\gamma\Gamma(N)\gamma^{-1}$, and hence $\Gamma(a^2N)$ is finite index in $\gamma\Gamma(N)\gamma^{-1}$. ☐

**Example 3.1.4.** Let $\gamma = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$, then

$$\gamma^{-1}\,\mathrm{SL}_2(\mathbb{Z})\gamma = \left\{ \begin{pmatrix} a & p^{-1}b \\ pc & d \end{pmatrix} : ad - bc = 1 \right\}, \text{ and } \mathrm{SL}_2(\mathbb{Z}) \cap \gamma^{-1}\,\mathrm{SL}_2(\mathbb{Z})\gamma = \Gamma_0(p).$$

**Exercise 3.1.5.** Show that the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is surjective for any $n > 1$. Show that the map $\mathrm{GL}_2(\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is not surjective for any $n > 6$.

**Exercise 3.1.6.** Let $p$ be prime.

(i) Show that $|\,\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})| = p(p^2 - 1)$.

(ii) Show by induction on $r$ that $|\,\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})| = p^{3r}(1 - \frac{1}{p^2})$.

(iii) Show that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N}(1 - \frac{1}{p^2})$.

(iv) Show that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] = N^2 \prod_{p|N}(1 - \frac{1}{p^2})$.

(v) Show that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N}(1 + \frac{1}{p})$.

### 3.1.2 Modular forms for congruence subgroups

We start with the following useful notation, which we use all the way through the rest of the course.

**Definition 3.1.7.** For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})^+$ and $z \in \mathbb{C}$, we define

$$j(\gamma, z) = (cz + d),$$

this is called the *automorphy factor*, and we put

$$f|_{k,\gamma}(z) = \det(\gamma)^{k-1} j(\gamma, z)^{-k} f(\gamma \cdot z).$$

Notice that, when $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the modular transformation law $(\star)$ for $\gamma$ is equivalent to $f \mid_{k,\gamma}= f$.

**Lemma 3.1.8.** For $\gamma, \gamma' \in \mathrm{GL}_2(\mathbb{R})^+$ and $k \in \mathbb{Z}$ we have

(i) $j(\gamma'\gamma, z) = j(\gamma', \gamma \cdot z) j(\gamma, z)$;

(ii) $(f|_{k,\gamma})|_{k,\gamma'} = f|_{k,\gamma\gamma'}$.

*Proof.* (i) We have

$$\gamma \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} az + b \\ cz + d \end{pmatrix} = \begin{pmatrix} \gamma \cdot z \\ 1 \end{pmatrix} j(\gamma, z).$$

Hence

$$\begin{aligned} j(\gamma'\gamma, z) \begin{pmatrix} \gamma'\gamma \cdot z \\ 1 \end{pmatrix} &= \gamma'\gamma \begin{pmatrix} z \\ 1 \end{pmatrix} \\ &= \gamma' \begin{pmatrix} \gamma \cdot z \\ 1 \end{pmatrix} j(\gamma, z) \\ &= \begin{pmatrix} \gamma'\gamma \cdot z \\ 1 \end{pmatrix} j(\gamma', \gamma \cdot z) j(\gamma, z). \end{aligned}$$

Hence

$$j(\gamma'\gamma, z) = j(\gamma', \gamma \cdot z) j(\gamma, z).$$

(ii) We have

$$\begin{aligned} (f \mid_{k,\gamma}) \mid_{k,\gamma'} (z) &= \det(\gamma')^{k-1} j(\gamma', z)^{-k} f \mid_{k,\gamma} (\gamma' \cdot z) \\ &= \det(\gamma)^{k-1} \det(\gamma')^{k-1} j(\gamma', z)^{-k} j(\gamma, \gamma' \cdot z) f(\gamma\gamma' \cdot z) \\ &= \det(\gamma\gamma')^{k-1} j(\gamma\gamma', z)^{-k} f(\gamma\gamma' \cdot z) \\ &= f \mid_{k,\gamma\gamma'} (z). \end{aligned}$$

□

**Definition 3.1.9.** Let $\Gamma$ be a congruence subgroup. A function $f : \mathbb{H} \to \mathbb{C}$ is called *weakly modular of level* $\Gamma$ and weight $k$ if it is meromorphic on $\mathbb{H}$ and, for all $\gamma \in \Gamma$,

$$f|_{k,\gamma} = f.$$

**Remark 3.1.10.** (i) If $\Gamma' \leqslant \Gamma$ is another congruent subgroup and $f$ is weakly modular of level $\Gamma$ and weight $k$ then it is also weakly modular of level $\Gamma'$ and weight $k$.

(ii) If $\gamma \in \mathrm{GL}_2(\mathbb{Q})$ and $f$ is weakly modular of level $\Gamma$ and weight $k$, then $f|_{k,\gamma}$ is weakly modular of level $\gamma^{-1}\Gamma\gamma$, as for $\gamma \in \gamma^{-1}\Gamma\gamma$

$$(f|_{k,\gamma})|_{k,\gamma^{-1}\delta\gamma} = f|_{k,\gamma'},$$

by Lemma 3.1.8. For example, if $f$ is weakly modular of level $\mathrm{SL}_2(\mathbb{Z})$ and weight $k$ then $f|_{k,\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)}$ is weakly modular for $\begin{pmatrix} p^{-1} & 0 \\ 0 & 1 \end{pmatrix} \mathrm{SL}_2(\mathbb{Z}) \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and hence also for $\Gamma_0(p)$.

**Lemma 3.1.11.** Let $\Gamma' \leqslant \Gamma$ be congruence subgroups and $f : \mathbb{H} \to \mathbb{C}$ be such that $f|_{k,\gamma} = f$ for all $\gamma \in \Gamma'$. Choose a set of coset representatives for $\Gamma' \backslash \Gamma$, i.e. $\Gamma = \bigsqcup_{\gamma_i \in \Gamma} \Gamma'\gamma_i$, and put

$$g = \sum_{i=1}^{n} f|_{k,\gamma_i}.$$

Then $g|_{k,\gamma} = g$ for all $\gamma \in \Gamma$ and $g$ is independent of choice of coset representatives.

*Proof.* We first show that $g$ is independent of choice. Suppose that $\Gamma'\gamma_i = \Gamma'\delta_i$ for $\delta_i \in \Gamma$. Then there exists $\gamma \in \Gamma'$ such that $\gamma_i = \gamma\delta_i$ and

$$f\mid_{k,\gamma_i} = f\mid_{k,\gamma\delta_i} = (f\mid_{k,\gamma})\mid_{k,\delta_i} = f\mid_{k,\delta_i}.$$

Hence $g$ is independent of choice of coset representatives. Now let $\gamma \in \Gamma$ then

$$g\mid_{k,\gamma} = \sum_{i=1}^{n}(f\mid_{k,\gamma_i})\mid_{k,\gamma} = \sum_{i=1}^{n} f\mid_{k,\gamma_i\gamma},$$

but this equals $g$ as $\{\gamma_i\gamma\}$ is another set of coset representatives. □

If $f$ is weakly modular of level $\Gamma$ and $\Gamma(N) \leqslant \Gamma$ then $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma'$ and $f(z+N) = f(z)$ for all $z \in \mathbb{H}$, hence there exists a meromorphic function $\widetilde{f} : \mathbb{D}^* \to \mathbb{C}$ such that

$$f(z) = \widetilde{f}(e^{2\pi i z/N}) = \widetilde{f}(q^{1/N}).$$

**Definition 3.1.12.** Let $f$ be a weakly modular function of level $\Gamma$.

(i) We say that $f$ *is meromorphic at* $\infty$ if $\widetilde{f}$ is meromorphic at 0 and so has a Laurent series expansion in $q^{1/N}$,

(ii) We say that $f$ *is holomorphic at* $\infty$ if $\widetilde{f}$ is holomorphic at 0 so has a power series expansion in $q^{1/N}$.

### 3.1.3 Fundamental domains for congruence subgroups

We now want to understand the extra conditions we need to impose to get a finite dimensional space of modular forms. For $\mathrm{SL}_2(\mathbb{Z})$, to compute the dimension of spaces of modular forms we first needed a better understanding of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$.

From now on, we suppose that $\Gamma \leqslant \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup contained in $\mathrm{SL}_2(\mathbb{Z})$.

This is not a strong assumption, as every congruence subgroup is conjugate to a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Our next goal is to understand the action of $\Gamma$ on $\mathbb{H}$ in terms of the fundamental domain $\mathcal{D}$ for $\mathrm{SL}_2(\mathbb{Z})$ acting on $\mathbb{H}$.

Recall, we showed that the set

$$\mathcal{D} = \{z \in \mathbb{H} : |z| \geqslant 1, |\mathbf{Re}(z)| \leqslant 1/2\},$$

is a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$. We decompose $\mathrm{SL}_2(\mathbb{Z})$ into $\pm\Gamma$-cosets

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i=1}^{d} \gamma_i(\pm\Gamma),$$

where $d = [\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma]$, and put

$$\mathcal{D}_\Gamma = \bigcup_{i=1}^{d} \gamma_i^{-1} \cdot \mathcal{D}.$$

**Example 3.1.13.** Let

$$\Gamma = \Gamma_0(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \in 2\mathbb{Z} \right\}.$$

Then

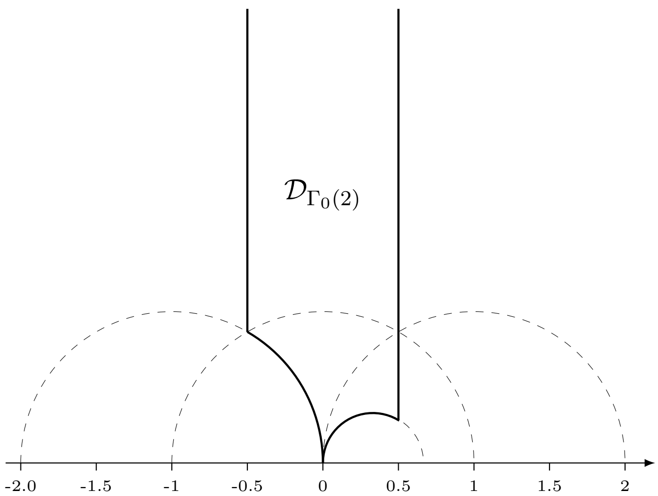
$$\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(2) \cup \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \Gamma_0(2) \cup \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \Gamma_0(2),$$

and we put

$$\gamma_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = S, \qquad \gamma_3 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} = TS.$$

Hence

$$\gamma_2^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = S^{-1}, \qquad \gamma_3^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = S^{-1}T^{-1}.$$




We now show that $\mathcal{D}_\Gamma$ is a good proxy for a fundamental domain of $\Gamma$, and we will refer to it as a *fundamental domain* for $\Gamma$.

**Theorem 3.1.14.** (i) For all $z \in \mathbb{H}$ there exists $\gamma \in \Gamma$ such that $\gamma \cdot z \in \mathcal{D}_\Gamma$.

(ii) Let $\mathcal{D}^\circ$ denote the interior of $\mathcal{D}$. For $\gamma \in \Gamma$ if $z, \gamma \cdot z \in \bigcup_{i=1}^{d} \gamma_i^{-1} \cdot \mathcal{D}^\circ$ then $\gamma \cdot z = z$. In particular, $\{z \in \mathcal{D}_\Gamma : \Gamma \cdot z \cap \mathcal{D}_\Gamma \neq z\}$ has measure zero.

*Proof.* Choose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma \cdot z \in \mathcal{D}$ then $\gamma = \pm\gamma_i\gamma'$ for some $i = 1, \ldots, d$ and $\gamma' \in \Gamma$. So $\gamma_i\gamma' \cdot z \in \mathcal{D}$ and hence $\gamma' \cdot z \in \gamma_i^{-1}\mathcal{D}$, as $\pm 1$ acts trivially on $\mathbb{H}$. Therefore, by definition, $\gamma' \cdot z \in \mathcal{D}_\Gamma$.

Suppose $z, \gamma \cdot z \in \bigcup_{i=1}^d \gamma_i^{-1} \cdot \mathcal{D}^\circ$ then there exist $i, j$ such that $\gamma_i \cdot z, \gamma_j\gamma \cdot z \in \mathcal{D}^\circ$ which implies that $\gamma_i = \gamma_j\gamma$ and $\gamma_i, \gamma_j$ are in the same coset of $\pm\Gamma$ hence $\gamma_i = \gamma_j$ and $\gamma = \pm 1$. □

One can escape $\mathcal{D}_\Gamma$ by moving to boundary points $\gamma_i^{-1}\infty$ for each $i$, a set of bad possibilities. These bad points represent the $\Gamma$-orbits in $\mathrm{SL}_2(\mathbb{Z}) \cdot \infty$.

**Lemma 3.1.15.** We have an equality of sets

$$\mathrm{SL}_2(\mathbb{Z}) \cdot \infty = \mathbb{Q} \cup \infty.$$

*Proof.* By definition,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \infty = \frac{a}{c}$$

which is in $\mathbb{Q} \cup \infty$. Any such matrix with $c = 0$ will fix $\infty$. So let $a/c \in \mathbb{Q}$ with $(a, c) = 1$ then there exists $b, d$ such that $ad - bc = 1$ and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \infty = a/c, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

□

**Definition 3.1.16.** The *cusps* of $\Gamma$ are the $\Gamma$-orbits in $\mathbb{Q} \cup \infty$.

**Example 3.1.17.** (i) The cusps for $\mathrm{SL}_2(\mathbb{Z})$ are $\mathrm{SL}_2(\mathbb{Z}) \cdot \{\infty\}$.

(ii) For $\begin{pmatrix} a & b \\ pc & d \end{pmatrix} \in \Gamma_0(p)$ we have $ad - pcb = 1$, and

$$\Gamma_0(p) \cdot \infty = \left\{ \frac{a}{pc} : (a, pc) = 1 \right\} \cup \{\infty\},$$
$$\Gamma_0(p) \cdot 0 = \left\{ \frac{b}{d} : (pb, d) = 1 \right\}.$$

We have $\mathbb{Q} \cup \infty = \Gamma_0(p) \cdot \infty \cup \Gamma_0(p) \cdot 0$, hence the cusps of $\Gamma_0(p)$ are

$$\Gamma_0(p) \cdot \infty \text{ and } \Gamma_0(p) \cdot 0.$$

**Definition 3.1.18.** (i) A weakly modular function of weight $k$ and level $\Gamma$ is called *holomorphic (respectively meromorphic) at* $\gamma \cdot \infty$ if $f|_{k,\gamma}$ is holomorphic (respectively meromorphic) at $\infty$.

(ii) A *modular form of weight* $k$ *and level* $\Gamma$ is a weakly modular function $f : \mathbb{H} \to \mathbb{C}$ of weight $k$ and level $\Gamma$ which is holomorphic on $\mathbb{H}$ and at all cusps. It is called a *cusp form* if $\nu_p(f) > 0$ for all cusps $p$, i.e. it vanishes at all cusps.

(iii) Let $M_k(\Gamma)$ denote the vector space of modular forms of weight $k$ and level $\Gamma$ and $S_k(\Gamma)$ denote the subspace of cusp forms.

Notice that $M_k = M_k(\mathrm{SL}_2(\mathbb{Z}))$ and $S_k = S_k(\mathrm{SL}_2(\mathbb{Z}))$ using our earlier notation.

**Exercise 3.1.19.** Let $\Gamma \leqslant \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup containing $\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. Let $x \in \mathbb{Q}\cup\{\infty\}$, and

$$Z_x = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma\cdot x = x\},$$

denote the stabiliser of $x$ in $\mathrm{SL}_2(\mathbb{Z})$. Let $\Gamma_x = Z_x \cap \Gamma$. The *width* of the cusp $x$ (relative to $\Gamma$) is defined to be

$$R_\Gamma(x) = [Z_x : \Gamma_x].$$

(i) For $\gamma \in \Gamma$, show that

$$R_\Gamma(\gamma\cdot x) = R_\Gamma(x).$$

(ii) For $x, y \in \mathbb{Q}\cup\{\infty\}$, let

$$Z_{x,y} = \{\delta \in \mathrm{SL}_2(\mathbb{Z}) : \delta\cdot x \in \Gamma\cdot y\}.$$

Show that for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma\cdot x = y$, $Z_{x,y}$ is equal to the double coset $\Gamma\gamma Z_x$ of elements of $\mathrm{SL}_2(\mathbb{Z})$ of the form $\gamma'\gamma z$ for $\gamma' \in \Gamma$ and $z \in Z_x$.

(iii) Let $G$ be a group, and $H$ and $K$ subgroups of finite index in $G$. Show that for any $g \in G$, the double coset $HgK = \{hgk : h \in H, k \in K\}$ is the disjoint union of $n$ cosets $Hg$, where $n$ is the index of $g^{-1}Hg \cap K$ in $K$.

(iv) Show that the sum of $R_\Gamma(x)$, as $x$ runs over a set of representatives for the $\Gamma$-orbits in $\mathbb{Q}\cup\{\infty\}$, is equal to $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$.
(Hint: write $\mathrm{SL}_2(\mathbb{Z})$ as a disjoint union of cosets $\Gamma\gamma_i$, and for each $\Gamma$-orbit $\Gamma x$ in $\mathbb{Q}\cup\{\infty\}$, count the number of such cosets that take $\infty$ to a point in $\Gamma x$.)

**Exercise 3.1.20.** (i) Find a set of representatives for the set of cusps of the congruence subgroups $\Gamma_0(4)$, $\Gamma_0(6)$, and $\Gamma_1(5)$, and find their widths.

(ii) Show that for $N$ squarefree, $\Gamma_0(N)$ has precisely one cusp of width $d$ for each divisor $d$ of $N$.

### 3.1.4 Finite dimensional spaces of modular forms

We now show that the dimension of the vector space $M_k(\Gamma)$ is finite. We will not provide dimension formulae as to prove these would require techniques we have not developed, see for example [2, Chapter 3]. Instead we use our work on $\mathrm{SL}_2(\mathbb{Z})$ to bound the dimension.

Let $f \in M_k(\Gamma)$ and decompose $\mathrm{SL}_2(\mathbb{Z})$ into $\Gamma$-cosets

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i=1}^{d} \Gamma\gamma_i,$$

put $d = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$, and set

$$g = \prod_{i=1}^{d} f\mid_{k,\gamma_i}.$$

**Lemma 3.1.21.** The function $g \in M_{dk}(\mathrm{SL}_2(\mathbb{Z}))$ and is independent of choice of coset representatives.

*Proof.* It is clearly holomorphic on $\mathbb{H}$ and at $\infty$. Replacing $\gamma_i$ with $\gamma\gamma_i$ for $\gamma \in \Gamma$ then

$$f\mid_{k,\gamma\gamma_i} = (f\mid_{k,\gamma})\mid_{k,\gamma_i} = f\mid_{k,\gamma_i},$$

so the definition is independent of choice of coset representatives. Suppose $\delta \in \mathrm{SL}_2(\mathbb{Z})$, then

$$g\mid_{dk,\delta} = \prod_{i=1}^{d}(f\mid_{k,\gamma_i})\mid_{k,\delta} = \prod_{i=1}^{d} f\mid_{k,\gamma_i\delta}.$$

However, $\gamma_i\delta$ is a set of coset representatives for $\Gamma\backslash\mathrm{SL}_2(\mathbb{Z})$, so this is equal to $g$. □

If $f$ is non-zero so is $g$. Hence as $M_{dk}(\mathrm{SL}_2(\mathbb{Z})) = 0$ for $dk < 0$, we have $M_k(\Gamma) = 0$ for $k < 0$. Moroever, as $M_0(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}$ we have $M_0(\Gamma) = \mathbb{C}$. So we now assume that $k > 0$, and we suppose that $f$ is non-zero.

By the $(k/12)$-proposition (Proposition 24) applied to $g$ which has weight $dk$ we get

$$\frac{dk}{12} = \nu_\infty(g) + \frac{\nu_i(g)}{2} + \frac{\nu_\rho(g)}{3} + \sum_{\substack{p\in\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}\\ p\neq i,\rho}} \nu_p(g). \qquad (\dagger)$$

As $g = \prod_{i=1}^d f\mid_{k,\gamma_i}$ the order of vanishing

$$\nu_p(g) = \sum_{i=1}^{d} \nu_p(f\mid_{k,\gamma_i}) = \sum_{i=1}^{d} \nu_{\gamma_i\cdot p}(f).$$

Now consider the $\mathrm{SL}_2(\mathbb{Z})$-orbit of $p$, we have

$$\mathrm{SL}_2(\mathbb{Z})\cdot p = \bigcup_{i=1}^{d} \Gamma\gamma_i\cdot p,$$

and $\gamma_i \cdot p$ runs over a set of representatives for the $\Gamma$-orbits in $\mathrm{SL}_2(\mathbb{Z})\cdot p$, each appearing at least once, but with the possibility of appearing more than once. If $\gamma_i\cdot p = \gamma_j\cdot p$ then $\nu_{\gamma_i\cdot p}(f) = \nu_{\gamma_j\cdot p}(f)$. Therefore, from (†) we get:

$$\frac{dk}{12} \geqslant n_\infty(f)\nu_\infty(f)$$

where $n_\infty(f) = \sharp\{j : \gamma_j\cdot\infty \text{ is in the } \Gamma\text{-orbit of } \infty\}$. Hence if $\nu_\infty(f) > \frac{dk}{12 n_\infty(f)}$ then $f$ is identically zero.

**Lemma 3.1.22.** $n_\infty(f) = [\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) : \mathrm{Stab}_\Gamma(\infty)]$.

*Proof.* Suppose that $\gamma_j\cdot\infty \in \Gamma\cdot\infty$. Then there exists $\gamma\in\Gamma$ such that

$$\gamma_j\cdot\infty = \gamma\cdot\infty.$$

Hence $\gamma_j^{-1}\gamma \in \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)$, and $\gamma_j^{-1} \in \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)\Gamma$. Therefore

$$\gamma_j^{-1}\Gamma \subseteq \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)\Gamma.$$

Hence

$$\begin{aligned} n_\infty(f) = \sharp\,\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)\Gamma/\Gamma &= \sharp\,\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)/(\Gamma\cap\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)) \\ &= \sharp\,\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)/\mathrm{Stab}_\Gamma(\infty) \\ &= [\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) : \mathrm{Stab}_\Gamma(\infty)]. \end{aligned}$$

□

For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we have $\gamma \cdot \infty = a/c$, so the stabiliser of $\infty$ is

$$\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) = \left\{ \begin{pmatrix} \pm 1 & n \\ 0 & \pm 1 \end{pmatrix} : n \in \mathbb{Z} \right\} = \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\mathbb{Z}}.$$

Hence Lemma 3.1.22 implies that $\left(\begin{smallmatrix} 1 & n_\infty(f) \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$ and $f$ has a $q$-expansion in $q^{1/n_\infty(f)}$. As the terms in the $q$-expansion of $f$ are powers of $q^{\frac{1}{n_\infty(f)}}$, $f$ has at most $1 + \frac{dk}{12}$ terms of degree less than or equal to $\frac{dk}{12 n_\infty(f)}$. We have already shown that if $\nu_\infty(f) > \frac{dk}{12 n_\infty(f)}$ then $f$ is identically zero, hence $f$ is determined by its first $1 + \frac{dk}{12}$-terms and we find:

**Theorem 3.1.23.** For $k < 0$, the space $M_k(\Gamma) = 0$ whereas $M_0(\Gamma) = \mathbb{C}$. For $k > 0$, put $d = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$, then we have

$$\dim(M_k(\Gamma)) \leqslant 1 + \left\lfloor \frac{dk}{12} \right\rfloor.$$

## 3.2 Hecke operators in higher level

We now introduce Hecke operators on the vector spaces $M_k(\Gamma)$. Again, our philosophy is that the eigenvectors for these operators are the modular forms with arithmetic content. We focus our attention on the congruence subgroups $\Gamma_0(N)$ and $\Gamma_1(N)$. This is not as strong an assumption as it appears, any congruence subgroup $\Gamma$ contains $\Gamma(N)$ for some $N$ by definition, and conjugating by $\left(\begin{smallmatrix} 0 & 1 \\ N & 0 \end{smallmatrix}\right)$ shows that a conjugate of $\Gamma$ contains $\Gamma_1(N^2)$.

### 3.2.1 Double coset operators and Hecke operators

Let $\Gamma, \Gamma'$ be congruence subgroups and $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, write

$$\Gamma \alpha \Gamma' = \bigsqcup_{i=1}^{r} \Gamma \alpha_i,$$

as a union of right cosets, and define

$$f \mid_{k, \Gamma\alpha\Gamma'} = \sum_{k=1}^{r} f \mid_{k, \alpha_i}.$$

**Lemma 3.2.1.** If $f \in M_k(\Gamma)$ then $f \mid_{k,\Gamma\alpha\Gamma'} \in M_k(\Gamma')$ and is independent of the choice of coset representatives $\alpha_i$. Moreover, if $f \in S_k(\Gamma)$ then $f \mid_{k,\Gamma\alpha\Gamma'} \in S_k(\Gamma')$.

*Proof.* Exercise, similar to the proof of Lemmas 3.1.11 and 3.1.21. □

Notice that, if $\Gamma' = \alpha^{-1}\Gamma\alpha$, then $\Gamma\alpha\Gamma' = \Gamma\alpha$ and $f \mid_{k,\Gamma\alpha\Gamma'} = f \mid_{k,\alpha}$.

**Definition 3.2.2.** Let $p$ be prime, $N \in \mathbb{Z}^+$, and set $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$. The *Hecke operator $T_p : M_k(\Gamma) \to M_k(\Gamma)$* is defined by

$$T_p f = f \mid_{k, \Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma}.$$

We claim this agrees with our definition for $\mathrm{SL}_2(\mathbb{Z})$. Recall, for $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ we had

$$\begin{aligned} T_p f(z) &= p^{k-1} \sum_{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_p} d^{-k} f\left(\frac{az+b}{d}\right) \\ &= \sum_{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_p} f\mid_{k,\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)} (z) \end{aligned}$$

where

$$S_p = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = p,\ a \geqslant 1,\ 0 \leqslant b < d \right\}.$$

To show that Definition 3.2.2 extends this definition it suffices to show that:

**Lemma 3.2.3.** We have an equality

$$\mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_p} \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

*Proof.* First we show that $\mathrm{SL}_2(\mathbb{Z})\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \subseteq \mathrm{SL}_2(\mathbb{Z}) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \mathrm{SL}_2(\mathbb{Z})$, i.e. we show that for all elements of $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_p$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \mathrm{SL}_2(\mathbb{Z}).$$

As $p$ is prime, the elements of $S_p$ are the matrix $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and the $p$ matrices $\left(\begin{smallmatrix} 1 & b \\ 0 & p \end{smallmatrix}\right)$ for $0 \leqslant b < p$. Now,

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

is in $\mathrm{SL}_2(\mathbb{Z}) \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \mathrm{SL}_2(\mathbb{Z})$. In the other cases, we have

$$\begin{aligned} \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \end{aligned}$$

and $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

Now we show that the cosets $\mathrm{SL}_2(\mathbb{Z}) \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ are disjoint. Suppose that

$$\mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix},$$

for $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right), \left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right) \in S_p$. Then

$$\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \begin{pmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

hence $a' = a$ and $d' = d$. If $a = a' = p$ then $d = d' = 1$ and $b = b' = 0$. If $a = a' = 1$ and $d = d' = p$ then multiplying the matrices out we find $p^{-1}(b' - b) \in \mathbb{Z}$ hence $p \mid (b' - b)$ which implies $b = b'$ (as $0 \leqslant b, b' < p$). Hence the union is disjoint and there are $(p+1)$ cosets. Hence it remains to show

$$\left| \mathrm{SL}_2(\mathbb{Z}) \backslash \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \mathrm{SL}_2(\mathbb{Z}) \right| = p + 1.$$

Conjugating $\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)$ by $S \in \mathrm{SL}_2(\mathbb{Z})$, by Lemma B.2.1 this is equal to the index of $\Gamma_0(p) = \mathrm{SL}_2(\mathbb{Z}) \cap \begin{pmatrix} p^{-1} & 0 \\ 0 & 1 \end{pmatrix} \mathrm{SL}_2(\mathbb{Z}) \left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$. However, from Exercise 3.1.6 we have

$$\Gamma(p)\backslash \mathrm{SL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/p),$$

which has order $p(p-1)(p+1)$ and

$$\Gamma(p)\backslash\Gamma_0(p) = \mathrm{SL}_2(\mathbb{Z}/p) \cap \begin{pmatrix} * & * \\ 0 & * \end{pmatrix},$$

which has order $p(p-1)$. Therefore

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(p)] = p(p-1)(p+1)/p(p-1) = p+1,$$

which completes the proof. □

### 3.2.2 Diamond operators

We have a homomorphism

$$\begin{aligned} \Gamma_0(N) &\to (\mathbb{Z}/N\mathbb{Z})^\times, \\ \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} &\mapsto d \pmod N \end{aligned}$$

whose kernel is $\Gamma_1(N)$, hence $\Gamma_1(N)$ is normal in $\Gamma_0(N)$.

Hence, for $\alpha \in \Gamma_0(N)$ and $f \in M_k(\Gamma_1(N))$ we have

$$f\,|_{k,\Gamma_1(N)\alpha\Gamma_1(N)} = f\,|_{k,\alpha},$$

which is an element of $M_k(\alpha^{-1}\Gamma_1(N)\alpha) = M_k(\Gamma_1(N))$.

For $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, let $\alpha = \begin{pmatrix} a & b \\ Nc & \widetilde{d} \end{pmatrix} \in \Gamma_0(N)$ with $\widetilde{d} \equiv d \pmod N$, and define

$$\begin{aligned} \langle d \rangle : M_k(\Gamma_1(N)) &\to M_k(\Gamma_1(N)) \\ f &\mapsto f\,|_{k,\alpha}, \end{aligned}$$

which is independent of the choice of $\alpha$ by Lemma 3.2.1. This defines a homomorphism

$$\begin{aligned} (\mathbb{Z}/N\mathbb{Z})^\times &\to \mathrm{GL}(M_k(\Gamma)) \\ d &\mapsto \langle d \rangle. \end{aligned}$$

**Theorem 3.2.4.** Let $V$ be a complex vector space with a homomorphism $\rho : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathrm{GL}(V)$. Then we have a direct sum decomposition of $V$

$$V = \bigoplus_{\substack{\chi:(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times \\ \text{homomorphism}}} V_\chi,$$

where $V_\chi = \{v \in V : \rho(g)v = \chi(g)v \text{ for all } g \in (\mathbb{Z}/N\mathbb{Z})^\times\}$ is the $\chi$-eigenspace.

For a homomorphism $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, we define

$$M_k(\Gamma_1(N), \chi) = M_k(\Gamma_1(N))_\chi = \{f \in M_k(\Gamma_1(N)) : \langle d \rangle f = \chi(d) f \text{ for all } d \in (\mathbb{Z}/N\mathbb{Z})^\times\}.$$

Hence we have

$$M_k(\Gamma_1(N)) = \bigoplus_{\substack{\chi:(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times \\ \text{homomorphism}}} M_k(\Gamma_1(N), \chi).$$

Notice that $M_k(\Gamma_1(N), \mathbf{1}) = M_k(\Gamma_0(N))$ where $\mathbf{1} : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is the trivial character, realising the embedding $M_k(\Gamma_0(N)) \hookrightarrow M_k(\Gamma_1(N))$.

### 3.2.3 Hecke operators commute

We now show that the Hecke operators and diamond operators commute.

**Lemma 3.2.5.** Let $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ and $p$ prime, then $\langle d\rangle T_p = T_p\langle d\rangle$.

*Proof.* Write

$$\Gamma_1(p)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(p) = \bigsqcup_{i=1}^{r}\Gamma_1(p)\alpha_i,$$

as a union of right cosets. Now (see for example [2]):

$$\Gamma_1(p)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(p) = \left\{A \in M_2(\mathbb{Z}) : A \equiv \begin{pmatrix}1 & *\\ 0 & p\end{pmatrix} \pmod N, \det(A) = p\right\}.$$

For any $\gamma \in \Gamma_0(p)$, we have

$$\gamma\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\gamma^{-1} \equiv \begin{pmatrix}1 & *\\ 0 & p\end{pmatrix} \pmod N,$$

and

$$\begin{aligned}\Gamma_1(p)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(p) &= \Gamma_1(p)\gamma\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\gamma^{-1}\Gamma_1(p)\\ &= \gamma\Gamma_1(p)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(p)\gamma^{-1}\\ &= \bigsqcup_{i=1}^{r}\Gamma_1(p)\gamma\alpha_i\gamma^{-1}.\end{aligned}$$

Hence

$$\bigsqcup_{i=1}^{r}\Gamma_1(p)\gamma\alpha_i = \bigsqcup_{i=1}^{r}\Gamma_1(p)\alpha_i\gamma.$$

By definition

$$\langle d\rangle T_p f = \sum_{k=1}^{r} f\mid_{k,\alpha_i\alpha},$$

whereas

$$T_p\langle d\rangle f = \sum_{k=1}^{r} f\mid_{k,\alpha\alpha_i},$$

and these coincide as they represent the same $\Gamma_1(p)$-cosets and the sum is independent of the choice of representatives. □

**Corollary 3.2.6.** The Hecke operator $T_p$ preserves $M_k(\Gamma_1(N),\chi)$ for all $\chi$.

*Proof.* Suppose $f \in M_k(\Gamma_1(N),\chi)$, then $\langle d\rangle T_p f = T_p\langle d\rangle f = T_p\chi(d) f = \chi(d) T_p f$. □

Let $f \in M_k(\Gamma_1(N),\chi)$, then since $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \in \Gamma_1(N)$, $f$ has a $q$-expansion $f(z) = \sum_{n=0}^{\infty} a(n)q^n$.

**Theorem 3.2.7.** Let $p$ be prime. Suppose $f \in M_k(\Gamma_1(N), \chi)$. The modular form $T_p f \in M_k(\Gamma_1(N), \chi)$, and $T_p f(z) = \sum_{n=0}^{\infty} \gamma(n) q^n$ with

$$\gamma(n) = \begin{cases} a(np) & \text{if } p \nmid n \\ a(np) + \chi(p) p^{k-1} a(n/p) & \text{if } p \mid n, \end{cases}$$

where we interpret $\chi(p) = 0$ if $p \mid N$.

*Proof.* To compute an explicit formula for $T_p F = f \mid_{k, \Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma}$ we need an explicit decomposition of $\Gamma_1(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma_1(N)$ as $\Gamma_1(N)$-cosets. We take this from [2]:

$$\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N) = \begin{cases} \bigsqcup_{j=0}^{p-1} \Gamma_1(N) \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right) & \text{if } p \mid N; \\ \bigsqcup_{j=0}^{p-1} \Gamma_1(N) \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right) \sqcup \left(\begin{smallmatrix} r & s \\ N & p \end{smallmatrix}\right) \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) & \text{if } p \nmid N. \end{cases}$$

where in the second case, $r, s$ are such that $rp - sN = 1$. Then for $p \mid N$ we have

$$\begin{aligned} T_p f(z) &= \sum_{j=0}^{p-1} f \mid_{k, \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)} (z) \\ &= \sum_{j=0}^{p-1} p^{k-1} p^{-k} f\left(\frac{z+j}{p}\right) \\ &= \frac{1}{p} \sum_{j=0}^{p-1} \sum_{n=0}^{\infty} a(n) e^{\frac{2\pi i(z+j)}{n}} p, \end{aligned}$$

by the $q$-expansion of $f\left(\frac{z+j}{p}\right)$. Now

$$\sum_{j=0}^{p-1} (e^{\frac{2\pi i n}{p}})^j = \begin{cases} p & \text{if } p \mid n \\ 0 & \text{otherwise,} \end{cases}$$

hence interchanging the order of summation we get

$$T_p f(z) = \sum_{p \mid n} a(n) e^{\frac{2\pi i z n}{p}} = \sum_{n=0}^{\infty} a(np) q^n.$$

This completes the proof in the case $p \mid N$.

If $p \nmid N$, we have an extra term coming from

$$f \mid_{k, \left(\begin{smallmatrix} r & s \\ N & p \end{smallmatrix}\right) \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)} (z) = (\langle p \rangle f) \mid_{k, \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)} (z),$$

as $\left(\begin{smallmatrix} r & s \\ N & p \end{smallmatrix}\right) \in \Gamma_0(N)$ with $(2,2)$-entry $p$ so $f \mid_{k, \left(\begin{smallmatrix} r & s \\ N & p \end{smallmatrix}\right)} = \langle p \rangle f$ and

$$f \mid_{k, \left(\begin{smallmatrix} r & s \\ N & p \end{smallmatrix}\right) \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)} = f \mid_{k, \left(\begin{smallmatrix} r & s \\ N & p \end{smallmatrix}\right)} \mid_{k, \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)}.$$

Now

$$(\langle p \rangle f) \mid_{k, \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)} (z) = p^{k-1} \chi(p) f(pz).$$

as $f \in M_k(\Gamma_1(N), \chi)$. Expanding $f(pz)$ as a $q$-expansion gives the extra term when $p \mid n$ and completes the proof. $\square$

**Corollary 3.2.8.** For $p, q$ prime, $T_p$ and $T_q$ commute.

*Proof.* We apply Theorem 3.2.7 twice to $T_q T_p f = \sum_{n=0}^{\infty} \delta(n) q^n$, to find

$$\delta(n) = a(npq) + \chi(q)a(np/q)q^{k-1} + \chi(p)a(nq/p)p^{k-1} + \chi(pq)(pq)^{k-1}a(n/pq),$$

which is symmetric in $p, q$, and hence equal to the coefficient in $T_q T_p$. □

**Definition 3.2.9.** For $p$ prime and $r$ a positive integer we inductively define the *Hecke operator* $T_{p^{r+1}}$ by

$$T_{p^{r+1}} = T_p T_{p^r} - p^{k-1}\langle p\rangle T_{p^{r-1}}$$

For $n, m$ coprime integers, we define the *Hecke operator* $T_{nm}$ by

$$T_{nm} = T_n T_m.$$

**Corollary 3.2.10.** The Hecke operators $T_m$ and $T_n$ commute for all $m, n$, and commute with the diamond operators.

*Proof.* This follows from their definitions and Corollary 3.2.8 and Lemma 3.2.5. □

## 3.3 Bases of eigenforms

We have defined Hecke operators $T_n$ and diamond operators $\langle d\rangle$ on $M_k(\Gamma_1(N))$ and showed that they all commute. Now we going to look at eigenforms for the Hecke operators, and in the process tie up a loose end from our work on modular forms for $\mathrm{SL}_2(\mathbb{Z})$: showing that $M_k = M_k(\mathrm{SL}_2(\mathbb{Z}))$ has a basis of eigenforms.

**Remark 3.3.1.** We note that we use $T_p$ for the Hecke operator $f \mid_{k,\Gamma\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma}$ for all primes $p$; some authors use $U_p$ for primes $p \mid N$ and $T_p$ for primes $p \nmid N$ to emphasize that they have very different properties.

In this section, we show that $S_k(\Gamma_1(N))$ has a basis of eigenforms for the Hecke operators $T_p$ with $p \nmid N$. We do this by first introducing an inner product on $S_k(\Gamma_1(N))$, computing the adjoints of the Hecke operators with respect to this inner product, and using Spectral Theory (Appendix C).

### 3.3.1 The Petersson inner product

Define the *hyperbolic measure* on the upper half plane to be

$$d\mu(z) = \frac{dxdy}{y^2}, \quad z = x + iy.$$

For a congruence subgroup $\Gamma \leqslant \mathrm{SL}_2(\mathbb{Z})$, write $\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i=1}^{d}(\pm\Gamma)\gamma_i$ and recall we defined

$$\mathcal{D}_\Gamma = \bigcup_{i=1}^{d} \gamma_i \cdot \mathcal{D},$$

a fundamental domain for $\Gamma$. We define for modular forms $f, f' \in M_k(\Gamma)$

$$\langle f, f'\rangle_\Gamma = \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma]} \int_{\mathcal{D}_\Gamma} f(z)\overline{f'(z)} y^k \frac{dxdy}{y^2}.$$

**Theorem 3.3.2.** (i) The integral $\langle f, f'\rangle_\Gamma$ is independent of the choice of $\mathcal{D}_\Gamma$, i.e. independent of the choice of $\gamma_i$.

(ii) The integral $\langle f, f'\rangle_\Gamma$ converges provided at least one of $f, f'$ is a cusp form.

(iii) If $\Gamma' \leqslant \Gamma$ is another congruence subgroup

$$\langle f, f'\rangle_{\Gamma'} = \langle f, f'\rangle_\Gamma.$$

*Proof.* We first show (iii). Let $\Gamma = \bigsqcup_{i=1}^{d'} (\pm\Gamma')\alpha_i$ be a decomposition into $\pm\Gamma$-cosets. Then $\alpha_i \mathcal{D}_\Gamma$ is a fundamental domain for $\Gamma$ and $\bigcup_{i=1}^{d'} \alpha_i \mathcal{D}_\Gamma$ is a fundamental domain for $\Gamma'$, then using (i) we have

$$\begin{aligned}
\langle f, f'\rangle_{\Gamma'} &= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma']} \int_{\mathcal{D}_{\Gamma'}} f(z)\overline{f'(z)} y^k \frac{dxdy}{y^2} \\
&= \sum_{i=1}^{d'} \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma']} \int_{\alpha_i \mathcal{D}_\Gamma} f(z)\overline{f'(z)} y^k \frac{dxdy}{y^2} \\
&= \frac{[\pm\Gamma : \pm\Gamma']}{[\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma']} \int_{\mathcal{D}_\Gamma} f(z)\overline{f'(z)} y^k \frac{dxdy}{y^2} \\
&= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma]} \int_{\mathcal{D}_\Gamma} f(z)\overline{f'(z)} y^k \frac{dxdy}{y^2} \\
&= \langle f, f'\rangle_\Gamma.
\end{aligned}$$

This completes the proof of (iii).

**Claim 1:** Let $\gamma \in \mathrm{GL}_2(\mathbb{R})^+$ and $\mathcal{D}$ denote a sufficiently nice subset in $\mathbb{H}$ (for example, a fundamental domain of $\Gamma$), then

$$\int_{\mathcal{D}} f(z) \frac{dxdy}{y^2} = \int_{\gamma^{-1}\mathcal{D}} f(\gamma \cdot z) \frac{dxdy}{y^2}.$$

In other words, the measure $d\mu(z)$ is invariant under the action of $\mathrm{GL}_2(\mathbb{R})^+$.

*Proof of Claim 1.* In two variables $(x, y) \mapsto \gamma(x, y)$, we have the following substitution formula

$$\int_{\mathcal{D}} f(x, y) dxdy = \int_{\gamma^{-1}\mathcal{D}} f(\gamma(x, y)) |\det(J_\gamma(x, y))| dxdy, \tag{$\dagger$}$$

where $J_\gamma(x, y)$ is the *Jacobian* of $\gamma$. Writing $\gamma(x, y) = (\gamma_1(x, y), \gamma_2(x, y))$, by definition $J_\gamma(x, y)$ is the matrix of partial derivatives

$$J_\gamma(x, y) = \begin{pmatrix} \frac{\partial \gamma_1}{\partial x} & \frac{\partial \gamma_2}{\partial x} \\ \frac{\partial \gamma_1}{\partial y} & \frac{\partial \gamma_2}{\partial y} \end{pmatrix}.$$

This has determinant

$$\det(J_\gamma(x, y)) = \frac{\partial \gamma_1}{\partial x}\frac{\partial \gamma_2}{\partial y} - \frac{\partial \gamma_2}{\partial x}\frac{\partial \gamma_1}{\partial y} = \left(\frac{\partial \gamma_1}{\partial x}\right)^2 + \left(\frac{\partial \gamma_2}{\partial y}\right)^2,$$

the last equality by the Cauchy–Riemann equations, which are satisfied since $\gamma : z \to \frac{az+b}{cz+d}$ is holomorphic on $\mathbb{H}$ for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})^+$. Moreover, taking the limit along the real part of $z$, we have $\gamma'(z) = \frac{\partial \gamma_1}{\partial x} + i\frac{\partial \gamma_2}{\partial x}$; hence

$$\det(J_\gamma(x,y)) = \left(\frac{\partial \gamma_1}{\partial x}\right)^2 + \left(\frac{\partial \gamma_2}{\partial y}\right)^2 = |\gamma'(z)|^2 = \frac{1}{|cz+d|^4},$$

the final equality as $\gamma'(z) = \frac{d}{dz}\left(\frac{az+b}{cz+d}\right) = \frac{1}{(cz+d)^2}$ by the product rule. By Lemma 2.1.1, we also have

$$\mathrm{Im}(\gamma \cdot z)^2 = y^2/|cz+d|^4.$$

Substituting these into (†) proves the claim. □

Now notice that the expression

$$f(\gamma \cdot z)\overline{f'(\gamma \cdot z)}\mathrm{Im}(\gamma \cdot z)^k = (cz+d)^k f(z)\overline{(cz+d)^k}\,\overline{f'(z)}\mathrm{Im}(z)^k|cz+d|^{2k} = f(z)\overline{f'(z)}\mathrm{Im}(z)^k$$

is $\Gamma$-invariant. Putting this together with Claim 1, for $\gamma \in \Gamma$, we get:

$$\int_{\mathcal{D}} f(z)\overline{f'(z)}y^k\frac{dxdy}{y^2} = \int_{\gamma^{-1}\mathcal{D}} f(z)\overline{f'(z)}y^k\frac{dxdy}{y^2},$$

which implies that $\langle f, f'\rangle_\Gamma$ does not depend on the choice of $\mathcal{D}_\Gamma$, and we have proved (i).

It remains to show (ii). Let $F(z) = f(z)\overline{f'(z)}y^k$, this is a continuous function on $\mathbb{H}$. If we can show $F$ is bounded on $\mathcal{D}_\Gamma$ (and hence on $\mathbb{H}$), and the hyperbolic volume $\frac{dxdy}{y^2}(\mathcal{D}_\Gamma)$ is finite, then the integral converges. We let $C_N$ denote the compact subregion of $\mathcal{D}$ of all points with imaginary part less than or equal to $N$, and $B_\infty$ the "neighbourhood of $\infty$" of all points with imaginary part greater than $N$. We have

$$\mathcal{D}_\Gamma = \bigcup_{i=1}^{d} \gamma_i C_N \cup \bigcup_{i=1}^{d} \gamma_i B_\infty.$$

The region $C = \bigcup_{i=1}^{d} \gamma_i C_N$ is compact, and $F$ is bounded on $C$ as it is continuous and $C$ is compact, moreover the volume of $C$ is finite as $C$ is compact, so the integral converges on $C$. It remains to consider the neighbourhoods $\bigcup \gamma_i B_\infty$ of the cusps. The volume of $B_\infty$ is

$$\frac{dxdy}{y^2}(B_\infty) = \int_{B_\infty}\frac{dxdy}{y^2} \leqslant \int_{-1/2}^{1/2}\left(\int_{\sqrt{3}/2}^{\infty}\frac{1}{y^2}dy\right)dx = \frac{2}{\sqrt{3}}.$$

This implies that all $\gamma_i B_\infty$ have finite volume (and hence so does their union), as $\frac{dxdy}{y^2}$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant. So it remains to show $F$ is bounded on each neighbourhood $B_c$ of each cusp $c$. By definition, $c$ is a $\Gamma$-orbit in $\mathbb{Q} \cup \{\infty\}$, and we write $x = \gamma \cdot \infty$ for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$(cz+d)^{-k}f(\gamma \cdot z) = f\mid_{k,\gamma}(z) = \sum_{n=0}^{\infty} a_c(n)q_c^n.$$

as $f$ is holomorphic at $c$. We have a similar expansion for $f'(\gamma \cdot z)$. And writing

$$F(\gamma \cdot z) = f(\gamma \cdot z)\overline{f'(\gamma \cdot z)}y^k,$$

if one of $f, f'$ vanishes at $c$ then, from the $q$-expansion we see that, this decays exponentially as $y \to \infty$ which implies $F$ is bounded on our neighbourhood of $c$. While we only use that one of each $f, f'$ vanishes at every cusp, this is certainly implied by one of $f, f'$ being a cusp form and vanishing at all cusps. □

In particular, part (ii) of Theorem 3.3.2 shows that $\langle\ ,\ \rangle_\Gamma$ converges on $M_k(\Gamma)\times S_k(\Gamma)$. By restricting both modular forms to be cusp forms we get a map

$$\langle\ ,\ \rangle_\Gamma : S_k(\Gamma)\times S_k(\Gamma)\to\mathbb{C},$$

and we easily see that $\langle\ ,\ \rangle_\Gamma$ is a Hermitian inner product on $S_k(\Gamma)$ called the *Petersson inner product*.

**Remark 3.3.3.** One can define the space of Eisenstein series to be the "orthogonal complement" of the space of cusp forms (the speech marks as $\langle\ ,\ \rangle_\Gamma$ is not an inner product on $M_k(\Gamma)$). Namely,

$$E_k(\Gamma)=\{f\in M_k(\Gamma):\langle f,f'\rangle_\Gamma=0 \text{ for all } f'\in S_k(\Gamma)\}.$$

Our next goal is to show that the Hecke operators $T_p$ for $p\nmid N$ and the diamond operators $\langle d\rangle$ are normal for the Petersson inner product, and then by Spectral Theory there exists a basis of $S_k(\Gamma)$ consisting of eigenforms for $\{T_p,\langle d\rangle : p\nmid N\}$.

### 3.3.2 Adjoints of Hecke operators and eigenforms

**Lemma 3.3.4.** Let $\alpha\in\mathrm{GL}_2(\mathbb{Q})^+$ and assume that $\alpha^{-1}\Gamma\alpha\subseteq\mathrm{SL}_2(\mathbb{Z})$, then

$$\langle f\,|_{k,\alpha},f'\rangle_{\alpha^{-1}\Gamma\alpha}=\langle f,f'\,|_{k,\det(\alpha)\alpha^{-1}}\rangle_\Gamma.$$

*Proof.* Put $c=[\mathrm{SL}_2(\mathbb{Z}):\pm\Gamma]^{-1}=[\mathrm{SL}_2(\mathbb{Z}):\pm\alpha^{-1}\Gamma\alpha]^{-1}$ and $\alpha=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$. Now $\alpha^{-1}\mathcal{D}_\Gamma$ is a fundamental domain for $\Gamma$, and by definition

$$\begin{aligned}\langle f\,|_{k,\alpha},f'\rangle_{\alpha^{-1}\Gamma\alpha}&=c\int_{\alpha^{-1}\mathcal{D}_\Gamma} f\,|_{k,\alpha}(z)\overline{f'(z)}y^k\frac{dxdy}{y^2}\\&=c\int_{\alpha^{-1}\mathcal{D}_\Gamma}\det(\alpha^{k-1})(cz+d)^{-k}f(\alpha\cdot z)\overline{f'(z)}y^k\frac{dxdy}{y^2}.\end{aligned}$$

We change variables $z'=\alpha\cdot z=\frac{az+b}{cz+d}$, and noting that the measure is invariant under $\mathrm{GL}_2(\mathbb{R})^+$, we have

$$\langle f\,|_{k,\alpha},f'\rangle_{\alpha^{-1}\Gamma\alpha}=c\int_{\mathcal{D}_\Gamma}\det(\alpha)^{k-1}(cz'+d)^{-k}f(z')\overline{f'(\alpha^{-1}\cdot z')}|cz+d|^{2k}y'^k\frac{dx'dy'}{y'^2}.$$

Now let $\alpha^{-1}=\left(\begin{smallmatrix}a'&b'\\c'&d'\end{smallmatrix}\right)$. As $f\,|_{k,\alpha^{-1}}|_{k,\alpha}=f$ we have $(cz+d)^k=(c'z'+d')^{-k}$, and so

$$\begin{aligned}\langle f\,|_{k,\alpha},f'\rangle_{\alpha^{-1}\Gamma\alpha}&=c\int_{\mathcal{D}_\Gamma}\det(\alpha)^{-1}(c'z'+d')^kf(z')\overline{f'(\alpha^{-1}\cdot z')}|c'z'+d'|^{-2k}y'^k\frac{dx'dy'}{y'^2}\\&=c\int_{\mathcal{D}_\Gamma}\det(\alpha)^{-1}f(z')\overline{(c'z'+d')}^{-k}\overline{f'(\alpha^{-1}\cdot z')}y'^k\frac{dx'dy'}{y'^2}.\end{aligned}$$

But, by definition of $f\,|_{k,\alpha^{-1}}$ this gives

$$\begin{aligned}\langle f\,|_{k,\alpha},f'\rangle_{\alpha^{-1}\Gamma\alpha}&=c\int_{\mathcal{D}_\Gamma}\det(\alpha)^{k-2}f(z')\overline{f'\,|_{k,\alpha^{-1}}(z')}y'^k\frac{dx'dy'}{y'^2}\\&=\det(\alpha)^{k-2}\langle f,f'\,|_{k,\alpha^{-1}}\rangle_\Gamma.\end{aligned}$$

Thus it remains to show $\det(\alpha)^{k-2}\langle f, f' |_{k,\alpha^{-1}}\rangle_\Gamma = \langle f, f' |_{k,\det(\alpha)\alpha^{-1}}\rangle_\Gamma$. However, for $\lambda \in \mathbb{C}^\times$ we have

$$f |_{k,\lambda\alpha} (z) = \det(\lambda\alpha)^{k-1}(\lambda\alpha cz + \lambda d)^{-k} f(\alpha \cdot z) = \lambda^{k-2} f |_{k,\alpha} (z).$$

Now $\langle\ ,\ \rangle_\Gamma$ is $\mathbb{R}$-linear in the second variable, and putting these facts together completes the proof. □

**Lemma 3.3.5.** For $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ there exist $\beta_1, \cdots, \beta_n \in \mathrm{GL}_2(\mathbb{Q})^+$ such that

$$\Gamma\alpha\Gamma = \bigsqcup_{i=1}^{n} \Gamma\beta_i = \bigsqcup_{i=1}^{n} \beta_i\Gamma.$$

*Proof.* Covered in lectures, see [2, 5.5.1.]. □

We now compute the adjoint of $|_{k,\Gamma\alpha\Gamma}$.

**Lemma 3.3.6.** Let $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ and $f, f' \in S_k(\Gamma)$. Then

$$\langle f |_{k,\Gamma\alpha\Gamma}, f'\rangle_\Gamma = \langle f, f' |_{k,\Gamma(\det(\alpha)\alpha^{-1})\Gamma}\rangle_\Gamma.$$

*Proof.* Choose $\beta_1, \ldots, \beta_n \in \mathrm{GL}_2(\mathbb{Q})^+$ such that

$$\Gamma\alpha\Gamma = \bigsqcup_{i=1}^{n} \Gamma\beta_i = \bigsqcup_{i=1}^{n} \beta_i\Gamma$$

as in Lemma 3.3.5. Then

$$\Gamma\alpha^{-1}\Gamma = \bigsqcup_{i=1}^{n} \Gamma\beta_i^{-1},$$

and hence

$$\Gamma(\det(\alpha)\alpha^{-1})\Gamma = \bigsqcup_{i=1}^{n} \Gamma(\det(\beta_i)\beta_i^{-1}).$$

By linearity of $\langle\ ,\ \rangle_\Gamma$ and Lemma 3.3.4, we then have

$$\begin{aligned}\langle f |_{k,\Gamma\alpha\Gamma}, f'\rangle_\Gamma &= \sum_{i=1}^{n} \langle f |_{k,\beta_i}, f'\rangle_{\beta_i^{-1}\Gamma\beta_i\cap\Gamma} \\ &= \sum_{i=1}^{n} \langle f, f' |_{k,\det(\beta_i)\beta_i^{-1}}\rangle_{\Gamma\cap\beta_i\Gamma\beta_i^{-1}} \\ &= \langle f, f' |_{k,\Gamma(\det(\alpha)\alpha^{-1})\Gamma}\rangle_\Gamma.\end{aligned}$$

□

**Proposition 3.3.7.** We have

$$T_p^* = \langle p\rangle^{-1} T_p \quad \text{and} \quad \langle p\rangle^* = \langle p\rangle^{-1}.$$

*Proof.* By definition

$$\langle p\rangle f = f |_{k,\gamma},$$

for any $\gamma \in \Gamma_0(N)$ such that

$$\gamma \equiv \begin{pmatrix} * & * \\ 0 & p \end{pmatrix} \pmod{N}.$$

Hence $f\mid_{k,\gamma^{-1}} = \langle d^{-1}\rangle f$, and by Lemma 3.3.4

$$\langle d\rangle^* = \langle d^{-1}\rangle.$$

By definition

$$T_p f = f\mid_{k,\Gamma_1(N)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma_1(N)}.$$

Hence, by Lemma 3.3.6,

$$T_p^* = f\mid_{k,\Gamma_1(N)\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)\Gamma_1(N)}.$$

There exist $r, s$ such that $sp - rN = 1$, and we have an equality

$$\begin{pmatrix}p&0\\0&1\end{pmatrix} = \begin{pmatrix}1&N\\r&sp\end{pmatrix}^{-1}\begin{pmatrix}1&0\\0&p\end{pmatrix}\begin{pmatrix}p&r\\N&s\end{pmatrix}$$

with $\left(\begin{smallmatrix}1&N\\r&sp\end{smallmatrix}\right)^{-1} \in \Gamma_1(N)$ and $\left(\begin{smallmatrix}p&r\\N&s\end{smallmatrix}\right) \in \Gamma_0(N)$. Hence we have an equality of sets (as $\Gamma_1(N)$ is normal in $\Gamma_0(N)$):

$$\Gamma_1(N)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma_1(N) = \Gamma_1(N)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma_1(N)\begin{pmatrix}p&r\\N&s\end{pmatrix}.$$

Hence if we choose coset representatives

$$\Gamma_1(N)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma_1(N) = \bigsqcup_{i=1}^{d}\Gamma_1(N)\beta_i,$$

then

$$\Gamma_1(N)\begin{pmatrix}p&0\\0&1\end{pmatrix}\Gamma_1(N) = \bigsqcup_{i=1}^{d}\Gamma_1(N)\beta_i\begin{pmatrix}p&r\\N&s\end{pmatrix}.$$

Therefore, by Lemma 3.3.6,

$$\begin{aligned}T_p^* &= f\mid_{k,\Gamma_1(N)\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)\Gamma_1(N)}\\ &= \left(f\mid_{k,\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)}\right)\mid_{k,\left(\begin{smallmatrix}p&r\\N&s\end{smallmatrix}\right)}\\ &= \langle p\rangle^{-1}T_p.\end{aligned}$$

□

By Proposition 3.3.7 and their definitions, it follows that $\langle m\rangle$ and $T_n$ for $m, n \in \mathbb{Z}^+$ with $(n, N) = 1$ are normal operators. Thus by The Spectral Theorem (Appendix C), we get:

**Theorem 3.3.8.** There space $S_k(\Gamma_1(N))$ has a basis consisting of eigenforms for $\{T_n, \langle m\rangle : (n, N) = 1\}$.

In the special case $N = 1$, together with Proposition 2.3.14 this gives:

**Corollary 3.3.9.** The space $M_k = M_k(\mathrm{SL}_2(\mathbb{Z}))$ has a basis of eigenforms.

## 3.4 Oldforms and newforms

We have bases of $S_k(\Gamma_1(N))$ consisting of eigenforms for $\{T_n, \langle m\rangle : (n, N) = 1\}$, we now consider the Hecke operators $T_p$ for $p \mid N$. We define maps taking forms of lower level $M \mid N$ to level $N$ whose image defines the space of *oldforms*. It will turn out that the space of *newforms*, the orthogonal complement in $S_k(\Gamma_1(N))$ of the space of oldforms with respect to the Petersson inner product, does have a basis of eigenforms for all the Hecke and diamond operators; these eigenforms are called *newforms*. Due to a lack of time, we will need to state two important results without proof.

Let $p \mid N$ be prime, then we have seen that we have an inclusion

$$S_k(\Gamma_1(p^{-1}N)) \subseteq S_k(\Gamma_1(N)).$$

There is another map between these spaces, as $\Gamma_1(N) \subseteq \begin{pmatrix} p^{-1} & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(p^{-1}N) \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we have

$$\begin{aligned} S_k(\Gamma_1(p^{-1}N)) &\to S_k(\Gamma_1(N)) \\ f &\mapsto f \mid_{k,\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)} = p^{k-1} f(pz). \end{aligned}$$

Write

$$\begin{aligned} i_p : S_k(\Gamma_1(p^{-1}N))^2 &\to S_k(\Gamma_1(N)) \\ (f, f') &\mapsto f + f' \mid_{k,\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)}. \end{aligned}$$

**Definition 3.4.1.** Define the *space of oldforms of weight $k$ and level $N$* by

$$S_k(\Gamma_1(N))^{\text{old}} = \sum_{\substack{p \mid N \\ \text{prime}}} i_p(S_k(\Gamma_1(p^{-1}N))^2).$$

Define the space of *newforms of weight $k$ and level $N$* to be the orthogonal complement of the space of oldforms of weight $k$ and level $N$ with respect to the Petersson inner product:

$$S_k(\Gamma_1(N))^{\text{new}} = \{f \in S_k(\Gamma_1(N)) : \langle f, f'\rangle_{\Gamma_1(N)} = 0 \text{ for all } f' \in S_k(\Gamma_1(N))^{\text{old}}\}.$$

The spaces of oldforms and newforms are stable under Hecke and diamond operators:

**Proposition 3.4.2.** The subspaces $S_k(\Gamma_1(N))^{\text{old}}$ and $S_k(\Gamma_1(N))^{\text{new}}$ are stable under $\{T_n, \langle n\rangle : n \in \mathbb{Z}^+\}$.

*Proof.* We do not provide a proof, the interested reader may see [2, 5.6.2]. □

**Corollary 3.4.3.** The subspaces $S_k(\Gamma_1(N))^{\text{old}}$ and $S_k(\Gamma_1(N))^{\text{new}}$ have bases of eigenforms for the operators $\{T_n, \langle m\rangle : (n, N) = 1\}$.

**Definition 3.4.4.** A non-zero modular form in $M_k(\Gamma_1(N))$ is called an *eigenform* if it is an eigenform for all $T_n, \langle n\rangle$ with $n \in \mathbb{Z}^+$. It is called *normalized* if the coefficient $c(1)$ of $q$ in its $q$-expansion is 1. A *newform* is a normalized eigenform in $S_k(\Gamma_1(N))^{new}$.

If $f \in S_k(\Gamma_1(N))$ is an eigenform for all diamond operators, then $\langle n\rangle f = d(n) f$ and as $\langle n\rangle\langle m\rangle = \langle nm\rangle$, the map $n \mapsto d(n)$ descends to a homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times,$$

and $f \in S_k(\Gamma_1(N), \chi)$. Hence the newforms in $S_k(\Gamma_1(N))^{\text{new}}$ lie in eigenspaces $S_k(\Gamma_1(N), \chi)^{\text{new}}$.

**Theorem 3.4.5** (Strong multiplicity one)**.** If $f \in S_k(\Gamma_1(N), \chi)^{\text{new}}$ and $f' \in S_k(\Gamma_1(N), \chi)$ be non-zero eigenforms for $\{T_n, \langle m \rangle : (n, N) = 1\}$ with the same $T_\ell$-eigenvalues for $\ell$ prime not dividing $N$. Then $f' = \lambda f$ for $\lambda \in \mathbb{C}^\times$.

*Proof.* We do not provide a proof of this important result, the interested reader may see [2, 5.8.2]. □

**Corollary 3.4.6.** Let $f \in S_k(\Gamma_1(N), \chi)^{\text{new}}$ be an eigenform for $\{T_n, \langle m \rangle : (n, N) = 1\}$ with $q$-expansion $f(z) = \sum_{n=0}^{\infty} c(n) q^n$. Then $c(1) \neq 0$.

*Proof.* In Theorem 3.2.7, we gave the $q$-expansion of $T_p f$. One can generalize this to get a formula for $T_n f$ as we did for Hecke operators on $M_k(\mathrm{SL}_2(\mathbb{Z}))$, and in particular putting $f(z) = \sum_{n=0}^{\infty} a(n) q^n$ and $T_n f(z) = \sum_{n=0}^{\infty} \gamma(n) q^n$ we would find

$$\gamma(1) = a(n).$$

Since, $f$ is an eigenform for $T_n$ with $(n, N) = 1$ we also have

$$\gamma(1) = \lambda_n a(1),$$

for $(n, N) = 1$ and with $\lambda_n \in \mathbb{C}^\times$. If $a(1) = 0$ then this implies that $a(n) = 0$ for all $(n, N) = 1$ which implies that $f$ is zero (hence not an eigenform, a contradiction). □

**Corollary 3.4.7.** Let $f \in S_k(\Gamma_1(N), \chi)^{\text{new}}$ be an eigenform for $\{T_n, \langle m \rangle : (n, N) = 1\}$, then it is an eigenform for $\{T_n, \langle n \rangle : n \in \mathbb{Z}^{\geqslant 0}\}$.

*Proof.* We have

$$T_\ell(T_p f) = T_p T_\ell f = T_p \lambda_\ell f = \lambda_\ell(T_p f),$$

so $T_p f$ and $f$ are both eigenvectors for all $T_\ell$ with the same eigenvalues. By strong multiplicity one $T_p f = \lambda_p f$, and $f$ is an eigenvector for $T_p$. □

**Corollary 3.4.8.** The set of newforms is a basis of the space $S_k(\Gamma_1(N))^{\text{new}}$.

Suppose $f \in S_k(\Gamma_1(N), \chi)^{\text{new}}$ is a newform with $q$-expansion $f(z) = \sum_{n=0}^{\infty} a(n) q^n$. We define its associated $L$-function by

$$L(s, f) = \sum_{n=1}^{\infty} a(n) q^n.$$

This $L$-function has nice analytic properties and a functional equation, analagous to the properties we had for $L$-functions of modular forms of level one in Section 2.4.2, together with an Euler product

$$L(s, f) = \prod_{p \nmid N} (1 - a(p) p^{-s} + \chi(p) p^{k-1-2s})^{-1} \prod_{p \mid N} (1 - a(p) p^{-s})^{-1}.$$

# Appendix A

# Complex Analysis

## A.1 Holomorphic and meromorphic functions

Let $\Omega \subseteq \mathbb{C}$ be a region in $\mathbb{C}$, for example the upper half plane $\mathbb{H}$, and $f : \Omega \to \mathbb{C}$ be a complex valued function.

**Definition A.1.1.** The function $f$ is called *differentiable* or *holomorphic* at $p \in \Omega$ if

$$\lim_{h \to 0} \frac{f(p+h) - f(p)}{h}$$

exists in $\mathbb{C}$. We say that $f$ is *holomorphic* on $\Omega$ if it is holomorphic at all points in $\Omega$.

The important point here is that $h \in \mathbb{C}$ can approach 0 from any direction and within this definition we are saying that all the limits are the same. That the limit with $h$ real and the limit with $h$ purely imaginary must agree leads to the *Cauchy–Riemann equations* a holomorphic function $f$ mush satisfy: write $z = x + iy$ and suppose that $f(z) = u(x, y) + iv(x, y)$ then

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \qquad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

**Amazing feature of complex analysis:** If $f$ is holomorphic on a region $\Omega$ in $\mathbb{C}$, then $f$ is infinitely differentiable on $\Omega$ (in contrast to real analysis!), and for $p \in \Omega$ we can expand $f$ as a power series valid in some neighbourhood of $p$.

**Theorem A.1.2** (Power series expansion)**.** Suppose $f$ is holomorphic in a region $\Omega$, and $p \in \Omega$. Then

$$f(z) = \sum_{i=0}^{\infty} a_i (z-p)^i,$$

for all $z$ in an open disc centred at $p$ within $\Omega$.

If $f$ is zero at $p$, but not identically zero, there is a unique smallest $n$ such that $a_n$ is non-zero and we say that $f$ has a zero of *order* $n$ at $p$.

We make use of the following two useful lemmas on holomorphic functions in the course:

**Lemma A.1.3.** Let $f_n$ be a sequence of holomorphic functions on a region $\Omega \subseteq \mathbb{C}$. If $\sum_{n=0}^{\infty} f_n(z)$ is uniformly convergent to $f(z)$ on all compact subsets of $\Omega$, then $f$ is holomorphic on $\Omega$.

**Lemma A.1.4.** A non-zero holomorphic function on a compact set has finitely many zeroes and is bounded.

Suppose $f$ is holomorphic for all $z$ in some disc centred at $p$, except for $p$ itself, then $p$ is called an *isolated singularity.* It is a *removable singularity* if we can redefine $f(p)$ so that $f$ is holomorphic in the whole disc. If $\lim_{z\to p} f(z) = \infty$, then $p$ is a *pole* of $f$. A function which is holomorphic in a region $\Omega$ in $\mathbb{C}$ except for poles is called *meromorphic* in $\Omega$.

For example, the function on the punctured unit disc $\mathbb{D}^*$ defined by:

(i) $f(z) = 1/z$ has a pole at 0.

(ii) $f(z) = e^{1/z}$ has an *essential singularity* at 0, the limit along the positive real line is $\infty$, the limit along the negative real line is 0, so the limit is not defined.

**Theorem A.1.5.** Let $f$ be a meromorphic function on a domain $\Omega$ with a pole at $p \in \Omega$, then in a neighbourhood of $p$, then there is a non-vanishing holomorphic function $g$ on a neighbourhood of $p$ and a unique $n \in \mathbb{Z}^+$ such that

$$f(z) = (z-p)^n g(z)$$

and we have an expansion:

$$f(z) = \frac{a_{-n}}{(z-p)^n} + \frac{a_{-n+1}}{(z-p)^{n-1}} + \cdots + \frac{a_{-1}}{z-p} + G(z)$$

with $G$ holomorphic in a neighbourhood of $p$.

The integer $n$ is called the *order* of the pole, and the coefficient $a_{-1}$ is called the *residue* of $f$ at $p$, $\mathrm{Res}_p(f) = a_{-1}$.

Let $f$ be a meromorphic function on $\Omega$.

**Theorem A.1.6** (Cauchy's residue theorem)**.** For $\gamma$ in $\Omega$ a simple closed curve (oriented counter clockwise) with $f$ holomorphic on $\gamma$, then

$$\int_\gamma f(z)dz = 2\pi i \sum_{\substack{\text{poles } p \\ \text{inside } \gamma}} \mathrm{Res}_p(f).$$

Let $\nu_p(f)$ denote the order of zero (or minus the order of pole) of $f(z)$ at $p$. Cauchy's residue theorem has the following corollary:

**Theorem A.1.7** (Cauchy's argument principle)**.**

$$\int_\gamma \frac{f'(z)}{f(z)}dz = 2\pi i \sum_{p \text{ inside } \gamma} \nu_p(f).$$

## A.2 A trigonometric identity

**Lemma A.2.1.**

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

# Appendix B

# Group Theory

## B.1 Structure of abelian groups

**Lemma B.1.1.** A finite abelian group $A$ of order $mn$ with $(m, n) = 1$ decomposes as $A = mA \times nA$ and $mA$ is the unique subgroup of order $n$, and $nA$ is the the unique subgroup of order $m$.

**Theorem B.1.2** (Fundamental Theorem of Finitely Generated Abelian Groups)**.** A finitely generated abelian group $A$ decomposes as a direct product

$$A = \mathbb{Z}^r \times \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{r_s}\mathbb{Z},$$

for (not necessarily distinct) prime numbers $p_1, \ldots, p_s$, and integers $r, r_1, \ldots, r_s \in \mathbb{Z}^{\geqslant 0}$.

## B.2 Double cosets

Let $H, K$ be subgroups of a group $G$ and $g \in G$. The *double coset*

$$HgK = \{hgk : h \in H, k \in K\},$$

is a union of left cosets $xK$ and also a union of right cosets $Hx$.

**Lemma B.2.1.** We have a bijection

$$(K \cap g^{-1}Hg)\backslash K \to H\backslash HgK,$$

induced by the map $K \to HgK$, $k \mapsto Hgk$.

*Proof.* The map is clearly surjective. Assume $Hgk \cap Hgk' \neq \emptyset$, then $gk \in Hgk'$ hence $k \in g^{-1}Hgk'$. As $k, k' \in K$ this implies $k \in (K \cap g^{-1}Hg)k'$ and hence $(K \cap g^{-1}Hg)k = (K \cap g^{-1}Hg)k'$. □

Similarly, we have a bijection $H/(H \cap gKg^{-1}) \to HgK/K$.

# Appendix C

# Spectral Theory

## C.1 Hermitian inner products and the Spectral Theorem

Let $V$ be a finite dimensional $\mathbb{C}$-vector space. A *positive definite Hermitian inner product* on $V$ is a pairing $\langle\ ,\ \rangle : V \times V \to \mathbb{C}$ such that

$$\begin{aligned} \langle \lambda v + v', w\rangle &= \lambda\langle v, w\rangle + \langle v', w\rangle \\ \langle v, w\rangle &= \overline{\langle w, v\rangle}, \quad \text{for all } v, v', w \in V \text{ and } \lambda \in \mathbb{C} \\ \langle v, v\rangle &\geqslant 0 \quad \text{with equality if and only if } v = 0. \text{ (notice by the last property } \langle v, v\rangle \in \mathbb{R}.) \end{aligned}$$

The first two properties imply that $\langle\ ,\ \rangle$ is conjugate-linear in the second variable, i.e.

$$\langle v, \lambda w + w'\rangle = \overline{\lambda}\langle v, w\rangle + \langle v, w'\rangle, \quad \text{for all } v, w, w' \in V \text{ and } \lambda \in \mathbb{C}.$$

Given a linear operator $A : V \to V$ there exists a unique map $A^* : V \to V$ called the *adjoint* of $A$ such that

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

for all $v, w \in V$. In the examples of linear operators and Hermitian inner products we consider in the course we compute their adjoints. Notice that $A^{**} = A$.

The linear operator $A$ is called *self adjoint* if $A^* = A$ and *normal* if $AA^* = A^*A$.

**Lemma C.1.1.** If $A$ is self adjoint then all of its eigenvalues are real.

*Proof.* Suppose $\lambda$ is an eigenvalue for $A$ with eigenvector $v$. We have

$$\lambda\langle v, v\rangle = \langle \lambda v, v\rangle = \langle Av, v\rangle = \langle v, Av\rangle = \langle v, \lambda v\rangle = \overline{\lambda}\langle v, v\rangle,$$

and hence $\lambda = \overline{\lambda}$. □

**Theorem C.1.2** (The Spectral Theorem)**.** If $(A_n)$ is a sequence of commuting normal operators, then there exists a basis of $V$ consisting of elements which are eigenvectors for all the $A_n$.

*Proof.* We first claim that If $A$ is normal then there exists a basis of $V$ consisting of eigenvectors of $A$. We begin with two observations:

(i) Let $A, B$ be commuting linear operators on $V$. Then $A$ preserves eigenspaces of $B$ and vice versa: Let $\lambda$ be an eigenvalue for $B$ with eigenspace $V_\lambda$ then

$$BAv = ABv = A\lambda v = \lambda Av, \text{ so } AV_\lambda \subseteq V_\lambda.$$

(ii) Let $W \subseteq V$ be a $A$-stable subspace of $V$, and put $W^\perp = \{v \in V : \langle v, w\rangle = 0 \text{ for all } w \in W\}$. Then for all $v \in W$, $w \in W^\perp$, $Av \in W$ as $W$ is $A$-stable and

$$\langle v, A^* w\rangle = \langle Av, w\rangle = 0,$$

so $W^\perp$ is stable under $A^*$.

We now prove the theorem by induction on the dimension of $V$, the one dimensional case being clear. Let $\lambda$ be an eigenvalue of $A$ with eigenspace $V_\lambda$. Then by normality $A$ and $A^*$ commute hence $V_\lambda$ is stable under $A^*$ by our first observation and hence $V_\lambda^\perp$ is stable under $A = A^{**}$ by our second observation. By restriction of $\langle\ ,\ \rangle$ to $V_\lambda^\perp$, the operator $T$ is still normal and so by induction on the dimension we have proved the claim.

If $A_1, A_2$ are normal commuting operators then we can write

$$V = \bigoplus_{\substack{\text{eigenvalues } \lambda \\ \text{of } A_2}} V_\lambda,$$

and $A_1$ preserves $V_\lambda$ so there is a basis of eigenvectors of $A_1$ for each $V_\lambda$. Putting these together gives a basis of $V$ of simultaneous eigenvectors for $A_1$ and $A_2$. We continue in this fashion and find a basis of simultaneous eigenvectors for all the $A_n$. □

# Bibliography


[1] Avner Ash and Robert Gross. *Summing it up*. Princeton University Press, Princeton, NJ, 2016. From one plus one to modern number theory.

[2] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[3] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[4] Toshitsune Miyake. *Modular forms*. Springer-Verlag, Berlin, 1989. Translated from the Japanese by Yoshitaka Maeda.

[5] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[6] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. Kanô Memorial Lectures, No. 1.