ORTHOGONAL DECOMPOSITION OF MODULAR FORMS

KARHAN K. KAYAN

Abstract. The aim of this paper is to prove that the space of modular forms can be orthogonally decomposed into the space of Eisenstein series and the space of cusp forms. However, we assume no previous knowledge of modular forms and build them from ground up. Along the way, we develop the machinery that is required to prove the decomposition theorem and delve into the theory of Hecke operators, Poincaré series, and Petersson inner product.

Contents

1. Introduction

The study of modular forms dates back to the nineteenth century when they were developed to study elliptic functions. Today they are largely known for the central role they play in number theory, the proof of Fermat's last theorem being just an example. Granted, it would be unfair to overlook their connection with the rest of mathematics. In the words of Alain Connes:

> Whatever the origin of one's journey, one day, if one walks far enough, one is bound to stumble on a well-known town: for instance, elliptic functions, modular forms, or zeta functions. "All roads lead to Rome," and the mathematical world is "connected." [1]

We can see them turn up in the study of combinatorics, arithmetic geometry, Riemann hypothesis, cryptography, analytic number theory, string theory, and the list continues to grow.

So, what are modular forms? Modular forms are holomorphic functions on the upper half-plane that satisfy certain growth conditions and functional equations under the action of linear fractional transformations. More precisely, when a modular form $f(z)$ defined for a subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is transformed by an element $\gamma \in \Gamma$, it gets scaled by an automorphy factor $j_\gamma(z)$ that depends on its so-called weight. We require the growth conditions so that we can expand $f(z)$ as a Fourier series in the limit as z goes to infinity. We will make it clear what this means in section 3. We shall also give a very concrete example by introducing the Eisenstein series, which arise naturally in the study of elliptic functions and 2-dimensional lattices.

As it turns out, a fundamental property of modular forms is that they form a finite-dimensional vector space, denoted $\mathbb{M}_k$. This is really surprising since most vector spaces of functions we are interested in are infinite-dimensional. This is true, for instance, for the space of holomorphic functions on $\mathbb{C}$. In section 2.4, we introduce the dimension theorem that gives the dimension of $\mathbb{M}_k$ explicitly and discuss the geometric ideas behind it.

We can define an inner product on the space of modular forms called the Petersson inner product and certain operators that are Hermitian with respect to it. These are the Hecke operators, which have a fascinating relationship with the so-called Poincaré series, a generalization of the Eisenstein series. Putting all of these tools together, we conclude the paper by showing that the space of modular forms can be decomposed into the space of Eisenstein series and their orthogonal complement, the space of cusp forms.

We assume the reader has some familiarity with complex analysis, basic abstract algebra, linear algebra, and basic Fourier analysis. Of course, the theory of modular forms draws from a very diverse range of topics, and some understanding of algebraic geometry and topology is useful; however, we do not make any further assumptions of background except for the ones mentioned.

2. Modular Forms

Definition 2.1. The principal congruence subgroup of level N is defined as

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

As a result, $\Gamma(1)$ is just $\mathrm{SL}_2(\mathbb{Z})$. Consider the homomorphism

$$h\colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

that takes the residue class modulo N of each entry of the input matrix. Then, by definition $\Gamma(N) = \ker h$. It follows that $\Gamma(N)$ is a normal subgroup of $\Gamma(1)$, which means $g\gamma g^{-1} \in \Gamma(N)$ for $g \in \Gamma(1)$ and $\gamma \in \Gamma(N)$. A fact we will not prove here about $\Gamma(1)$ is that the transformations

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

generate $\Gamma(1)$. A proof of this can be found in the section 1.2 of [2].

We often want to think about arbitrary subgroups of $\Gamma(1)$, so in this paper we will always denote an arbitrary finite-index subgroup of $\Gamma(1)$ by Γ unless otherwise stated. With this in mind, we now touch on how such Γ acts on the upper-half plane and introduce the important notion of a cusp.

2.1. **Action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$.** We define the upper-half plane as

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

We then define the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ by the Möbius transformation:

$$\gamma(z) = \frac{az+b}{cz+d}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

This action restricts to an action of Γ for an arbitrary subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$. The following proposition shows that if $z \in \mathbb{H}$, then $\gamma z \in \mathbb{H}$.

Proposition 2.2. *For* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$*, we have*

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

Proof. We have

$$\mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \mathrm{Im}\left(\frac{(az+b)\overline{(cz+d)}}{|cz+d|^2}\right) = \frac{\mathrm{Im}(adz + bc\overline{z})}{|cz+d|^2} = \frac{\mathrm{Im}(z)}{|cz+d|^2}$$

since $ad - bc = 1$. $\square$

A surprising fact about the upper-half plane is that it is conformally equivalent to the unit disk $\mathbb{D}$. In fact, we can write this conformal equivalence explicitly as $f(z) = \frac{i-z}{i+z}$. Furthermore, every conformal equivalence from $\mathbb{H}$ to itself (automorphism) is of the form γz for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. The proof of these two results can be found in the Chapter 8 of [4].

We define the projective line as $\mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$, which identifies the lines in $\mathbb{C}$ that pass through the origin. Then, $\mathrm{SL}_2(\mathbb{Z})$ acts on the projective line with the same Möbius transformation, so that:

$$\gamma z = \begin{cases} \frac{az+b}{cz+d} & \text{if } z \neq \infty \\ \frac{a}{c} & \text{if } z = \infty \end{cases} \quad , \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

We similarly define $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, and the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{P}^1(\mathbb{R})$ restricts to $\mathbb{P}^1(\mathbb{Q})$. We are now ready to define the notion of a cusp:

Definition 2.3. The cusps of a subgroup Γ are the orbits of points in $\mathbb{P}^1(\mathbb{Q})$ under the action of Γ.

We will usually identify these orbits by a representative element. As we shall prove below, because $\Gamma(1)$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$, the only cusp of $\Gamma(1)$ is $[\infty]$.

Proposition 2.4. $\Gamma(1)$ *acts transitively on* $\mathbb{P}^1(\mathbb{Q})$*. In other words, for any* $z, w \in \mathbb{P}^1(\mathbb{Q})$*, there exists a* $\gamma \in \Gamma(1)$ *such that* $\gamma(z) = w$*.*

Proof. We will show that we can send ∞ to any element of $\mathbb{P}^1(\mathbb{Q})$. Without loss of generality, let $n/m \in \mathbb{Q}$ be such that $\gcd(n, m) = 1$. Then, there exists a solution to the linear Diophantine equation $nd - bm = 1$ by Bézout's lemma. Thus, we can define

$$\gamma = \begin{pmatrix} n & b \\ m & d \end{pmatrix} \in \Gamma(1),$$

which sends ∞ to n/m. We can also handle the case of 0 with the transformation $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. $\square$

Definition 2.5. The width of the cusp ∞ for the group Γ is the smallest positive integer h such that the unipotent matrix

$$u_h := \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma.$$

For a general cusp x, the width of x for Γ is defined as the width of ∞ for $\gamma^{-1}\Gamma\gamma$ where $\gamma \in \Gamma(1)$ and $\gamma(\infty) = x$.

The transformation u_h is the translation mapping $z \mapsto z + h$. For this reason, the width of the cusp ∞ is sometimes called the least translation of Γ.

Having introduced the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ and the notion of cusps, we are now ready to define modular forms.

Definition 2.6. A function $f\colon \mathbb{H} \to \mathbb{C}$ is called a modular form of weight k for Γ if it satisfies the following conditions:

(1) f is holomorphic on $\mathbb{H}$.
(2) $f(\gamma z) = (cz + d)^k f(z)$, for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. (Automorphy condition)
(3) f is holomorphic (or equivalently bounded) at the cusps of Γ.

What we mean by the third condition is the following: Suppose f satisfies the first two conditions. Since $u_h \in \Gamma$, the second condition ensures that f is periodic with period h, and therefore has a Fourier expansion. Thus, we can write f as a function on a punctured disk so that $f(z) = F(q)$, where $q = \exp(2\pi i z/h)$. We call f holomorphic at the cusp ∞ if F is holomorphic at 0. For a general cusp x, let $\gamma \in \Gamma(1)$ such that $\gamma(\infty) = x$, and let h now denote its width. If f satisfies the first two conditions for Γ, then $g(z) := f(\gamma z)$ satisfies them for $\gamma^{-1}\Gamma\gamma$. Then, g is periodic with period h by Definition 2.5. We call f holomorphic at x if g is holomorphic at the cusp ∞.

We denote the space of all modular forms of weight k for Γ with $\mathbb{M}_k(\Gamma)$. Let I denote the identity matrix. Since $-I \in \Gamma$ for any subgroup Γ, the second condition implies that $f(z) = (-1)^k f(z)$. This means that f is always 0 for odd k. Therefore, $\mathbb{M}_k(\Gamma)$ always has dimension 0 for odd k, and thus is not an interesting case that we will consider. So, we will think of weight k as being even throughout the rest of this paper.

An example of modular forms is the Eisenstein series.

Definition 2.7. The Eisenstein series of weight k is the series

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

Proposition 2.8. *If $k > 2$, then the Eisenstein series of weight k converges absolutely uniformly.*

Proof. If we can prove that the series $\sum\limits_{(n,m)\neq 0}(|n|+|m|)^{-k}$ converges, then the result will follow by the M-test. We compute

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

Using the integral test we get

$$\begin{aligned}\sum_{(n,m)\neq 0}(|n|+|m|)^{-k} &\leq \sum_{m\in\mathbb{Z}}\left(\frac{1}{|m|^k}+2\int_{|m|}^{\infty}x^{-k}dx\right)\\ &= \sum_{m\in\mathbb{Z}}\left(\frac{1}{|m|^k}+K|m|^{1-k}\right)\end{aligned}$$

for a constant K. Since $k > 2$, both of the resulting sums converge and therefore $\sum_{(n,m)\neq 0}(|n|+|m|)^{-k} < \infty$. □

Since every term of the Eisenstein series is holomorphic, and it converges absolutely uniformly, it follows that it is holomorphic on the upper half-plane.

Now, let's check the modularity condition for Eisenstein series. We know that the transformations S and T generate $\Gamma(1)$. So it is enough to check the condition for these two matrices. We have

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

which follows from the fact that Eisenstein series converges absolutely, and thus can be rearranged. Furthermore,

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

Using absolute convergence again, we get

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

For the third condition of modular forms, observe that as $z\to i\infty$, $G_k(z)$ approaches $\sum_{m\in\mathbb{Z}\setminus\{0\}}1/m^k = 2\zeta(k)$. It follows that G_k is a modular form.

2.2. **Fundamental Domain.** For each subgroup Γ, we have a so-called fundamental domain associated with it. A fundamental domain is a region in the upper half-plane that contains exactly one point from each Γ-orbit. The following proposition shows what the fundamental domain for the action of $\Gamma(1)$ looks like.

Proposition 2.9. *Let* $D = \{z \in \mathbb{H} : |z| > 1, -\frac{1}{2} \leq \mathrm{Re}(z) < \frac{1}{2}\}$. *Then,* D *is a fundamental domain for* $\Gamma(1)$.

We will not prove this theorem here as the complete proof is quite tedious. But, the idea of the proof is as follows: Given any $z \in \mathbb{H}$, we can send it to the strip $-\frac{1}{2} \leq \mathrm{Re}(z) < \frac{1}{2}$ by applying the transformation T finitely many times. If after that transformation the point is not in the unit disk around the origin, then we are done. If it is, we apply S finitely many times and send it into D. To prove that any two points in D are not in the same $\Gamma(1)$ orbit, we argue by contradiction. Suppose there exist $z, z' \in D$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$ such that $\gamma z = z'$, and without loss of generality, assume that $\mathrm{Im}(z) \leq \mathrm{Im}(z')$. By Proposition 2.2, this implies that $|cz + d| \leq 1$. It can be shown that this is impossible for an element of D.

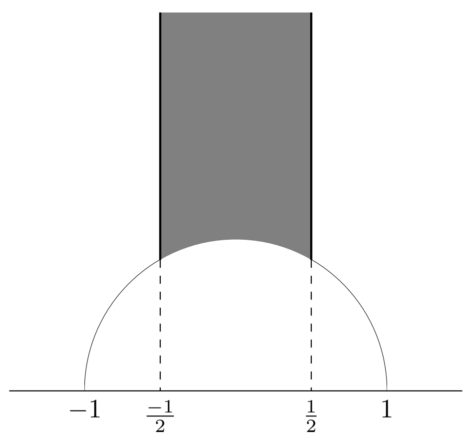

Figure 1. Fundamental Domain for $\Gamma(1)$

2.3. **Modular Forms and Lattices.** We define a complex lattice $\Lambda(z, w)$ to be a set of the form $\mathbb{Z}z + \mathbb{Z}w$ for some $z, w \neq 0 \in \mathbb{C}$. It turns out that we can alternatively define modular forms for $\Gamma(1)$ in terms of these lattices. More precisely, we will show that for certain functions F defined on the set of complex lattices, $f(z) = F(\Lambda(z, 1))$ is a modular form. This equivalent definition will give us a simpler and more intuitive definition of Eisenstein series, and it is usually used to define Hecke operators. Let $\mathbb{L}$ be the set of all complex lattices. We shall consider functions $F : \mathbb{L} \to \mathbb{C}$ that satisfy the following conditions:

(1) $F(\Lambda(z, 1))$ is a holomorphic function on $\mathbb{H}$ and at infinity.
(2) For $\lambda \in \mathbb{C}$, $F(\lambda\Lambda) = \lambda^{-k} F(\Lambda)$.

where the scaling action of $\mathbb{C}^\times$ on $\mathbb{L}$ is defined as $\lambda\Lambda(z, w) = \Lambda(\lambda z, \lambda w)$ for $\lambda \in \mathbb{C}$. We shall denote the set of all functions that satisfy the above conditions by $\mathbb{M}_k(\mathbb{L}, \mathbb{C})$.

Theorem 2.10. *If $F\colon \mathbb{L} \to \mathbb{C}$ satisfies the above conditions, then $f(z) = F(\Lambda(z,1))$ is a modular form of weight k for $\Gamma(1)$. Furthermore, the map $f \mapsto F$ is a bijection $\mathbb{M}_k(\Gamma(1)) \to \mathbb{M}_k(\mathbb{L},\mathbb{C})$.*

Proof. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. The key observation we will use is that $\Lambda(z,w)$ remains invariant under the transformation of γ. That is,

$$\Lambda(z,w) = \Lambda(z',w'), \text{ where } \begin{pmatrix} z' \\ w' \end{pmatrix} = \gamma \begin{pmatrix} z \\ w \end{pmatrix}.$$

The reason for this is that $\Lambda(z',w') \subset \Lambda(z,w)$ is already satisfied for any 2×2 integer matrix, and the equality holds if and only if the matrix is invertible, which is only true when $\det\gamma = \pm 1$.

With that in mind, to prove that f is a modular form of weight k, we only need to prove the automorphy condition since the other two conditions in Definition 2.6 are already assumed. We have

$$\begin{aligned} f(z) &= F(\Lambda(z,1)) \\ &= F(\Lambda(az+b, cz+d)) \\ &= (cz+d)^{-k} F(\Lambda((az+b)/(cz+d),1)). \end{aligned}$$

Since $F(\Lambda((az+b)/(cz+d),1)) = f(\gamma(z))$, we get

$$f(\gamma z) = (cz+d)^k f(z),$$

which satisfies the automorphy condition. □

Thus, we can define Eisenstein series as a function on the set of complex lattices:

$$G_k(\Lambda) = \sum_{w \in \mathbb{L}, w \neq 0} w^{-k},$$

which makes the automorphy condition seem more natural.

2.4. **Dimension of $\mathbb{M}_k$.** One of the most important facts about modular forms is that they constitute a finite-dimensional vector space. More precisely, $\mathbb{M}_k(\Gamma)$ is finite-dimensional for an arbitrary subgroup Γ of finite index. In fact, we can compute this dimension explicitly.

Theorem 2.11. *The dimension of $\mathbb{M}_k(\Gamma)$ is given by*

$$\dim(\mathbb{M}_{2k}(\Gamma)) = \begin{cases} 0 & \text{if } k \leq -1 \\ 1 & \text{if } k = 0 \\ (2k-1)(g-1) + v_\infty k + \sum_P \lfloor k(1-1/e_p) \rfloor & \text{if } k \geq 1 \end{cases}$$

where above:

- *g is the genus of the compactified Riemann surface $X(\Gamma) := \Gamma\backslash\mathbb{H}^*$,*
- *v_∞ is the number of inequivalent cusps of $X(\Gamma)$,*
- *e_p is the order of the stabilizer of p in the image $\overline{\Gamma}$ of Γ in $\Gamma(1)/\{\pm I\}$,*
- *the sum runs over a set of representatives for the elliptic points p of Γ.*

Proving this theorem is beyond the scope of this paper; however, we shall give a sense of what the jargon in its statement means and where the idea of the proof comes from. The general idea is that the quotient space of the upper half-plane under the action of Γ, denoted $\Gamma\backslash\mathbb{H}$, is a Riemann surface, or equivalently a one-dimensional complex manifold (up to finitely many points). We can compactify this surface by adding the cusp points to the upper half-plane and taking the quotient of this so-called extended upper half-plane. This is denoted by $X(\Gamma) := \Gamma\backslash\mathbb{H}^*$, and it turns out that it is a compact Riemann surface. Compact Riemann surfaces look like closed, orientable surfaces with a number of holes in them, and this number is called the genus of the surface. For instance, a sphere has genus 0, and a torus has genus 1. The points on $\mathbb{H}$ with a stabilizer larger than $\{\pm 1\}$ in Γ are called elliptic points. The idea is that because $X(\Gamma)$ is a compact Riemann surface, we can use a theorem from algebraic geometry called the Riemann–Roch theorem, which states the dimension of the space of meromorphic functions defined on a compact Riemann surface. Applying this theorem to $X(\Gamma)$ yields the dimension theorem for modular forms. A complete proof of this theorem can be found in section 2.8 of [3]. In the special case where it is applied to $\Gamma(1)$, we have the following result:

Theorem 2.12. $\dim(\mathbb{M}_{2k}(\Gamma(1))) = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor & k \equiv 2 \pmod{12} \\ \left\lfloor \frac{k}{12} \right\rfloor + 1 & \textit{else} \end{cases}$

As we have already discussed, there are no nonzero modular forms for $\Gamma(1)$ of odd weight. So, $\dim(\mathbb{M}_k(\Gamma(1))) = 0$ for odd k.

We will not need to use either of these dimension theorems to prove the orthogonal decomposition theorem. We only need the fact that $\mathbb{M}_k(\Gamma)$ is finite-dimensional. However, we shall demonstrate their usefulness in the next section by giving an example application in number theory.

3. Fourier Expansion of Modular Forms

Let f be a modular form for Γ. Let the least translation of f be h so that $f(z+h) = f(z)$ for all $z \in \mathbb{H}$. Because f is periodic with period h, it has a Fourier expansion of the form

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i z n/h} = \sum_{n=0}^{\infty} a_n q^{n/h}$$

where $q = e^{2\pi i z}$. As a result of this convention, this Fourier series is sometimes called the q-expansion of f. We can write $z = x + yi$ where $y > 0$ as z is in the upper half-plane. Then $|q| = |e^{2\pi i x/h}||e^{-2\pi y/h}| = |e^{-2\pi y/h}| < 1$. As a result, $f\colon \mathbb{H} \to \mathbb{C}$ corresponds to another function $F(q)\colon \mathbb{D} \to \mathbb{C}$ such that $F(q^{1/h}) = f(z)$. For a general cusp, we define everything very similarly, except that h is now the width of the cusp. We write the Laurent expansion of $F(q^{1/h})$ on the punctured unit disk and call it the Fourier expansion of f around that cusp. And because of the third condition of modular forms, the principal part of the Laurent series is 0. In other words, what the third condition means is that the q-expansion converges at the origin when $q = 0$. Thus, a_0 is the value of f at the cusp as all the other terms go to 0 as z approaches the cusp.

Example 3.1. As an example, we will derive the Fourier expansion of Eisenstein series. Let $\sigma_k(n) = \sum_{d|n} d^k$. The key step is that for $\tau \in \mathbb{H}$ and $k > 2$, we have

$$\sum_{n\in\mathbb{Z}} (\tau + n)^{-k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} m^{k-1} e^{-2\pi i m \tau},$$

which will take care of the inner sum for us. To prove this identity, we can immediately think of using the Poisson summation formula. It states that for a well-behaved function f,

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

where $\hat{f}$ is the Fourier transform of f [4]. For our purposes, choose $f(z) = (z+\tau)^{-k}$. Using contour integration, the Fourier transform of f is

$$\begin{aligned}\hat{f}(y) &= \int_{-\infty}^{\infty} (z+\tau)^{-k} e^{-2\pi i z y} dz \\ &= \int_{C} (z+\tau)^{-k} e^{-2\pi i z y} dz - \int_{C'} (z+\tau)^{-k} e^{-2\pi i z y} dz,\end{aligned}$$

where C' is the infinite half circle in the lower half plane, and C is the curve that consist of the real line and C'.

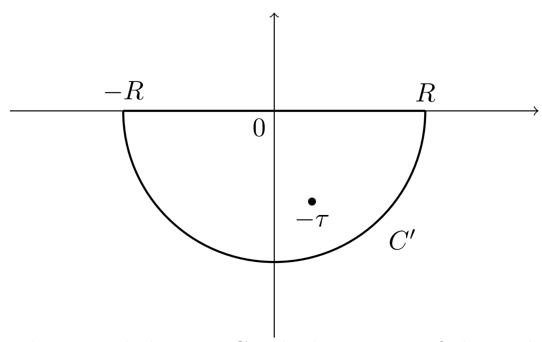

FIGURE 2. The intended curve C, which consists of the real line and C'

The integral in the lower half plane is 0 since $f(z)e^{-2\pi i z y}$ is a fast decaying function such that $|f(z)e^{-2\pi i z y}| = O(|z|^{-k})$. Furthermore, the only pole of the integrand is at $-\tau$. The residue at that pole is

$$\frac{(-2\pi i y)^{k-1}}{(m-1)!} e^{-2\pi i \tau y}.$$

We apply the residue theorem to find that

$$\hat{f}(y) = \frac{(-2\pi i)^k y^{k-1}}{(m-1)!} e^{-2\pi i \tau y}.$$

Then, the Poisson summation formula yields our identity. Now, we can turn our attention to the Eisenstein series:

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

Summing over divisors we obtain

$$\begin{aligned} G_k(z) &= 2\zeta(2) + 2\sum_{n=1}^{\infty}\sum_{d|n} \frac{(-2\pi i)^k}{(k-1)!} d^{k-1} e^{-2\pi i n z} \\ &= 2\zeta(2) + 2\frac{(-2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} \sigma_{k-1}(n) e^{-2\pi i n z}, \end{aligned}$$

which is exactly the q-expansion of the Eisenstein series.

As we have promised in the previous section, we shall now derive a purely number theoretic identity using the dimension theorem. We know that multiplying a modular form of weight k_1 and a modular form of weight k_2 gives us a modular form of weight $k_1 + k_2$. Therefore, squaring the Eisenstein series of weight 4 gives us a modular form of weight 8. By the dimension theorem for modular forms, we know that $\mathbb{M}_k(\Gamma(1))$ has dimension 1. Therefore, G_4^2 has to be a scalar multiple of G_8. If we write out the Fourier expansions of both functions we see that $G_4^2 = G_8$. As we have shown in the previous example, the Fourier coefficients of G_4 and G_8 are related to σ_3 and σ_7 respectively. Solving the equation $G_4^2 = G_8$ by substituting their Fourier expansions shows that we have

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

Notice that we could have also used this trick to find relations between divisor sums of different powers by multiplying Eisenstein series of different weights, for instance $G_4G_6 = G_{10}$, or $G_4G_{10} = G_{14}$.

4. Cusp Forms

A cusp form is a modular form that vanishes at all cusps. In other words, $f \in \mathbb{M}_k(\Gamma)$ is a cusp form if the coefficient $a_0 = 0$ in the Fourier expansion at any cusp. The space of all cusp forms in $\mathbb{M}_k(\Gamma)$ is denoted $\mathbb{S}_k(\Gamma)$. In this section, we will find upper bounds for cusp forms and their Fourier coefficients.

Lemma 4.1. *Let $f \in \mathbb{M}_k(\Gamma)$. Then*

$$z \mapsto y^{k/2}|f(z)|$$

is Γ invariant and bounded.

Proof. Let $z = x + yi$. Using Proposition 2.2, we have

$$\begin{aligned} \mathrm{Im}(\gamma z)^{k/2}|f(\gamma z)| &= \frac{y^{k/2}}{|cz+d|^k}|cz+d|^k|f(z)| \\ &= y^{k/2}|f(z)| \end{aligned}$$

Hence, it is invariant under the action of Γ. Then, it is enough to check boundedness in the fundamental domain. Given any horizontal line in $\mathbb{H}$, the lower part of the fundamental domain is compact, and when z approaches $i\infty$, f decays exponentially since it is a cusp form. Therefore, $y^{k/2}|f(z)|$ is bounded. □

Theorem 4.2. *Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a cusp form of weight k. Then, $|a_n| = O(n^{k/2})$.*

Proof. Let M be the bound in Lemma 4.1. We can write

$$\begin{aligned}|a_n| &= \left| \int_{-1/2}^{1/2} f(z) e^{-2\pi i n z} dx \right| \\ &\leq \int_{-1/2}^{1/2} |f(z)| e^{2\pi i n y} dx \\ &\leq \int_{-1/2}^{1/2} \frac{M}{y^{k/2}} e^{2\pi i n y} dx.\end{aligned}$$

Then, for $y > 0$ we obtain

$$|a_n| = \frac{M}{y^{k/2}} e^{2\pi i n y}.$$

Taking $y = 1/n$ yields the result

$$|a_n| \leq C n^{k/2}$$

for a constant C.

□

5. Petersson Inner Product

Definition 5.1. Let f and g be modular forms of weight k for Γ, where at least one of them is a cusp form. Let D be a fundamental domain for Γ. The function $\langle \cdot, \cdot \rangle \colon \mathbb{M}_k \times \mathbb{S}_k \to \mathbb{C}$, $\langle f, g \rangle = \iint_D f(z)\overline{g(z)} y^{k-2}\, dx\, dy$ is called the Petersson inner product.

It can be shown that the differential $f(z)\overline{g(z)}y^{k-2}\, dx\, dy$ is invariant under the action of $\Gamma(1)$, which means that the inner product is independent of the fundamental domain chosen.

It is immediate from the definition of the Petersson inner product that if the integral converges, it is a Hermitian inner product. That is, it satisfies the following properties:

(1) $\langle \alpha f + \beta g, h \rangle = \alpha \langle f, h \rangle + \beta \langle g, h \rangle$
(2) $\langle f, \alpha g + \beta h \rangle = \bar{\alpha} \langle f, g \rangle + \bar{\beta} \langle f, h \rangle$
(3) $\langle f, f \rangle \geq 0$, and $\langle f, f \rangle = 0$ if and only if $f = 0$.

We now show that the integral converges.

Proposition 5.2. *The Petersson inner product converges when it is defined on a fundamental domain of* $\Gamma(1)$.

Proof. It is enough to show that given an arbitrary cusp, the integral converges on a neighborhood of the cusp because then the remaining part is compact. Writing the Fourier expansions of f, g and using triangle inequalities, we can show that

$$\langle f, g \rangle \leq \iint_D \sum_{n=2}^{\infty} c_n q^{n/h} y^{k-2}\, dx\, dy,$$

where c_n are positive and the sum converges absolutely uniformly on a neighborhood around $q = 0$. This implies that we can interchange the order of summation and integration and obtain

$$\langle f, g \rangle \leq C \sum_{n=2}^{\infty} c_n q^{n/h}$$

for a constant C, which implies the result. $\square$

6. Poincaré Series

Our goal in this section is to be able to define an explicit modular form for any finite index subgroup $\Gamma \in \Gamma(1)$. If we wanted to construct a Γ invariant function, we could use the standard technique of averaging over group elements and define $f(z) = \sum\limits_{\gamma \in \Gamma} h(\gamma z)$ for a holomorphic function h. We adopt a similar strategy to construct a function that satisfies the automorphy condition of modular forms.

Definition 6.1. Given $\gamma \in \Gamma$, an automorphy factor is a nonzero holomorphic function $j_\gamma \colon \mathbb{H} \to \mathbb{C}$ satisfying the condition $j_{\gamma\alpha}(z) = j_\gamma(\alpha z) j_\alpha(z)$ for $\gamma, \alpha \in \Gamma$.

We shall construct a function f such that $f(\gamma z) = j_\gamma(z) f(z)$. In the case of modular forms, we have

$$j_\gamma(z) = (cz+d)^k \text{ and } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Identifying opposite signed matrices to be the same, we define $\Gamma' := \Gamma/\{I, -I\}$. If we were to define f such that $f(z) = \sum_{\gamma \in \Gamma} \frac{h(\gamma z)}{j_\gamma(z)}$, then under the action of $\alpha \in \Gamma$, we would get

$$\begin{aligned} f(\alpha z) &= \sum_{\gamma \in \Gamma} \frac{h(\gamma \alpha z)}{j_\gamma(\alpha z)} \\ &= \sum_{\gamma \in \Gamma} \frac{h(\gamma \alpha z) j_\alpha(z)}{j_{\gamma\alpha}(z)}. \end{aligned}$$

Since $\gamma\alpha$ runs through all elements of Γ, this gives us $f(\alpha z) = j_\alpha(z) f(z)$.

The problem with this definition turns out to be convergence. However, we can get the same automorphy property while also having less terms in the sum. To be able to do this, we look at the subset $\Gamma_\infty := \{\gamma \in \Gamma \colon j_\gamma = 1\}$. Because $j_{\gamma\alpha}(z) = j_\gamma(\alpha z) j_\alpha(z)$, if $\gamma, \alpha \in \Gamma_\infty$, then $j_{\gamma\alpha}(z) = 1, \forall z \in \mathbb{H}$. Therefore Γ_∞ is closed. Furthermore, we have

$$\begin{aligned} j_I(z) &= j_{\gamma\gamma^{-1}}(z) \\ &= j_\gamma(\gamma^{-1} z) j_{\gamma^{-1}}(z), \end{aligned}$$

so $j_\gamma = 1$ implies that $j_{\gamma^{-1}} = 1$. Thus, Γ_∞ is closed under inverses. As a result, Γ_∞ is a subgroup of Γ.

We can immediately think about summing over the quotient subgroup. However, if we are to sum over $\Gamma_\infty \setminus \Gamma'$, we should make sure that given an arbitrary $\theta \in \Gamma$, the choice of representatives of the coset $\Gamma_\infty \theta$ should not change the sum. Indeed, if choose h to be a function that is invariant under Γ_∞, we get exactly what we want: for $\alpha \in \Gamma_\infty\theta$ where $\alpha = \gamma_\infty\theta, \gamma_\infty \in \Gamma_\infty$:

$$\begin{aligned}\frac{h(\alpha z)}{j_\alpha(z)} &= \frac{h(\gamma_\infty \theta z)}{j_{\gamma_\infty\theta}(z)} \\ &= \frac{h(\theta z)}{j_{\gamma_\infty(\theta z)} j_\theta(z)} \\ &= \frac{h(\theta z)}{j_\theta(z)}\end{aligned}$$

The last step follows because $j_{\gamma_\infty} = 1$, for $\gamma_\infty \in \Gamma_\infty$.

Now let's look at the case of modular forms. We have $j_\gamma(z) = (cz+d)^k$. Also $(cz+d)^k = 1$ implies that $c = 0$ and $d = \pm 1$. Therefore, in our case Γ_∞ consists of matrices of the form $\begin{pmatrix} a & b \\ 0 & \pm 1\end{pmatrix}$. For the determinant to be 1, we require $a = \pm 1$. So,

$$\Gamma_\infty = \left\{ \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1\end{pmatrix} : b \in \mathbb{Z} \right\}.$$

As a result, we should be looking for a holomorphic function h that is invariant under the transformations of the form $\gamma(z) = z + b$, where b is the least translation of Γ. We see that $h(z) = e^{2\pi i n z/h}$ is exactly what we are looking for.

Definition 6.2. The Poincaré series for Γ of weight k and character n is the series

$$\varphi_n(z) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \frac{e^{\frac{2\pi i n \gamma(z)}{h}}}{(cz+d)^k}$$

where h is the least translation of Γ_∞

Proposition 6.3. *The Poincaré series of weight $k > 1$ and character $n \geq 0$ converges converges absolutely and uniformly on compact subsets of $\mathbb{H}$ and any fundamental domain of Γ.*

Proof. We will bound the Poincaré series by the Eisenstein series. We let $\gamma(z) = x + yi$. We have

$$\begin{aligned}\varphi_n(z) &\leq \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \frac{|e^{\frac{2\pi i n \gamma(z)}{h}}|}{|(cz+d)|^k} \\ &= \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \frac{e^{\frac{-2\pi n y}{h}}}{|(cz+d)|^k}.\end{aligned}$$

Since $\gamma(z) \in \mathbb{H}$, we have $e^{\frac{-2\pi n y}{h}} \leq 1$. Therefore,

$$\varphi_n(z) \leq \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \frac{1}{|(cz+d)|^k},$$

which is just the Eisenstein series with fewer terms. ∎

Lemma 6.4. *If f is a cusp form of weight k:*

$$\langle f, \varphi_n \rangle = \frac{h^k (k-2)! n^{1-k}}{(4\pi)^{k-1}} a_n$$

where a_n is the nth Fourier coefficient of f.

Proof.

$$\langle f, \varphi_n \rangle = \iint_D f(z) \sum_{\gamma \in \Gamma_\infty \setminus \Gamma} e^{\frac{-2\pi i n \overline{\gamma(z)}}{h}} \overline{(cz+d)^{-k}} y^{k-2}\, dx\, dy$$

We know that $\mathrm{Im}(\gamma z) = Im(z)/|cz+d|^2$. Then, substituting for y we get

$$\iint_D f(z) \sum_{\gamma \in \Gamma_\infty \setminus \Gamma} e^{\frac{-2\pi i n \overline{\gamma(z)}}{h}} \overline{(cz+d)^{-k}}\, \mathrm{Im}(\gamma z)^k |cz+d|^{2k} y^{-2}\, dx\, dy,$$

which is equivalent to

$$\iint_D f(z) \sum_{\gamma \in \Gamma_\infty \setminus \Gamma} e^{\frac{-2\pi i n \overline{\gamma(z)}}{h}} (cz+d)^k\, \mathrm{Im}(\gamma z)^k y^{-2}\, dx\, dy.$$

Using the automorphic property of f, we get

$$\iint_D \sum_{\gamma \in \Gamma_\infty \setminus \Gamma} e^{\frac{-2\pi i n \overline{\gamma(z)}}{h}} f(\gamma z)\, \mathrm{Im}(\gamma z)^k y^{-2}\, dx\, dy.$$

Because the sum converges absolutely and uniformly, we can interchange the sum and the integral to get

$$\sum_{\gamma \in \Gamma_\infty \setminus \Gamma} \iint_D e^{\frac{-2\pi i n \overline{\gamma(z)}}{h}} f(\gamma z)\, \mathrm{Im}(\gamma z)^k y^{-2}\, dx\, dy.$$

By making the change of variables $t = \gamma z$ and letting $t = x + yi$, we obtain

$$\sum_{\gamma \in \Gamma_\infty \setminus \Gamma} \iint_{\gamma D} e^{\frac{-2\pi i n (x - yi)}{h}} f(x+yi) y^k y^{-2}\, dx\, dy.$$

Since the intersection $\gamma_1 D \cap \gamma_2 D$ is a set of measure zero (a line) for $\gamma_1, \gamma_2 \in \Gamma_\infty \setminus \Gamma$ we can take the union and write

$$\iint_{\bigcup \gamma D} e^{\frac{-2\pi i n (x - yi)}{h}} f(x+yi) y^k y^{-2}\, dx\, dy.$$

This union covers the whole upper half-plane, so we have

$$\int_0^h \int_0^\infty e^{\frac{-2\pi i n (x - yi)}{h}} f(x+yi) y^k y^{-2}\, dy\, dx.$$

Plugging in the Fourier series for f, and interchanging the sum and the integrals, we get

$$\begin{aligned} &\sum_{m=1}^{\infty} \int_0^h \int_0^\infty e^{\frac{-2\pi i n (x - yi)}{h}} a_m e^{\frac{2\pi i m x}{h}} e^{\frac{-2\pi m y}{h}} y^k y^{-2}\, dy\, dx \\ &= \sum_{m=1}^{\infty} a_m \int_0^h e^{\frac{2\pi i x (m-n)}{h}}\, dx \int_0^\infty e^{\frac{-2\pi y (n+m)}{h}} y^{k-2}\, dy. \end{aligned}$$

The solution to the integral over x is $\delta_{m,n} h$. As a result, we obtain

$$\langle f, \varphi_n \rangle = a_n h \int_0^\infty e^{\frac{-4\pi y n}{h}} y^{k-2}\, dy.$$

The last integral can be turned into the gamma function by change of variables, so we get the desired result

$$\langle f, \varphi_n \rangle = \frac{h^k (k-2)! n^{1-k}}{(4\pi)^{k-1}} a_n.$$

□

Due to the previous lemma, we have the following result:

Theorem 6.5. $\mathbb{S}_k$ *is in the span of the set of Poincaré series of weight* k *and character* $n \geq 1$.

Proof. Let f be a cusp form. Since $\mathbb{M}_k = \operatorname{span}(\{\varphi_n\}_{n=1}^{\infty}) \oplus \operatorname{span}(\{\varphi_n\}_{n=1}^{\infty})^{\perp}$, we have $f = \varphi + g$ for $\varphi \in \operatorname{span}(\{\varphi_n\}_{n=1}^{\infty})$ and g in the orthogonal complement. Because both f and φ are cusp forms, g is a cusp form. But, $\langle \varphi_n, g \rangle = 0$ for all $n \geq 1$ as $g \in \operatorname{span}(\{\varphi_n\}_{n=1}^{\infty})^{\perp}$, which implies that all Fourier coefficients of g are 0. So, $g = 0$ and $f = \varphi$, which is in the span of Poincaré series. □

7. Hecke Operators

7.1. **Introduction to Hecke Operators.** In this section we will develop a tool known as Hecke operators. Denoting the nth Hecke operator by T_n, each T_n maps $\mathbb{M}_k(\Gamma(1))$ onto itself. We could also define them as operators on $\mathbb{M}_k(\Gamma)$ for arbitrary Γ, but the results are very similar to the case of $\Gamma(1)$, and thus we assume $\Gamma = \Gamma(1)$ for simplicity. These operators satisfy the following key properties:

(1) Hecke operators are multiplicative, that is $T_n \circ T_m = T_{nm}$ for $(n, m) = 1$.
(2) Hecke operators are Hermitian with respect to the Petersson inner product. So, $\langle T_n f, g \rangle = \langle f, T_n g \rangle$
(3) T_n maps the space of cusp forms $\mathbb{S}_k(\Gamma(1))$ onto itself .
(4) Hecke operators are commutative, that is $T_n T_m = T_m T_n$.

We shall exclusively consider modular forms of even weight k in this section. Let M_n be the set of 2×2 integer matrices with determinant n. For instance, for $n = 1$, M_1 is just $\Gamma(1)$. For $M \in M_n$, we define the operation

$$f|_k M(z) = (\det M)^{k/2} (cz + d)^{-k} f(Mz).$$

If for all $M \in M_1$, f satisfies $f|_k M(z) = f(z)$, then f is a modular form.

Definition 7.1. Given $f \in \mathbb{M}_k(\Gamma(1))$ and $n \in \mathbb{N}$, the nth Hecke operator is defined as

$$T_n f = n^{k-1} \sum_{M \in \Gamma \setminus M_n} f|_k M$$

Of course, we have to show that the sum is well defined, just as we did for the Poincaré series. Let $M = \gamma\theta$ for $\gamma \in \Gamma$ and $\theta \in M_n$. We have

$$f|_k(\gamma M)(z) = (f|_k \gamma)|_k M = f|_k M.$$

Therefore, the terms do not change for different representatives. We should also show that T_n maps the space of modular forms onto itself. That is, $T_n f$ is a modular form.

Proposition 7.2. *For every* $n \in \mathbb{N}$, $T_n f$ *is a modular form.*

Proof. We should show that $T_n f|\gamma = T_n f$ for $\gamma \in \Gamma$. We can see that

$$\begin{aligned} T_n f|\gamma &= n^{k-1} \sum_{M \in \Gamma \backslash M_n} f|M|\gamma \\ &= n^{k-1} \sum_{M \in \Gamma \backslash M_n} f|(M\gamma) \\ &= n^{k-1} \sum_{M \in \Gamma \backslash M_n} f|M \\ &= T_n f. \end{aligned}$$

The last step follows because $M\gamma$ is just a different representative. □

Now, how do we identify the elements of $\Gamma\backslash M_n$? In the next lemma, we find a set of representatives for $\Gamma\backslash M_n$. The subset

$$M' := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = n, d > 0, 0 \leq b < d \right\}$$

of M_n does the job.

Lemma 7.3. *M' is a complete set of representatives for $\Gamma\backslash M_n$.*

Proof. The mapping we will use is as follows: Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_n$. We choose c', d' in the representative such that

$$c' = c/\gcd(a,c) \text{ and } d' = -a/\gcd(a,c),$$

which implies that $\gcd(c', d') = 1$. Therefore, there exist integers a', b' such that $a'c' - b'd' = 1$. Then, the corresponding transformation satisfies

$$\gamma := \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma(1).$$

Let $P = \gamma M$. We see that $P_{2,1} = 0$ because

$$c'a + d'c = \frac{ac}{\gcd(a,c)} + \frac{-ac}{\gcd(a,c)} = 0.$$

Also, because $\det(\gamma) = 1$, we have $P_{1,1}P_{2,2} = n$. We can get $P_{2,2} > 0$ by changing the sign of M. The inequality $P_{1,2} < P_{2,2}$ can also be obtained through scaling γ by a $\Gamma(1)$ matrix of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. □

Using Lemma 7.3, we can define T_n more explicitly:

$$T_n f(z) = n^{k-1} \sum_{\substack{ad=n, d>0, \\ 0 \leq b < d}} d^{-k} f\left(\frac{az+b}{d}\right)$$

As a result of this new representation, we have the multiplicative property of Hecke operators.

Proposition 7.4. *Hecke operators are multiplicative, that is $T_n \circ T_m = T_{nm}$ for $(n, m) = 1$.*

Proof. Writing out the definitions, we get

$$T_nT_mf(z) = (nm)^{k-1} \sum_{\substack{ad=n,d>0,\\ 0\le b<d}} \sum_{\substack{a'd'=m,d'>0,\\ 0\le b'<d'}} (dd')^{-k} f\left(\frac{aa'z + (ab' + bd')}{dd'}\right).$$

As b runs through a residue system mod d, and b' runs through a residue system mod d', $ab' + bd'$ runs through a residue system mod dd'. Furthermore, for each term in the sum, $aa'dd' = nm$. As a result, we can substitute $a'' = aa', b'' = ab' + bd', d'' = dd'$ and get

$$T_nT_mf(z) = (nm)^{k-1} \sum_{\substack{a''d''=nm,d''>0,\\ 0\le b''<d''}} d''^{-k} f\left(\frac{a''z + b''}{d''}\right) = T_{nm}f(z).$$

□

Since T_nf is a modular function, it has a Fourier expansion. We would like to know the Fourier coefficients in terms of the Fourier coefficients of f.

Theorem 7.5. *Let $f = \sum_{n=0}^{\infty} c_nq^n$ be a modular form of weight k and $T_nf = n^{k-1}\sum_{m=0}^{\infty} b_mq^m$. Then, $b_m = \sum_{a|\gcd(m,n),a\ge1} a^{k-1}c_{mn/a^2}$.*

Proof. We start with

$$\begin{aligned} T_nf(z) &= n^{k-1} \sum_{\substack{ad=n,d>0,\\ 0\le b<d}} d^{-k} f\left(\frac{az+b}{d}\right) \\ &= n^{k-1} \sum_{\substack{ad=n,d>0,\\ 0\le b<d}} d^{-k} \sum_{m=0}^{\infty} c_m e^{2\pi im(az+b)/d}. \end{aligned}$$

Because $\sum_{b=0}^{d-1} e^{2\pi imb/d} = d$ for $d|m$ and 0 otherwise, we can write

$$\begin{aligned} T_nf(z) &= n^{k-1} \sum_{ad=n,d>0} d^{-k} \sum_{m=0}^{\infty} \sum_{0\le b<d} c_m e^{2\pi im(az+b)/d} \\ &= n^{k-1} \sum_{ad=n,d>0} \sum_{m'=0}^{\infty} d^{-k+1} c_{m'd} q^{am'} \end{aligned}$$

where we substituted $m = m'd$. Next, we substitute $j = am'$ and obtain

$$T_nf(z) = n^{k-1} \sum_{j=0}^{\infty} \sum_{a|(n,j),a\ge1} (n/a)^{-k+1} c_{jd/a} q^j,$$

which implies that the Fourier coefficients of T_nf are

$$b_j = \sum_{a|\gcd(n,j),a\ge1} a^{k-1} c_{nj/a^2}.$$

□

Corollary 7.6. *Let the nth Fourier coefficient of f be c_n. Then, we have $b_1 = c_n$ where b_1 is the 1st Fourier coefficient of $T_n f$.*

Corollary 7.7. *If f is a cusp form, then $T_n f$ is also a cusp form.*

Proof. Taking $m = 0$ in Theorem 7.5, we get $b_0 = \sigma_{k-1}(n)c_0$. So, whenever $c_0 = 0$, b_0 is also 0. □

7.2. **Eigenfunctions of Hecke operators.** One way to conceive Hecke operators is as operators acting on the finite-dimensional vector space $\mathbb{M}_k(\Gamma(1))$. Consequently, a fundamental we should ask is what the eigenfunctions and eigenvalues of these operators look like. It turns out that this problem is closely related to the Fourier coefficients of such eigenfunctions.

Theorem 7.8. *Let $f = \sum_{n=0}^{\infty} c_n q^n$ be an eigenfunction for all T_n, which means that $T_n f = \lambda_n f$ for some $\lambda_n \in \mathbb{C}$. If $c_1 = 0$, then f is 0. But, if $c_1 \neq 0$ and f is normalized such that $c_1 = 1$, then $\lambda_n = c_n$.*

Proof. In the case where $c_0 = 0$, comparing the Fourier coefficients of $T_n f$ and $\lambda_n f$, we get $b_1 = \lambda_n c_1$. Now, we use Corollary 7.6 and obtain $\lambda_n c_1 = c_n = 0$ for all $n \in \mathbb{N}$ since $c_0 = 0$. Hence, $f = 0$.

For the second part, we use the same argument to get $\lambda_n c_1 = c_n$. Since $c_1 = 1$, we get $\lambda_n = c_n$. □

Corollary 7.9. *Let f be a normalized eigenform for all T_n and c_n be its Fourier coefficients. Then, for $(n, m) = 1$, we have $c_{nm} = c_n c_m$ for all $n, m \in \mathbb{N}$.*

Proof. Because of the multiplicative property of Hecke operators, we have

$$\lambda_n \lambda_m f = T_n T_m f = T_{nm} f = \lambda_{nm} f,$$

which means that $\lambda_n \lambda_m = \lambda_{nm}$. By Theorem 7.8, we obtain $c_{nm} = c_n c_m$. □

Now, we will look at how Hecke operators act on Poincaré series. We will later use these relations to prove that Hecke operators are Hermitian and Eisenstein series are eigenforms.

Theorem 7.10. *Let φ_m be the mth Poincaré series of weight k. Then*

$$T_n \varphi_m = n^{k-1} \sum_{d|(n,m)} d^{1-k} \varphi_{nm/d^2}$$

Proof. The idea and calculations are very similar to the proof of Theorem 7.5. □

A special case of this theorem yields a very important corollary.

Corollary 7.11. *Eisenstein series is an eigenform for every Hecke operator.*

Proof. Taking $m = 0$ in the previous theorem yields $T_n \varphi_0 = \sigma_{k-1}(n)\varphi_0$. □

We will use this corollary later on to prove that Eisenstein series are orthogonal to cusp forms.

7.3. **Hecke operators are Hermitian.** One of the most important properties of Hecke operators is that they are Hermitian with respect to the Petersson inner product. In this section we will prove this result. The idea is to first prove that Hecke operators are Hermitian on Poincaré series. Then, we extend the result to cusp forms by writing them as linear combinations of Poincaré series. For the rest of this section, let $c_l(n,m), c_m(l)$ denote the mth Fourier coefficient of $n^{1-k}T_n\varphi_m(z)$ and φ_l respectively.

Lemma 7.12. *We have the following identities*

(1) $\langle T_n\varphi_l, \varphi_m\rangle = A\sum_{d|(n,l)} d^{1-k}c_m(nl/d^2)$ *for some constant* A.
(2) $m^{1-k}c_m(l,n) = n^{1-k}c_n(l,m)$
(3) $c_l(n,m) = c_l(m,n)$

Proof. (1) is a straightforward application of Theorem 7.5 and Lemma 6.4. The second identity follows immediately from the symmetry in Theorem 7.5. The third identity follows from the symmetry in the first identity. □

These symmetry relations will help us manipulate inner products of Poincaré series.

Lemma 7.13.

$$\langle T_n\varphi_m, \varphi_q\rangle = \langle T_n\varphi_q, \varphi_m\rangle$$

for all n, m, q.

Proof. Using Lemma 6.4 we get

$$\langle T_n\varphi_m, \varphi_q\rangle = An^{k-1}q^{1-k}c_q(n,m).$$

Then, we use the symmetry identities to obtain

$$An^{k-1}q^{1-k}c_q(n,m) = An^{k-1}m^{1-k}c_m(n,q),$$

which equals $\langle T_n\varphi_q, \varphi_m\rangle$. □

Corollary 7.14. *Fourier coefficients of Poincaré series are real.*

Proof. Since $T_1\varphi_a = \varphi_a$, we can see that

$$\begin{aligned}\langle \varphi_a, \varphi_b\rangle &= \langle T_1\varphi_a, \varphi_b\rangle \\ &= \langle T_1\varphi_b, \varphi_a\rangle \\ &= \langle \varphi_b, \varphi_a\rangle,\end{aligned}$$

which implies that $c_a(b)$ is real due to Lemma 6.4. □

Corollary 7.15. $\langle T_n\varphi_l, \varphi_m\rangle$ *is real and therefore equals* $\langle \varphi_m, T_n\varphi_l\rangle$.

Proof. We just have to apply Corollary 7.14 to identity (3) in Lemma 7.12. □

Theorem 7.16. *Hecke operators are Hermitian with respect to the Petersson inner product, that is*

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

for cusp forms f, g.

Proof. By Theorem 6.5, f and g are linear combinations of $\{\varphi_n\}_{n\geq 1}$. Then, we can write

$$f = \sum_{l=1}^{L} a_l \varphi_l, g = \sum_{m=1}^{M} b_m \varphi_m.$$

Substituting these series into the equation we get

$$\begin{aligned} \langle T_n f, g\rangle &= \langle T_n \sum_{l=1}^{L} a_l \varphi_l, \sum_{m=1}^{M} b_m \varphi_m\rangle \\ &= \sum_{l=1}^{L}\sum_{m=1}^{M} a_l b_m \langle T_n \varphi_l, \varphi_m\rangle. \end{aligned}$$

Next, we use Lemma 7.13 to get

$$\langle T_n f, g\rangle = \sum_{l=1}^{L}\sum_{m=1}^{M} a_l b_m \langle T_n \varphi_m, \varphi_l\rangle.$$

We can now apply Corollary 7.15 to change the order of the inner product and get

$$\langle T_n f, g\rangle = \sum_{l=1}^{L}\sum_{m=1}^{M} a_l b_m \langle \varphi_l, T_n \varphi_m\rangle.$$

Now, we just follow through and obtain the result

$$\langle T_n f, g\rangle = \langle \sum_{l=1}^{L} a_l \varphi_l, \sum_{m=1}^{M} b_m T_n \varphi_m\rangle = \langle f, T_n g\rangle.$$

□

We know that $\mathbb{S}_k(\Gamma)$ is a finite-dimensional vector space. Since Hecke operators are Hermitian, we can apply the spectral theorem to get the following corollary:

Corollary 7.17. *For every positive integer n, there exists a basis of eigenforms of T_n for $\mathbb{S}_k(\Gamma)$.*

This corollary will constitute a central piece in the proof of $\mathbb{E}_k(\Gamma) \oplus \mathbb{S}_k(\Gamma)$, the orthogonal decomposition theorem. We also get another corollary due to linear algebra.

Corollary 7.18. *If f is a normalized eigenform for all hecke operators, then the Fourier coefficients of f are real.*

Proof. Due to Theorem 7.8, we only need to show that the eigenvalues of f are real. But, it is a standard result in linear algebra that hermitian operators have real eigenvalues. □

8. Orthogonal Decomposition of $\mathbb{M}_k(\Gamma)$

In this section, we will prove that $\mathbb{M}_k(\Gamma)$ can be orthogonally decomposed into a direct sum of cusp forms and Eisenstein series. To be able to do this, we will need to assume that the subgroup Γ is normal. Therefore, for the rest of this section Γ denotes $\Gamma(N)$ for an arbitrary N, which we know to be a normal subgroup. What we mean by the space of Eisenstein series for an arbitrary Γ is the space spanned by the Poincaré series of character 0 for Γ, and we denote this space by $\mathbb{E}_k(\Gamma)$.

The strategy we shall adopt for the proof is as follows: We first prove that Eisenstein series are orthogonal to cusp forms that are also eigenforms. This can be achieved by using the tools we developed in the section on eigenfunctions of Hecke operators. To generalize this result, we shall use the fact that $\mathbb{S}_k(\Gamma)$ has a basis of eigenforms. Then, we move on to prove that every modular form in $\mathbb{M}_k(\Gamma)$ can be written as a sum of cusp forms and Eisenstein series.

Theorem 8.1. *If $f \in \mathbb{S}_k$ is an eigenform for all T_n, then $\langle G_k, f\rangle = 0$. That is, the set of cusp forms that are eigenforms is orthogonal to the set of Eisenstein series.*

Proof. Without loss of generality assume that G_k and f are normalized. Suppose, for the sake of contradiction, that $\langle G_k, f\rangle \neq 0$. Let

$$G_k(z) = \sum_{n=0}^{\infty} a_n q^n \text{ and } f(z) = \sum_{n=1}^{\infty} b_n q^n$$

be the q-expansions of G_k and f respectively. By Corollary 7.11, G_k is an eigenform for all T_n. Then, because both are normalized eigenforms, we have $T_n G_k = a_n G_k$ and $T_n f = b_n f$ for $n \geq 1$. Since Hecke operators are Hermitian, we can write

$$\begin{aligned} a_n\langle G_k, f\rangle &= \langle T_n G_k, f\rangle \\ &= \langle G_k, T_n f\rangle \\ &= \overline{b_n}\langle G_k, f\rangle. \end{aligned}$$

We know by Corollary 7.18 that b_n is real. Therefore, $a_n\langle G_k, f\rangle = b_n\langle G_k, f\rangle$ for $n \geq 1$. But, $\langle G_k, f\rangle \neq 0$ implies that $a_n = b_n$ for $n \geq 1$. Hence G_k and f differ by a constant. But, this is impossible since $G_k - f$ is a modular form of weight k. □

We have proved in Corollary 7.17 that $\mathbb{S}_k(\Gamma)$ has a basis of eigenforms. Since we also know that it is a finite-dimensional vector space, we have the following result

Corollary 8.2. *The set of cusp forms $\mathbb{S}_k(\Gamma)$ is orthogonal to the set of Eisenstein series $\mathbb{E}_k(\Gamma)$.*

We have essentially proved $\mathbb{S}_k(\Gamma) \perp \mathbb{E}_k(\Gamma)$. But, how can show that this decomposition actually gives us a direct sum, i.e. $\mathbb{M}_k(\Gamma) = \mathbb{S}_k(\Gamma) \oplus \mathbb{E}_k(\Gamma)$? Let $f \in \mathbb{M}_k(\Gamma)$ be an arbitrary modular form. Suppose that for each cusp, we can find an Eisenstein series that takes a nonzero value at that cusp, but vanishes at all the other cusps. For a given cusp p, denote this function by φ^p. Then, for suitable coefficients a_p, we can write

$$f - \sum_{\text{cusps } p \text{ in } \Gamma} a_p \varphi^p = g$$

so that g is a cusp form. This means that if we can manage to find such φ^p, then $\mathbb{M}_k(\Gamma) = \mathbb{S}_k(\Gamma) \oplus \mathbb{E}_k(\Gamma)$ follows, which is exactly what we will be doing in the next theorem.

Let p be the cusp we are working with. Due to Proposition 2.4, we know that $\Gamma(1)$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$, which means that there exists $\sigma \in \Gamma(1)$ such that $\sigma(p) = i\infty$. We shall define

$$\varphi^p(z) = j_\sigma(z)^k \varphi_0(\sigma z)$$

where $j_\sigma(z)$ denotes $1/(cz+d)^k$ for $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and φ_0 is the Poincaré series of character 0 and weight k for Γ.

Theorem 8.3. *Given a cusp p, φ^p is a modular form of weight k for Γ. Furthermore, it takes a nonzero value at the cusp p, and vanishes at all the other cusps.*

Proof. Since p is fixed, we simply denote φ^p by φ in this proof. To prove that φ is a modular form, it is enough to check the automorphy condition as the other two conditions follow immediately from the definition of φ. Let γ be an arbitrary element of Γ. By definition

$$\varphi(\gamma z) = j_\sigma(\gamma z)^k \varphi_0(\sigma\gamma z).$$

We know that Γ is normal, which means that $\sigma\gamma\sigma^{-1} \in \Gamma$, therefore we can use the automorphy condition for φ_0 and get

$$\varphi_0(\sigma\gamma z) = \varphi_0(\sigma\gamma\sigma^{-1}\ \sigma z) = j_{\sigma\gamma\sigma^{-1}}(\sigma z)^{-k}\varphi_0(\sigma z).$$

We can also write $\varphi_0(\sigma z)$ in this equation in terms of $\varphi(z)$ by using the definition of $\varphi(z)$:

$$\varphi_0(\sigma z) = \varphi(z) j_\sigma(z)^{-k}$$

Substituting all of these into the first equation, we get

$$\varphi(\gamma z) = j_\sigma(\gamma z)^k j_{\sigma\gamma\sigma^{-1}}(\sigma z)^{-k}\varphi(z) j_\sigma(z)^{-k}.$$

But, the automorphy factors combine so that

$$j_{\sigma\gamma\sigma^{-1}}(\sigma z)^{-k} j_\sigma(z)^{-k} = j_{\sigma\gamma}(z)^{-k} = j_\sigma(\gamma z)^{-k} j_\gamma(z)^{-k}.$$

Substituting this into the equation, we obtain

$$\varphi(\gamma z) = j_\gamma(z)^{-k}\varphi(z),$$

which is exactly the automorphy condition for modular forms.

The next step is to prove that φ takes a nonzero value at the cusp p, but it is 0 at the other cusps. We shall first prove that φ should be zero at the other cusps. Let μ be a different cusp. Then, $\sigma\mu$ is a cusp, but $\sigma\mu \neq i\infty$. This means that $\varphi_0(\sigma\mu) = 0$, which implies $\varphi(\mu) = 0$. Now, suppose for the sake of contradiction that φ is a cusp form. Thus, φ can be written as a linear combination of $\{\varphi_n\}_{n\geq 1}$. Let

$$\varphi(z) = j_\sigma(z)^k \varphi_0(\sigma z) = \sum_{n=1}^{N} a_n \varphi_n(z).$$

Taking $\sigma^{-1}z$ in the argument we see that

$$j_\sigma(\sigma^{-1}z)^k \varphi_0(z) = \frac{1}{j_{\sigma^{-1}}(z)^k}\varphi_0(z) = \sum_{n=1}^{N} a_n \varphi_n(\sigma^{-1}z).$$

We then take out the σ^{-1}s to get

$$\varphi_0(z) = \sum_{n=1}^{N} a_n \varphi_n(z),$$

which is a contradiction since we know that φ_0 is not a cusp form. $\square$

Combining the previous theorem and the fact that $\mathbb{S}_k(\Gamma) \perp \mathbb{E}_k(\Gamma)$, we conclude this paper with the desired result

Corollary 8.4. *We have the following orthogonal decomposition*

$$\mathbb{M}_k(\Gamma) = \mathbb{E}_k(\Gamma) \oplus \mathbb{S}_k(\Gamma)$$

Acknowledgments

I would like to thank my mentor Minh-Tam Trinh who not only guided me through this project, but also helped me see the bigger picture in every step of the way. It has been a pleasure for me to work with someone as inspiring as he is. I also want to thank Prof. Peter May for organizing this wonderful research program at the University of Chicago.

References

[1] Timothy Gowers, June Barrow-Green, Imre Leader. Princeton Companion to Mathematics. Princeton University Press, 2008.
[2] J.S. Milne. Modular Functions and Modular Forms. http://www.jmilne.org/math/CourseNotes/MF.pdf
[3] R. C. Gunning. Lectures on Modular Forms. Princeton University Press, 1962.
[4] Elias M. Stein, Rami Shakarchi. Complex Analysis. Princeton University Press, 2003