MODULAR FORMS AND HECKE OPERATORS

SAMANDA (YUTING) HU

Abstract. This paper focuses on discussing Hecke operators in the theory of modular forms and its relation to Hecke rings which occur in representation theory. We will first introduce the basic definitions and properties of modular forms and Hecke operators. In particular, we will show that the space of cusp forms of an arbitrary weight with respect to a specific congruence subgroup is an inner product space and discuss that the space has an orthogonal basis of simultaneous eigenvectors for the Hecke operators. We will then shift the focus to Hecke rings and do relevant computations regarding the Hecke ring of $GL_2(\mathbb{Q}_p)$.

Contents

1. Introduction

Modular forms are functions on the complex upper half plane that satisfy certain transformation conditions and holomorphy conditions. The theory of modular forms is a significant branch of modern number theory – for instance, the Modularity Theorem suggests that *all rational elliptic curves arise from modular forms* with some restrictions. This theorem was essential to the proof of Fermat's Last Theorem by Richard Taylor and Andrew Wiles.

In this paper, we aim to discuss Hecke operators in the theory of modular forms. We will show how the Hecke ring $\mathcal{H}(GL_2(\mathbb{Q}_p), GL_2(\mathbb{Z}_p))$, the ring of all locally constant, compactly supported $GL_2(\mathbb{Z}_p)$-bi-invariant functions $f : GL_2(\mathbb{Q}_p) \to \mathbb{C}$, is associated with the Hecke operator attached to p. To do so, we will first give an introduction to modular forms with some relevant properties and basic

Date: August 28 2020.

computations. We will then introduce Hecke operators and discuss some of their properties. From here, we will shift topics to discuss Hecke rings and give relevant computations on the Hecke ring of $GL_2(\mathbb{Q}_p)$.

This expository paper is written in part for the University of Chicago REU programme of 2020. For the paper, we will presume basic knowledge of linear algebra, algebra and complex analysis.

2. Modular Form and Congruence Subgroup

In order to define modular forms, we will first introduce principal congruence subgroup and congruence subgroups.

Definition 2.1. Let N be a positive integer. The *principal congruence subgroup of level* N is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

A subgroup Γ of $SL_2(\mathbb{Z})$ is a *congruence subgroup* if $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbb{Z}^+$, in which case Γ is a *congruence subgroup of level* N.

Some important congruence subgroups are

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} \star & \star \\ 0 & \star \end{pmatrix} \mod N \right\} \tag{2.2}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix} \mod N \right\} \tag{2.3}$$

where $\star$ denotes unspecified value at that position.

We need two more definitions to define what a modular forms with respect to a congruence subgroup.

Definition 2.4. Let $\mathbb{H}$ denote the upper half complex plane, i.e.

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

Let $\gamma \in SL_2(\mathbb{Z})$ be $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\tau \in \mathbb{H}$. The *factor of automorphy* $j(\gamma, \tau)$ is

$$j(\gamma, \tau) = c\tau + d.$$

Now, let f be a function mapping from $\mathbb{H}$ to $\mathbb{C}$ and k be an element in $\mathbb{Z}$. The *weight-k operator* $[\gamma]_k$ on f is

$$(f[\gamma]_k)(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau))$$

where $\gamma(\tau)$ is

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d}. \tag{2.5}$$

Using the above notation,

Definition 2.6. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and k be an integer. A function $f : \mathbb{H} \to \mathbb{C}$ is a *modular form of weight k with respect to* Γ if

(i) f is holomorphic
(ii) f is weight-k invariant under Γ, i.e. for all $\gamma \in \Gamma$, $f[\gamma]_k = f$
(iii) $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$.

The set of modular forms of weight k with respect to Γ is denoted as $\mathcal{M}_k(\Gamma)$. In addition, the set of $\mathcal{M}_k(\Gamma)$ forms a graded ring. This can be denoted as

$$\mathcal{M}(\Gamma) = \bigoplus_{k\in\mathbb{Z}} \mathcal{M}_k(\Gamma).$$

In addition, $\mathcal{M}_k(\Gamma)$ are vector spaces over $\mathbb{C}$.

Some trivial examples include constant functions on $\mathbb{H}$ – they are modular forms of weight 0; in particular, the zero function on $\mathbb{H}$ is a modular form of every weight. For non-trivial examples, we turn to Eisenstein series of even weight greater than 2. They are defined as follows,

Definition 2.7. An *Eisenstein series of weight* $2k$, with $k > 1, k \in \mathbb{Z}$, is defined as

$$\mathrm{G}_{2k}(\tau) = \sum_{(c,d)\in\mathbb{Z}^2-\{(0,0)\}} \frac{1}{(c\tau+d)^{2k}}, \tau \in \mathbb{H}.$$

By checking conditions in the definition, we see that Eisenstein series of weight $2k$ for $k > 1$ is a modular form of weight $2k$.

Each congruence subgroup Γ of $SL_2(\mathbb{Z})$ contains a translation matrix $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ for some minimal $h \in \mathbb{Z}^+$. Thus, if f is a modular form with respect to Γ, then f has a Fourier expansion,

$$f(\tau) = \sum_{n=0}^{\infty} a_n {q_h}^n, q_h = e^{2\pi i\tau/h}.$$

By considering the Fourier expansion of $f[\alpha]_k$ for all $\alpha \in SL_2(\mathbb{Z})$, we can define a cusp form with respect to Γ.

Definition 2.8. A *cusp form of weight k with respect to* Γ is a modular form of weight k with respect to Γ such that for all $\alpha \in SL_2(\mathbb{Z})$, the Fourier expansion of $f[\alpha]_k$ has no constant coefficients, i.e. $a_0 = 0$.

The set of cusp forms of weight k with respect to Γ is denoted as $\mathcal{S}_k(\Gamma)$ and the set of cusp forms with respect to Γ forms a graded ideal in $\mathcal{M}(\Gamma)$, denoted as

$$\mathcal{S}(\Gamma) = \bigoplus_{k\in\mathbb{Z}} \mathcal{S}_k(\Gamma).$$

3. Action of $GL_2^+(\mathbb{Q})$ on $\mathbb{H}$

Hecke operators are defined by double coset operators, which are characterized by the action of $GL_2^+(\mathbb{Q})$, the group of 2-by-2 matrices with positive determinant and rational entries, on modular forms. We will first look at how $GL_2^+(\mathbb{Q})$ acts on $\mathbb{H}$. From here, by extending the definition of factors of automorphy and weight-k operators to $GL_2^+(\mathbb{Q})$, we get an action of $GL_2^+(\mathbb{Q})$ on the space of modular forms.

For $\gamma \in GL_2^+(\mathbb{Q})$ and $\tau \in \mathbb{H}$, define $\gamma(\tau)$ as

$$\gamma(\tau) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau+b}{c\tau+d}.$$

Because $\mathrm{Im}(\gamma(\tau)) = \det\gamma \cdot \mathrm{Im}(\tau)/|c\tau+d|^2$ and $\det\gamma \geq 0$, i$\gamma(\tau) \in \mathbb{H}$. The definition above gives us an action of $GL_2^+(\mathbb{Q})$ on $\mathbb{H}$.

Definition 3.1. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{Q})$ and $\tau \in \mathbb{H}$. The *factor of automorphy* $j(\gamma, \tau)$ is

$$j(\gamma, \tau) = c\tau + d. \tag{3.2}$$

For $f : \mathbb{H} \to \mathbb{C}$ and $k \in \mathbb{Z}^+$. The *weight-k operator* $[\gamma]_k$ on f is

$$(f[\gamma]_k)(\tau) = (\det \gamma)^{k-1} j(\gamma, \tau)^{-k} f(\gamma(\tau)). \tag{3.3}$$

The following result gives us that by mapping $f \in \mathcal{M}_k(\Gamma)$ to $f[\gamma]_k$ for $\gamma \in GL_2^+(\mathbb{Q})$, $GL_2^+(\mathbb{Q})$ acts on $\mathcal{M}_k(\Gamma)$ for a congruence subgroup Γ.

Lemma 3.4. *For all $\gamma, \gamma' \in GL_2^+(\mathbb{Q})$ and $\tau \in \mathbb{H}$*

(i) $j(\gamma\gamma', \tau) = j(\gamma, \gamma'(\tau)) j(\gamma', \tau)$
(ii) $(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau))$
(iii) $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$

Proof. The first two parts of the lemma can be proven by direct computations. For the last part of the lemma, take $f : \mathbb{H} \to \mathbb{C}$. By direct substitution on the left hand side of the equation,

$$(f[\gamma\gamma']_k)(\tau) = (\det(\gamma\gamma'))^{k-1} j(\gamma\gamma', \tau)^{-k} f(\gamma\gamma'(\tau)). \tag{3.5}$$

On the right hand side of $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$,

$$((f([\gamma]_k))[\gamma']_k)(\tau) = (\det \gamma')^{k-1} j(\gamma', \tau))^{-k} (f([\gamma]_k))(\gamma'(\tau)).$$

Expanding the equation gives

$$((f([\gamma]_k))[\gamma']_k)(\tau) = (\det \gamma' \cdot \det \gamma)^{k-1} j(\gamma', \tau))^{-k} j(\gamma, \gamma'(\tau))^{-k} f(\gamma(\gamma'(\tau))). \tag{3.6}$$

By rearranging, applying the first two parts of the current proposition and the fact that the determinant is multiplicative, the right-hand side of (3.6) is thus equal to the right-hand side of (3.5). Therefore, $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$. $\square$

4. Hecke Operators

Since Hecke operators are defined through double coset operators, we will first introduce double coset operators and prove the definition is well-defined. Then, we will define Hecke operators and introduce some of their properties, in particular, proving that the Hecke operators commute with each other. From here, we will focus on the space of cusp forms $\mathcal{S}_k(\Gamma_1(N))$ and show that it is an inner product space with an orthogonal basis of simultaneous eigenvectors of Hecke operators.

4.1. Double Coset Operator.

Let Γ_1 and Γ_2 be congruence subgroups of $SL_2(\mathbb{Z})$. For $\alpha \in GL_2^+(\mathbb{Q})$,

$$\Gamma_1 \alpha \Gamma_2 = \{\gamma_1 \alpha \gamma_2 : \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}$$

is a *double coset* of $GL_2^+(\mathbb{Q})$. Because Γ_1 acts on the double coset $\Gamma_1 \alpha \Gamma_2$ by left multiplication, we can rewrite $\Gamma_1 \alpha \Gamma_2$ as a disjoint union of orbit spaces of the group action,

$$\Gamma_1 \alpha \Gamma_2 = \bigcup \Gamma_1 \beta_j$$

where β_j are orbit representatives.

We will define the double coset operator as the sum of the weight-k operator for each right coset representative. However, for the definition to be well-defined, we need to show the decomposition of the double coset is a *finite* disjoint union of right cosets of Γ_1.

Proposition 4.1. *The double coset* $\Gamma_1\alpha\Gamma_2 = \bigcup \Gamma_1\beta_j$ *and the union is finite.*

Proof. We will follow the proof presented on [1] P164. In order to show that the union is finite, we will first show two following lemmas:

Lemma 4.2. *Let* α *be an element in* ${GL_2}^+(\mathbb{Q})$ *and* Γ *be a congruence subgroup. Then* $\alpha^{-1}\Gamma\alpha \cap SL_2(\mathbb{Z})$ *is also a congruence subgroup.*

Proof of the lemma. By $\alpha \in {GL_2}^+(\mathbb{Q})$, there exists minimal positive integers n_0, n_1 such that $n_0\alpha \in M_2(\mathbb{Z})$, $n_1\alpha^{-1} \in M_2(\mathbb{Z})$. Additionally, as Γ is a congruence subgroup, there exists $n \in \mathbb{Z}$ such that $\Gamma(n) \subseteq \Gamma$. Let $\tilde{N}$ be the product n_0n_1n and N be $\tilde{N}^3$. This gives us the following containment,

$$\alpha\Gamma(N)\alpha^{-1} \subseteq \alpha(I + N \cdot M_2(\mathbb{Z}))\alpha^{-1} = I + \tilde{N} \cdot \alpha \cdot \tilde{N} \cdot M_2(\mathbb{Z}) \cdot \tilde{N} \cdot \alpha^{-1}.$$

By the above expression, we have

$$\alpha\Gamma(N)\alpha^{-1} \cap SL_2(\mathbb{Z}) \subseteq \Gamma(\tilde{N}).$$

Rearranging the equation gives

$$\Gamma(N) \subseteq \alpha^{-1}\Gamma(\tilde{N})\alpha \cap SL_2(\mathbb{Z}) \subseteq \alpha^{-1}\Gamma(n)\alpha \cap SL_2(\mathbb{Z}) \subseteq \alpha^{-1}\Gamma\alpha \cap SL_2(\mathbb{Z}),$$

hence proving the lemma. □

Lemma 4.3. *Let* $\Gamma_3 = \alpha\Gamma_1\alpha^{-1} \cap \Gamma_2$. Γ_3 *is a subgroup of* Γ_2 *and it acts on* Γ_2 *by left multiplication. Let* l_α *denote left multiplication by* α*,*

$$l_\alpha : \Gamma_2 \to \Gamma_1\alpha\Gamma_2$$

$$\gamma_2 \longmapsto \alpha\gamma_2. \tag{4.4}$$

The left multiplication induces a bijection mapping from the orbit space of left multiplication by Γ_3 *on* Γ_2 *to the orbit space of the left multiplication by* Γ_1 *on* $\Gamma_1\alpha\Gamma_2$*.*

Proof of the lemma. Notice that all orbit space representatives are of the form $\gamma_1\alpha\gamma_2$ for some $\gamma_1 \in \Gamma_1$ and $\gamma_2 \in \Gamma_2$. Since Γ_1 acts on $\Gamma_1\alpha\Gamma_2$ by left multiplication, each orbit representative can be rewritten as $\alpha \cdot \beta_i$ for some $\beta_i \in \Gamma_2$. This shows that l_α is a surjection.

For proving the map is an injection, let $\gamma, \gamma' \in \Gamma_2$ be two orbit space representatives such that

$$\Gamma_1\alpha\gamma = \Gamma_1\alpha\gamma'.$$

This implies that

$$\alpha\gamma{\gamma'}^{-1} \in \Gamma_1\alpha.$$

Multiplying on the left with α^{-1} on both sides of the equations gives us

$$\gamma{\gamma'}^{-1} \in \alpha^{-1}\Gamma_1\alpha.$$

Since $\gamma, \gamma' \in \Gamma_2$, $\gamma{\gamma'}^{-1}$ is also contained in Γ_2. This implies that

$$\gamma{\gamma'}^{-1} \in \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2 = \Gamma_3.$$

Therefore,

$$\Gamma_3\gamma = \Gamma_3\gamma',$$

and the left multiplication by α induces a bijection on orbit spaces. □

By definition of left multiplication, all orbit spaces of the action by Γ_3 are right cosets of Γ_3 in Γ_2. Hence, the number of orbits is the same as $[\Gamma_2 : \Gamma_3]$. By Lemma 4.3, the fact that Γ_1 is a congruence subgroup implies that $\alpha\Gamma_1\alpha^{-1}$ is also a congruence subgroup. Since the index $[SL_2(\mathbb{Z}) : \Gamma(N)]$ is finite for any $n \in \mathbb{Z}$ ([1] P13) and there exists a $N \in \mathbb{Z}$ such that $\Gamma(N) \subseteq \Gamma_3$, $[SL_2(\mathbb{Z}) : \Gamma_3]$ is finite. This implies that $[\Gamma_2 : \Gamma_3]$ is also finite. By bijection of orbit spaces,

$$\Gamma_1\alpha\Gamma_2 = \bigcup \Gamma_1\beta_j$$

is a finite union. □

Because the double coset is a finite union of orbit spaces, we can define an action on modular forms.

Definition 4.5. Let Γ_1 and Γ_2 be congruence subgroups of $SL_2(\mathbb{Z})$ and α be an element in $GL_2^+(\mathbb{Q})$. The *weight–k* $\Gamma_1\alpha\Gamma_2$ *operator* takes functions $f \in \mathcal{M}_k(\Gamma_1)$ to

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\beta_j]_k \tag{4.6}$$

where $\{\beta_j\}$ are orbit representatives.

For any two orbit representatives β, β' of the same orbit, $\beta\beta'^{-1} \in \Gamma_1$. For $f \in \mathcal{M}_k(\Gamma_1)$, this implies that

$$f[\beta]_k = f[\beta\beta'^{-1}]_k[\beta']_k = f[\beta']_k.$$

The definition of the double coset operator is therefore well-defined.

4.2. $\langle d \rangle$ **and** T_p **operator.** For this section, we will first define two types of Hecke operators and then generalize the definitions. The operators we introduced are presumed to be on modular forms with respect to $\Gamma_1(N)$.

Definition 4.7. Let α be the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ and define

$$\langle d \rangle : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$$

by

$$\langle d \rangle f = f[\alpha]_k \text{ for any } \alpha = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N) \text{ with } \delta \equiv d \mod N.$$

This is the first type of Hecke operators, also known as a *diamond operator*. To prove that the diamond operator is well-defined, we will first show that $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$. By definition of $\Gamma_0(N)$, the map

$$\phi : \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto d \mod (N) \tag{4.8}$$

is well-defined and has $\Gamma_1(N)$ as the kernel. Hence, $\Gamma_1(N) \lhd \Gamma_0(N)$.

For α and α' with $\phi(\alpha) = \phi(\alpha')$, we have

$$\alpha' \in \Gamma_1(N)\alpha\Gamma_1(N).$$

Given $\Gamma_1(N) \lhd \Gamma_0(N)$ and equation above, $\Gamma_1(N)$ acts trivially on $\mathcal{M}_k(\Gamma_1(N))$. Thus $\langle d \rangle$ is well-defined. The second type of Hecke operator is denoted as T_p. It is defined as follows,

$$T_p : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$$

$$T_p f = f[\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)]_k$$

for p prime.

Recall that the weight-k double coset operator is defined to be the sum of weight-k operators of the right coset representatives of the double coset. (Definition 4.5) Therefore, by finding the right coset representatives of $\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)$, we can find an explicit representation of the T_p operator.

Proposition 4.9. *Let N be a positive integer, and let both Γ_1 and Γ_2 be equal to the congruence subgroup $\Gamma_1(N)$ (as in (2.3)), and let α be the matrix $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ where p is prime. The operator $T_p = [\Gamma_1 \alpha \Gamma_2]_k$ on $\mathcal{M}_k(\Gamma_1(N))$ is given by*

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f\left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}\right]_k & \text{if } p \mid N \\ \sum_{j=0}^{p-1} f\left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}\right]_k + f\left[\begin{pmatrix} m & n \\ N & p \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right]_k & \text{if } p \nmid N, \text{ and } mp - nN = 1. \end{cases}$$

Proof. By definition of T_p, it suffices to find the orbit representatives of $\Gamma_1(N)\alpha\Gamma_1(N)$ for α as defined by (4.15). By Lemma 4.3, the orbits of $\Gamma_1(N)\alpha\Gamma_1(N)$ correspond bijectively with right cosets of $\Gamma_3 = \alpha^{-1}\Gamma_1(N)\alpha \cap \Gamma_1(N)$ in $\Gamma_1(N)$. In particular, since l_α (defined in 4.4) denotes left multiplication with α, all orbit representatives of $\Gamma_1(N)\alpha\Gamma_1(N)$ are of the form $\alpha\beta_j$ with β_j are right coset representatives of Γ_3 in $\Gamma_1(N)$. Thus, it suffices to find the right coset representatives of Γ_3 in $\Gamma_1(N)$.

Let

$$\Gamma^0(N,p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} \star & 0 \\ \star & \star \end{pmatrix} \mod p \right\} \cap \Gamma_1(N).$$

We claim that

$$\Gamma_3 = \Gamma^0(N,p).$$

By computation, for $\alpha^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & p^{-1} \end{pmatrix}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_3$, we have

$$\alpha^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha = \begin{pmatrix} a & pb \\ p^{-1}c & d \end{pmatrix}. \tag{4.10}$$

In order for $\alpha^{-1}\gamma\alpha \in \Gamma_1(N)$, c must be divisible by p and

$$\begin{pmatrix} a & pb \\ p^{-1}c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix} \mod N.$$

In addition, by (4.10),

$$\begin{pmatrix} a & pb \\ p^{-1}c & d \end{pmatrix} \equiv \begin{pmatrix} \star & 0 \\ \star & \star \end{pmatrix} \mod p.$$

This implies $\Gamma \subseteq \Gamma^0(N,p)$.

For reverse containment, take $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma^0(N,p)$, in particular, let c' denotes the element $p \cdot c$ and b denotes the element $p \cdot k$, where $k \in \mathbb{Z}$ by definition of

$\Gamma^0(N,p)$. By computation,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p^{-1} \end{pmatrix} \begin{pmatrix} a & k \\ c' & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$$

where $\begin{pmatrix} a & k \\ c' & d \end{pmatrix} \in \Gamma_1(N)$. Thus, $\Gamma_3 = \Gamma^0(N,p)$. In fact, Γ_3 is just $\Gamma_1(N)$ with the additional requirement that $b \equiv 0 \mod p$.

Now let

$$\gamma_{2,j} = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \text{ for } 0 \le j < p.$$

We claim that $\gamma_{2,j}$ are right coset representatives of Γ_3 in $\Gamma_1(N)$. For

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N), \tag{4.11}$$

consider

$$\gamma\gamma_{2,j}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -j \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b-aj \\ c & d-cj \end{pmatrix}.$$

If $\gamma\gamma_{2,j} \in \Gamma_3$ for some $0 \le j < p$, we then must have

$$b \equiv aj \mod p.$$

This splits into 2 possible cases: $p \not| a$ and $p|a$. If $p \not| a$, then we are done by taking $j \equiv a^{-1}b \mod p$. If $p|a$, b has to be divisible by p by computation. However, this would contradict that $ad - bc = 1$, so a has to be indivisible by p. Instances of $\gamma \in \Gamma_1(N)$ with $p|a$ occurs if and only if $p \not| N$. This happens when the set $\{\gamma_{2,j} |\ 0 \le j < p\}$ fails to be the complete right coset representatives of Γ_3 in $\Gamma_1(N)$. In this case, let

$$\gamma_{2,\infty} = \begin{pmatrix} mp & n \\ N & 1 \end{pmatrix} \text{ where } mp - nN = 1.$$

For γ defined by (4.11) with $p|a$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -n \\ -N & mp \end{pmatrix} = \begin{pmatrix} a-Nb & bmp-na \\ c-dN & dmp-nc \end{pmatrix} \text{ with } bmp - na \equiv 0 \mod p \text{ as } p|a,$$

implies that $\gamma\gamma_{2,\infty}^{-1} \in \Gamma_3$.

We will now show that $\gamma_{2,\infty}$ and $\gamma_{2,j}$ for j between 0 and $p-1$ represent distinct right cosets. Let $0 \le j, j' < p$ be distinct and consider

$$\gamma_{2,j} \cdot \gamma_{2,j'} = \begin{pmatrix} 1 & j-j' \\ 0 & 1 \end{pmatrix}.$$

$\gamma_{2,j} \cdot \gamma_{2,j'}^{-1}$ is contained in Γ_3 if and only if $j - j' \equiv 0 \mod p$. This could only happen if $j \equiv j' \mod p$. Since $0 \le j, j' < p$, $\gamma_{2,j}$ and $\gamma_{2,j'}$ must represent distinct right cosets.

For

$$\gamma_{2,j} \cdot \gamma_{2,\infty}^{-1} = \begin{pmatrix} 1-Nj & jmp-n \\ -N & mp \end{pmatrix},$$

because $nN = 1 + mp$ and $p \not| n$ (as p is prime and $p \not| nN$), $\gamma_{2,j}\gamma_{2,\infty}^{-1} \notin \Gamma_3$. Therefore, $\gamma_{2,\infty}$ and $\gamma_{2,j}$ $(0 \le j < p)$ represent distinct right cosets.

This suggests that $\beta_j = \alpha\gamma_{2,j}$ represents distinct orbit representatives of $\Gamma_1(N)\alpha\Gamma_1(N)$. By computation,

$$\beta_j = \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \text{ for } 0 \leq j < p$$

and

$$\beta_\infty = \alpha\gamma_{2,\infty} = \begin{pmatrix} m & n \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

Since $\begin{pmatrix} m & n \\ N & p \end{pmatrix} \in \Gamma_1(N)$, it suffices to define $\beta_\infty = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. Therefore,

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f\left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}\right]_k & \text{if } p|N \\ \sum_{j=0}^{p-1} f\left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}\right]_k + f\left[\begin{pmatrix} m & n \\ N & p \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right]_k & \text{if } p \nmid N, \text{ and } mp - nN = 1. \end{cases}$$

□

The explicit representation of T_p allows us to prove result on how T_p operators affect the Fourier coefficients of a modular form.

Proposition 4.12. *Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a character and $\mathcal{M}_k(N,\chi)$ denote the set,*

$$\mathcal{M}_k(N,\chi) = \{f \in \mathcal{M}_k(\Gamma_1(N) : \langle d\rangle f = \chi(d)f \text{ for all } d \in (\mathbb{Z}/N\mathbb{Z})^\times\}.$$

If f is an element in $\mathcal{M}_k(N,\chi)$, then $T_p f$ is also contained in $\mathcal{M}_k(N,\chi)$. Furthermore, its Fourier expansion is

$$(T_p f)(\tau) = \sum_{n=0}^{\infty} a_{np}(f)q^n + \chi(p)p^{k-1}\sum_{n=0}^{\infty} a_n(f)q^{np}$$
$$= \sum_{n=0}^{\infty} \left(a_{np}(f) + \chi(p)p^{k-1}a_{n/p}(f)\right) q^n.$$

That is

$$a_n(T_p f) = a_{np}(f) + \chi(p)p^{k-1}a_{n/p}(f) \text{ for } f \in \mathcal{M}_k(N,\chi). \tag{4.13}$$

Proof. The proof of the proposition is on Page 171-172 of [1]. □

The result above allows us to prove that the Hecke operators commute.

Proposition 4.14. *Let d and e be elements in $(\mathbb{Z}/n\mathbb{Z})^*$, and let p, q be prime. Then*

(a) $\langle d\rangle T_p = T_p\langle d\rangle$
(b) $\langle d\rangle\langle e\rangle = \langle e\rangle\langle d\rangle$
(c) $T_pT_q = T_qT_p$

Proof. We will prove each part of the proposition separately. Let

$$\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \text{ for some prime } p. \tag{4.15}$$

(a) We will compute both side of the equation for $f \in \mathcal{M}_k(\Gamma_1(N))$. Let $\gamma = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N)$ with $\delta \equiv d \mod N$ and β_j be orbit representatives of the double coset $\Gamma_1(N)\alpha\Gamma_1(N)$. Because showing that $\langle d\rangle T_p f = T_p\langle d\rangle f$ is equivalently to showing that
$$\langle d\rangle T_p f = \sum f[\beta_j\gamma]_k = \sum f[\gamma\beta_j]_k = T_p\langle d\rangle f,$$
it suffices to show that
$$\bigcup \Gamma_1(N)\beta_j\gamma = \bigcup \Gamma_1(N)\gamma\beta_j.$$

For this, we will first check that $\gamma\alpha\gamma^{-1} \in \Gamma_1(N)\alpha\Gamma_1(N)$. By definition of the double coset, it suffices to check that
$$\gamma\alpha\gamma^{-1} \equiv \begin{pmatrix} 1 & \star \\ 0 & p \end{pmatrix} \mod N.$$
For $\gamma = \begin{pmatrix} a & b \\ Nk & \delta \end{pmatrix}$, $\gamma\alpha\gamma^{-1}$ is
$$\gamma\alpha\gamma^{-1} = \begin{pmatrix} a & b \\ Nk & \delta \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} \delta & -b \\ -Nk & a \end{pmatrix} = \begin{pmatrix} a\delta - pbNk & pab - ab \\ Nk\delta - Nkp\delta & a\delta p - Nkb \end{pmatrix}.$$
Taking the equation modulo N,
$$\gamma\alpha\gamma^{-1} \equiv \begin{pmatrix} a\delta - bNk & \star \\ 0 & p(a\delta - Nkb) \end{pmatrix} \mod N.$$
Since $a\delta - Nkb = \det\gamma = 1$,
$$\gamma\alpha\gamma^{-1} = \begin{pmatrix} 1 & \star \\ 0 & p \end{pmatrix} \in \Gamma_1(N)\alpha\Gamma_1(N).$$
Hence,
$$\begin{aligned}\Gamma_1(N)\alpha\Gamma_1(N) &= \Gamma_1(N)\gamma\alpha\gamma^{-1}\Gamma_1(N) = \gamma\Gamma_1(N)\alpha\Gamma_1(N)\gamma^{-1} \\ &= \gamma\bigcup\Gamma_1(N)\beta_j\gamma^{-1} = \bigcup\Gamma_1(N)\gamma\beta_j\gamma^{-1}.\end{aligned}$$
This gives us that
$$\bigcup \Gamma_1(N)\beta_j\gamma = \bigcup \Gamma_1(N)\gamma\beta_j.$$
Referring back to the definition of $\langle d\rangle$ and T_p, we have that
$$\langle d\rangle T_p f = \sum f[\beta_j\gamma]_k = \sum f[\gamma\beta_j]_k = T_p\langle d\rangle f.$$
Thus, the two operators commute.

(b) Let $\alpha = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix}$ such that $\delta \equiv d \mod N$ and $\beta = \begin{pmatrix} a' & b' \\ c' & \varepsilon \end{pmatrix}$ such that $\varepsilon \equiv e \mod N$. Thus,
$$\alpha\beta \equiv \begin{pmatrix} \star & \star \\ \star & de \end{pmatrix} \mod N.$$
On the other hand,
$$\beta\alpha \equiv \begin{pmatrix} \star & \star \\ \star & de \end{pmatrix}.$$
This gives us that
$$\langle d\rangle\langle e\rangle f = f[\beta\alpha]_k = \langle de\rangle f = f[\alpha\beta]_k = \langle e\rangle\langle d\rangle f.$$

(c) To prove that the T_p operators commute, we will apply Proposition 4.12 and follow the proof on [1] Page 173. By applying (4.13) twice, we have

$$a_n(T_p(T_qf)) = a_{np}(T_pf) + \chi(p)p^{k-1}a_{n/p}(T_pf)$$
$$= a_{npq}(f) + \chi(q)q^{k-1}a_{np/q}(f) + \chi(p)p^{k-1}(a_{nq/p}(f) + \chi(q)q^{k-1}a_{n/pq}(f))$$
$$= a_{npq}(f) + \chi(q)q^{k-1}a_{np/q}(f) + \chi(p)p^{k-1}a_{nq/p}(f) + \chi(pq)(pq)^{k-1}a_{n/pq}(f)$$

which is symmetric in p and q. Given all coefficients of the Fourier expansion of T_pT_q and T_qT_p are the same, the T_p operators commute.

□

The definitions of the two type of Hecke operators can be generalised for any $n \in \mathbb{Z}^+$. This gives us an algebra generated by Hecke operators. By Proposition 4.14, the algebra formed is commutative.

Definition 4.16. Let Γ be $\Gamma_1(N)$. Then,

$$\langle n \rangle = \begin{cases} \Gamma \begin{pmatrix} \star & \star \\ \star & n \end{pmatrix} \Gamma \text{ where } \begin{pmatrix} \star & \star \\ \star & n \end{pmatrix} \in \Gamma_0(N) & \text{if } \gcd(n, N) = 1 \\ \\ 0 & \text{if } \gcd(n, N) > 1 \end{cases}$$

and

$$T_n = \prod T_{p_i^{r_i}}, \text{ where } n = \prod p_i^{r_i}$$

with $T_1 = 1$ and T_{p^r} is defined inductively

$$T_{p^r} = T_pT_{p^{r-1}} - p^{k-1}\langle p \rangle T_{p^{r-2}}, \text{ for } r \geq 2.$$

The $\mathbb{C}$-algebra generated by all $\langle n \rangle$ and T_n operators for $n \in \mathbb{Z}^+$ is known as the *Hecke algebra over* $\mathbb{C}$.

4.3. **Petersson Inner Product and Adjoints of Hecke Operators.** In this section, we will focus on studying the space $\mathcal{S}_k(\Gamma_1(N))$. In particular, we will establish that $\mathcal{S}_k(\Gamma_1(N))$ is an inner product space and has an orthogonal basis of simultaneous eigenvectors.

4.3.1. *Petersson Inner Product.* Define the *hyperbolic measure* on the upper half plane as

$$d\mu(\tau) = \frac{dxdy}{y^2}, \text{ for } \tau = x + iy \in \mathbb{H}.$$

One can check that the measure is invariant under the automorphism group $GL_2^+(\mathbb{R})$ and in particular, $d\mu$ is $SL_2(\mathbb{Z})$-invariant. Recall that a fundamental domain of $\mathbb{H}^*$ under the action of $SL_2(\mathbb{Z})$ is

$$\mathbb{D}^* = \{\tau \in \mathbb{H} : |\mathrm{Re}(\tau)| \leq \frac{1}{2}, |\tau| \geq 1\} \cup \{\infty\}.$$

Let Γ be a congruence subgroup and $\{\alpha_j\}$ be the set of right coset representatives of $\{\pm I\}\Gamma$ in $SL_2(\mathbb{Z})$. Thus,

$$SL_2(\mathbb{Z}) = \bigcup_j \{\pm I\}\Gamma\alpha_j$$

and it is a disjoint union. For $\phi \in \mathcal{M}_k(\Gamma)$, because ϕ is Γ-invariant and $d\mu$ is $SL_2(\mathbb{Z})$-invariant,

$$\sum_j \int_{\mathbb{D}^*} \phi(\alpha_j(\tau))d\mu(\tau) = \int_{\cup\alpha_j(\mathbb{D}^*)} \phi(\tau)d\mu(\tau).$$

Since $\cup\alpha_j(\mathbb{D}^*)$ represents the modular curve $X(\Gamma)$ up to some boundary identifications, we denote that

$$\int_{X(\Gamma)} \phi(\tau)d\mu(\tau) = \int_{\cup\alpha_j(\mathbb{D}^*)} \phi(\tau)d\mu(\tau).$$

In particular, when $\phi = 1$,

$$\int_{X(\Gamma)} d\mu(\tau) = V_\Gamma.$$

The volume and index of a congruence subgroup are related by

$$V_\Gamma = [SL_2(\mathbb{Z}) : \{\pm I\}\Gamma]V_{SL_2(\mathbb{Z})}.$$

Definition 4.17. Let $\Gamma \subseteq SL_2(\mathbb{Z})$ be a congruence subgroup. The *Petersson inner product* is defined as

$$\langle \cdot, \cdot \rangle_\Gamma : \mathcal{S}_k(\Gamma) \times \mathcal{S}_k(\Gamma) \to \mathbb{C}$$
$$\langle f, g \rangle_\Gamma = \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(\tau)\overline{g(\tau)}(\mathrm{Im}(\tau))^k d\mu(\tau).$$

The proof for the definition is well-defined and convergent is on Page 183 of [1]. Furthermore, the product defined above is linear in f, conjugate linear in g, Hermitian-symmetric and positive definite.

4.3.2. *Adjoints of Hecke Algebra.* Recall that if V is an inner product space and T is a linear operator on V, then *the adjoint* $T^\dagger$ is the linear operator on V defined by the condition

$$\langle Tv, w \rangle = \langle v, T^\dagger w \rangle \text{ for all } v, w \in V.$$

The operator T is called *normal* when it commutes with its adjoint. We will continue working with the inner product space $\mathcal{S}_k(\Gamma_1(N))$ endowed with the Petersson inner product. For this section, we will refer all the proofs of lemmas, propositions and theorems mentioned to Section 5.5 of [1].

Let $\Gamma \subseteq SL_2(\mathbb{Z})$ be a congruence subgroup and $SL_2(\mathbb{Z}) = \cup_j \{\pm I\}\Gamma\alpha_j$. Consider $\alpha \in GL_2^+(\mathbb{Q})$, then the map $\tau \mapsto \alpha(\tau)$ induces a bijection from $\alpha^{-1}\Gamma\alpha\backslash\mathbb{H}^*$ to $X(\Gamma)$. We thus have that

Lemma 4.18. *Let $\Gamma \subseteq SL_2(\mathbb{Z})$ be a congruence subgroup, and $\alpha \in GL_2^+(\mathbb{Q})$.*

(a) If $\phi : \mathbb{H} \to \mathbb{C}$ is continuous, bounded and Γ-invariant, then

$$\int_{\alpha^{-1}\Gamma\alpha\backslash\mathbb{H}^*} \phi(\alpha(\tau))d\mu(\tau) = \int_{X(\Gamma)} \phi(\tau)d\mu(\tau)$$

(b) If $\alpha^{-1}\Gamma\alpha \subseteq SL_2(\mathbb{Z})$, then $V_{\alpha^{-1}\Gamma\alpha} = V_\Gamma$ and $[SL_2(\mathbb{Z}) : \alpha^{-1}\Gamma\alpha] = [SL_2(\mathbb{Z}) : \Gamma]$.

(c) There exist $\beta_1, \ldots, \beta_n \in GL_2^+(\mathbb{Q})$, where $n = [\Gamma : \alpha^{-1}\Gamma\alpha \cap \Gamma] = [\Gamma : \alpha\Gamma\alpha^{-1} \cap \Gamma]$, such that

$$\Gamma\alpha\Gamma = \bigcup \Gamma\beta_j = \bigcup \beta_j\Gamma.$$

Both unions are disjoint.

With this fact established, we could now know how to compute the adjoints.

Proposition 4.19. *Let $\Gamma \subseteq SL_2(\mathbb{Z})$ be a congruence subgroup, and $\alpha \in GL_2^+(\mathbb{Q})$. Set $\alpha' = \det(\alpha)\alpha^{-1}$. Then*

(a) If $\alpha^{-1}\Gamma\alpha \subseteq SL_2(\mathbb{Z})$, then for all $f \in \mathcal{S}_k(\Gamma)$ and $g \in \mathcal{S}_k(\alpha^{-1}\Gamma\alpha)$,

$$\langle f[\alpha]_k, g\rangle_{\alpha^{-1}\Gamma\alpha} = \langle f, g[\alpha']_k\rangle_\Gamma.$$

(b) For all $f, g \in \mathcal{S}_k(\Gamma)$,

$$\langle f[\Gamma\alpha\Gamma]_k, g\rangle = \langle f, g[\Gamma\alpha'\Gamma]_k\rangle.$$

In particular, if $\alpha^{-1}\Gamma\alpha = \Gamma$, then $[\alpha]_k^\dagger = [\alpha']_k$, and in any case $[\Gamma\alpha\Gamma]_k^\dagger = [\Gamma\alpha'\Gamma]_k$.

Following the proposition above, we could deduce that

Theorem 4.20. *In the inner product space $\mathcal{S}_k(\Gamma_1(N))$, the Hecke operators $\langle p\rangle$ and T_p for $p \nmid N$ have adjoints*

$$\langle p\rangle^\dagger = \langle p\rangle^{-1} \text{ and } T_p^\dagger = \langle p\rangle^{-1}T_p.$$

Thus, for n and N are relatively prime, the Hecke operators $\langle n\rangle$ and T_n are normal.

From the Spectral Theorem of linear algebra, since $\mathcal{S}_k(\Gamma_1(N))$ is a finite-dimensional inner product space with a commuting family of normal operators, it has an orthogonal basis of simultaneous eigenvectors for the operators. We refer these eigenvectors as *eigenforms*. Therefore,

Theorem 4.21. *The space $\mathcal{S}_k(\Gamma_1(N))$ has an orthogonal basis of simultaneous eigenforms for the Hecke operators $\{\langle n\rangle, T_n : (n, N) = 1\}$.*

5. Another Interpretation of Hecke Algebra

We will now shift away from the theory of modular forms. In the greater theory of the Langlands program, we view modular forms as automorphic forms. Under the scenario of the Langlands program, modular forms generate sub-representations of the space $L^2(G)$. There is also an analogous theory of Hecke operators in this context. The Hecke algebra is commutative like in the classical setting. Analogous to how the Hecke operators act on the modular forms and decompose spaces of modular forms into eigenspaces, here we look at how the Hecke ring acts on representations and how the representations break down into irreducible sub-representations. In particular, because of Schur's lemma, elements in the Hecke ring act as scalars on the irreducible representations. Thus we have the following correspondence where the eigenforms correspond to the irreducible sub-representations and the eigenvalues correspond to the scalars (as determined by Schur's lemma) the ring acts by. The material of the rest of the paper is primarily based on the paper [2].

For this section, we will ignore the general case but focus primarily on explaining the theory for the case of $GL_2(\mathbb{Q}_p)$ (we will denote as GL_2 for $GL_2(\mathbb{Q}_p)$ for the rest of the section unless specified otherwise). Its maximal torus is T, the set of invertible diagonal matrices over $\mathbb{Q}_p$, and is contained in the Borel subgroup, B, the set of invertible upper triangular matrices over $\mathbb{Q}_p$. The Weyl group of T is S_2, which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

The characters and co-characters for the maximal torus is defined by

$$X^\bullet = X^\bullet(\underline{T}) = \operatorname{Hom}(\underline{T}, \mathbb{G}_m)$$

$$X_\bullet = X_\bullet(\underline{T}) = \mathrm{Hom}(\mathbb{G}_m, \underline{T}).$$

All characters in $X^\bullet$ are generated by the characters $\varepsilon_i : \underline{T} \to \mathbb{G}_m$ with $\varepsilon_i(g) = t_i$ (t_i is the i-th diagonal entry of the matrix g). All co-characters in $X_\bullet$ are generated by the co-character $e_i : \mathbb{G}_m \to \underline{T}$ with $e_i(a) = A_i$ (A_i is the diagonal matrix with a at ii-th entry and the rest of the diagonal entries are 1). Thus, $X^\bullet$ is a $\mathbb{Z}$-module generated by $\varepsilon_1, \varepsilon_2$ and $X_\bullet$ is a $\mathbb{Z}$-module generated by e_1, e_2.

For $\chi \in X^\bullet$ and $\gamma \in X_\bullet$, $\chi \circ \gamma \in \mathrm{End}(\mathbb{G}_m) = \mathbb{Z}$ (proof is on page 15-16 of [4]). For $a \in \mathbb{G}_m$, there exists an integer $\langle \gamma, \chi \rangle$ with $\chi \circ \gamma(a) = a^{\langle \gamma, \chi \rangle}$. In particular, for ε_i and e_j, $\langle \varepsilon_i, e_j \rangle = \delta_{ij}$.

The roots are $\varepsilon_1 - \varepsilon_2$ and $\varepsilon_2 - \varepsilon_2$ with $\varepsilon_1 - \varepsilon_2$ being the positive root (due to our choice of the Borel subgroup). The set of roots is denoted as Φ with Φ^+ denotes the set of positive roots. The positive Weyl chamber P^+ in $X_\bullet(\underline{T})$ is

$$P^+ = \{\lambda \in X_\bullet : \langle \lambda, \alpha \rangle \geq 0, \forall \alpha \in \Phi^+\}.$$

Given $\varepsilon_1 - \varepsilon_2$ is the only positive root,

$$P^+ = \{\lambda \in X_\bullet : \langle \lambda, \varepsilon_1 - \varepsilon_2 \rangle \geq 0\}.$$

For all $\lambda \in X_\bullet$, $\lambda = k_1 e_1 + k_2 e_2$ for some $k_1, k_2 \in \mathbb{Z}$. Because $\langle \lambda, \varepsilon_1 - \varepsilon_2 \rangle$ is defined by the exponent of $(\varepsilon_1 - \varepsilon_2)(\lambda(t))$ for $t \in \mathbb{G}_m$ and

$$(\varepsilon_1 - \varepsilon_2)(k_1 e_1 + k_2 e_2)((t)) = (\varepsilon_1 - \varepsilon_2)) \begin{pmatrix} t^{k_1} & 0 \\ 0 & t^{k_2} \end{pmatrix} = t^{k_1 - k_2},$$

$\langle \lambda, \varepsilon_1 - \varepsilon_2 \rangle \geq 0$ is equivalent to $k_1 - k_2 \geq 0$. This suggests that

$$P^+ = \{k_1 e_1 + k_2 e_2 \in X_\bullet : k_1 - k_2 \geq 0\}.$$

There is a partial ordering on P^+: $\lambda \geq \mu$ if $\lambda - \mu$ can be written as sum of positive co-roots. In particular, for $\rho = \frac{1}{2}(\varepsilon_1 - \varepsilon_2)$, $\lambda \geq \mu$ implies that $\langle \lambda - \mu, \rho \rangle \geq 0$ and is an integer.

5.1. **Hecke Ring.**

Let G denote the group $GL_2(\mathbb{Q}_p)$ and K denote $GL_2(\mathbb{Z}_p)$.

Definition 5.1. The *Hecke ring* $\mathcal{H} = \mathcal{H}(G, K)$ is defined as the ring of all smooth, compactly supported functions $f : G \to \mathbb{C}$ which are K-bi-invariant, i.e. $f(kx) = f(xk') = f(x)$ for all $k, k' \in K$ and $x \in G$. This is also denoted as $C_c^\infty(K \backslash G / K)$.

The multiplication in $\mathcal{H}$ is defined by convolution

$$(f \cdot g)(z) = \int_G f(x) \cdot g(x^{-1} z) dx$$

where dx is the unique Haar measure on G giving K volume 1 and the unit element of $\mathcal{H}$ is the characteristic function of K.

Smooth functions on $\mathbb{Q}_p$ are locally constant. Given functions in the Hecke ring are also compactly supported and K-bi-invariant, they are finite sums of characteristic functions of double cosets KxK. Thus, the characteristic functions $\mathbb{1}_{KxK}$ form a $\mathbb{C}$-basis of $\mathcal{H}$.

Denote π as the unformizer of $\mathbb{Q}_p$, i.e. $\pi = p$. For any $\lambda \in X_\bullet(\underline{T})$, $\lambda(\pi)$ is in T. Since $\lambda(\mathbb{Z}_p^*) \subseteq K$, the double coset $K\lambda(\pi)K$ is independent of the choice of the uniformizer. Furthermore, from [6] P51, which we will state without proof,

Proposition 5.2. *The group G is the disjoint union of the double cosets $K\lambda(\pi)K$, where λ runs through the cocharacters in P^+ [2].*

It follows that the elements

$$c_\lambda = \mathbb{1}_{K\lambda(\pi)K} : G \to \mathbb{C}$$

$$g \mapsto \begin{cases} 1 & \text{if } g \in KxK \\ 0 & \text{otherwise} \end{cases}$$

form a $\mathbb{C}$-basis of $\mathcal{H}$ and multiplication is determined by the products

$$c_\lambda \cdot c_\mu = \sum n_{\lambda,\mu}(\nu) \cdot c_\nu, \ \text{ with } n_{\lambda,\mu}(\nu(\pi)) \in \mathbb{C}. \tag{5.3}$$

From the proposition, GL_2 is the disjoint union of the double cosets $GL_2(\mathbb{Z}_p)\lambda(\pi)GL_2(\mathbb{Z}_p)$, where $\lambda = ae_1 + be_2$ has $a - b \geq 0$, i.e.,

$$GL_2 = \coprod_{a \geq b} GL_2(\mathbb{Z}_p) \begin{pmatrix} p^a & 0 \\ 0 & p^b \end{pmatrix} GL_2(\mathbb{Z}_p). \tag{5.4}$$

We are particularly interested in the following two double cosets

$$K \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K \text{ and } K \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} K.$$

Define

$$T_p = \mathbb{1}_{K\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}K} \text{ and } R_p = \mathbb{1}_{K\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}K}.$$

Notice that the T_p here is similar to that of the T_p operator in the theory of modular forms.

We will now find an explicit formula for $n_{\lambda,\mu}(\nu(\pi))$. Similar to the computation for finding the explicit formula for T_p operators in the theory of modular forms, we will consider the action of right multiplication on the double cosets. The double cosets are then written in terms of left coset representatives where

$$K\lambda(\pi)K = \coprod x_i K$$

and

$$K\mu(\pi)K = \coprod y_j K.$$

Thus, we have the following result

Proposition 5.5.

$$n_{\lambda,\mu}(\nu(\pi)) = |\{(i,j) : \nu(\pi) \in x_i y_j K\}|.$$

Proof. Let $t = \nu(\pi)$. By the definition of characteristic function and (5.3), it suffices to compute $c_\lambda \cdot c_\mu$ at the left coset $K\nu(\pi)K$ for calculating $n_{\lambda,\mu}(\nu)$,. Thus,

$$n_{\lambda,\mu}(\nu(\pi)) = (c_\lambda \cdot c_\mu)(\nu(\pi)) = \int_G c_\lambda(x) c_\mu(x^{-1}t)dx.$$

Since $c_\lambda(x) = 1$ if and only if $x \in K\lambda(\pi)K$,

$$n_{\lambda,\mu}(\nu(\pi)) = \int_{K\lambda(\pi)K} c_\mu(x^{-1}t)dx.$$

Because $K\lambda(\pi)K = \coprod x_i K$, the equation can be rewritten as

$$n_{\lambda,\mu}(\nu) = \sum_{x_i} \int_{x_i K} c_\mu((k \cdot x_i)^{-1} t) dx.$$

By c_μ is K-bi-invariant,

$$\begin{aligned} n_{\lambda,\mu}(\nu) &= \sum_{x_i} \int_K c_\mu({x_i}^{-1} t) dx \\ &= \sum_i \mathrm{vol}(K) \cdot c_\mu({x_i}^{-1} t). \end{aligned}$$

Given c_μ is a characteristic function, $c_\mu({x_i}^{-1}t) \neq 0$ if and only if ${x_i}^{-1}t \in K\mu(\pi)K$. This is then equivalent to ${x_i}^{-1}t \in \bigcup y_j K$, which is also equivalent to $t \in \bigcup x_i y_j K$. Thus,

$$n_{\lambda,\mu}(\nu(\pi)) = \sum_i \mathrm{vol}(K) \cdot c_\mu({x_i}^{-1} t) = |\{(i,j) : \nu(\pi) \in x_i y_j K\}|.$$

$\square$

By proposition,

$$n_{\lambda,\mu}(\lambda + \mu)(\pi) = |\{(i,j) : (\lambda + \mu)(\pi) \in x_i y_j K\}|.$$

and $(\lambda + \mu)(\pi) \in \lambda(\pi)\mu(\pi)K$. This implies that

$$n_{\lambda,\mu}(\lambda + \mu)(\pi) \geq 1.$$

In fact, $n_{\lambda,\mu}(\lambda + \mu) = 1$ and $n_{\lambda,\mu}(\nu) \neq 0$ implies that $\nu \leq (\lambda + \mu)$. Thus,

$$c_\lambda \cdot c_\mu = c_{\lambda+\mu} + \sum_{\nu < (\lambda+\mu)} n_{\lambda,\mu}(\nu) \cdot c_\nu. \tag{5.6}$$

Following Proposition 5.2, we will find a set of left coset representatives for the double coset $K \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K$. Then, we will compute $c_{e_1} \cdot c_{e_1}$. Similar to Lemma 4.3 and the proof of Proposition 4.9, consider the right multiplication action by K on $K \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K$ and the right multiplication action by $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}^{-1} \cap K$ on K. Analogous to Lemma 4.3, define

$$\begin{aligned} \rho : K &\to K \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K \\ k &\longmapsto k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

The map also induces a bijection between the orbit space of $K \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K$ and the left cosets of $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}^{-1} \cap K$ in K. (The proof is almost exactly the same as the proof for Lemma 4.3). Similar to the proof of Proposition 4.9, for

$$H = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}^{-1} \cap K,$$

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} \star & 0 \\ \star & \star \end{pmatrix} \mod p \right\}.$$

Thus, consider the elements

$$\mu_{2,j} = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \text{ for } 0 \le j < p$$

and

$$\mu_{2,\infty} = \begin{pmatrix} 1 & p-1 \\ 1 & p \end{pmatrix}.$$

They represent distinct cosets and form a complete set of left coset representatives of H. Since ρ is a bijection on the cosets, the orbit representatives are

$$\beta_j = \mu_{2,j} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \text{ for } 0 \le j < p,$$

which is

$$\beta_j = \begin{pmatrix} p & j \\ 0 & 1 \end{pmatrix} \text{ for } 0 \le j < p.$$

Given

$$\mu_{2,\infty} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} p & p-1 \\ 1 & 1 \end{pmatrix}$$

and $\begin{pmatrix} p & p-1 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}_p)$, define

$$\beta_\infty = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}.$$

Therefore,

$$K \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K = \coprod_{k=0}^{p-1} \begin{pmatrix} p & j \\ 0 & 1 \end{pmatrix} K \coprod \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} K. \tag{5.7}$$

We will now compute $c_{e_1} \cdot c_{e_1}$. By Proposition 5.5, for $\nu = k_1 e_1 + k_2 e_2$ with $a \ge b$,

$$n_{e_1,e_1} = c_{e_1} \cdot c_{e_1}(\nu(p)) = |\{(i,j) : \nu(p) \in \beta_i \beta_j K\}|$$

for β_j defined above. We will now look at each $\beta_i \beta_j K$ and check whether $\nu(p) = \begin{pmatrix} p^{k_1} & 0 \\ 0 & p^{k_2} \end{pmatrix} \in \beta_i \beta_j K$.

For both β_i, β_j with indices between 0 and $p-1$,

$$\begin{pmatrix} p & i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & j \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} p^2 a & p^2 b + d(i + pj) \\ c & d \end{pmatrix}$$

If $\nu(p) = \begin{pmatrix} p^{k_1} & 0 \\ 0 & p^{k_2} \end{pmatrix} \in \beta_i \beta_j K$, then the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ must has $c = 0$ and $d = 1$. Furthermore, since $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_p)$, the determinant of the matrix must be in $\mathbb{Z}_p^\times$. Given $c = 0$ and $d = 1$, a must be 1. In order for $\nu(p) \in \beta_i \beta_j K$, $\nu(p)$ must satisfy

$$\nu(p) = \begin{pmatrix} p^2 & 0 \\ 0 & 1 \end{pmatrix}.$$

Because $p^2 b + pj + i = 0$ has integer solutions only if $p|i$ (i has to be $-p(pb + j)$), $\begin{pmatrix} p^2 & 0 \\ 0 & 1 \end{pmatrix}$ is contained in $\beta_i \beta_j K$ only if $i = j = 0$.

Now consider $\beta_j = \beta_\infty$ and β_i with index between 0 and $p-1$. Thus,

$$\begin{pmatrix} p & i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} p(a+ic) & p(b+id) \\ pc & pd \end{pmatrix}.$$

Again given $\nu(p) = \begin{pmatrix} p^{k_1} & 0 \\ 0 & p^{k_2} \end{pmatrix}$, c has to be 0 and $a = d = 1$. Since for all i between 0 and $p-1$, there is an integer solution to $b+i=0$. Therefore, for all i between 0 and $p-1$, $\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \in \beta_i \beta_\infty K$.

Now consider $\beta_i = \beta_\infty$ and β_j with index between 0 and $p-1$. In order for $\nu(p) \in \beta_\infty \beta_j K$, the computation

$$\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} p & j \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} pa+cj & pb+dj \\ pc & pd \end{pmatrix} = \begin{pmatrix} p^{k_1} & 0 \\ 0 & p^{k_2} \end{pmatrix}$$

must imply that $c = 0$ and $a = d = 1$. Furthermore, for $0 \le j < p$ to be an integer solution of $pb + j = 0$, p must divides j. Therefore, j has to be 0.

For $\beta_i = \beta_j = \beta_\infty$, we have that

$$\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ p^2 c & p^2 d \end{pmatrix}.$$

By $\nu \in P^+$, $\nu(p)$ can not be contained in $\beta_\infty \beta_\infty K$.

Given $c_{e_1} = T_p$ and $c_{e_2} = R_p$,

$$T_p \cdot T_p = T_{p^2} + (p+1) \cdot R_p.$$

Compare to the formula of T_p^2 in the theory of modular forms

$$T_p \cdot T_p = T_{p^2} - p^{k-1} \langle p \rangle$$

for T_p operator on $\mathcal{M}_k(\Gamma_1(N)$, we see a similarity between the two formulas. Moreover, similar to the Hecke algebra in the theory of modular form,

Proposition 5.8. *The Hecke ring $\mathcal{H}$ is commutative.*

There are two ways to prove the proposition. One method of proving the commutativity is through applying Gelfand's lemma [3], which suggests that if there exists an anti-involution of G that stabilizes K and acts trivially on the double coset space $K \setminus G/K$, then the Hecke algebra is commutative and (G, K) is a Gelfand pair. Consider the map

$$\iota : GL_2 \mapsto GL_2$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^t.$$

One can check by direct computation that $\iota^2 = \mathrm{id}$, $\iota(gh) = \iota(h)\iota(g)$ for $g, h \in GL_2$, and $GL_2(\mathbb{Z}_p)$ is stable under ι. Furthermore, by (5.4), all double cosets are of the form $GL_2(\mathbb{Z}_p) \begin{pmatrix} p^a & 0 \\ 0 & p^b \end{pmatrix} GL_2(\mathbb{Z}_p)$ with $a \ge b$. By definition of transposition, ι clearly acts trivially on the double coset space. Therefore, ι is an anti-involution satisfying the condition of Gelfand's lemma. This implies that the Hecke ring $\mathcal{H}(GL_2, GL_2(\mathbb{Z}_p))$ is commutative.

Another method of proving the commutativity is through applying the Satake transform which injects $\mathcal{H}$ into the commutative ring $\mathbb{C}[e_1, e_2]^{S_2}$ (the set of homogeneous polynomials in 2 variables over $\mathbb{C}$). We will discuss about the Satake transform in the next section.

5.1.1. *Hecke Ring of the Torus.* Before we discuss about the Satake transform, we will investigate further in propoerties of the Hecke ring for the torus. Denote the Hecke ring for T the torus as $\mathcal{H}_T$. Since the set of invertible diagonal 2-by-2 matrices over $\mathbb{Q}_p$ (also denote as T) is the torus of GL_2, $\mathcal{H}_T$ is commutative. Furthermore, we have the following exact sequence

(5.9)
$$0 \longrightarrow \begin{pmatrix} \mathbb{Z}_p^\times & 0 \\ 0 & \mathbb{Z}_p^\times \end{pmatrix} \longrightarrow \begin{pmatrix} \mathbb{Q}_p^\times & 0 \\ 0 & \mathbb{Q}_p^\times \end{pmatrix} \xrightarrow{\gamma} X_\bullet\left(\begin{pmatrix} \mathbb{Q}_p^\times & 0 \\ 0 & \mathbb{Q}_p^\times \end{pmatrix}\right) \longrightarrow 0$$

with $\gamma(t)$ a co-character satisfying

$$\langle \gamma(t), \chi \rangle = \operatorname{ord}(\chi(t))$$

for all characters $\chi \in X^\bullet(\underline{T})$. In fact, we can find an explicit formula for γ. Let t be the matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in T$ with $ab = 1$. Given $\operatorname{ord}(\chi(t)) = \langle \gamma(t), \chi \rangle$ is defined as the exponent of $(\chi\gamma(t))(g)$ for $g \in \mathbb{G}_m$, we will define $\gamma(t)$ as follow,

$$\gamma(t) : \mathbb{G}_m \to \underline{T}$$
$$g \longmapsto \begin{pmatrix} g^{v_p(a)} & 0 \\ 0 & g^{v_p(b)} \end{pmatrix}.$$

Because $X^\bullet(\underline{T}) = \mathbb{Z}[\varepsilon_1, \varepsilon_2]$, for any $\chi \in X^\bullet$, for $\chi = c\varepsilon_1 + d\varepsilon_2$,

$$\chi(t) = a^c \cdot b^d.$$

This implies that

$$\operatorname{ord}(\chi(t)) = v_p(a^c \cdot b^d) = cv_p(a) + dv_p(b).$$

On the other hand,

$$(\chi(\gamma(t)))(g) = \chi\left(\begin{pmatrix} g^{v_p(a)} & 0 \\ 0 & g^{v_p(b)} \end{pmatrix}\right) = g^{c \cdot v_p(a) + d \cdot v_p(b)}$$

implies that

$$\langle \gamma(t), \chi \rangle = c \cdot v_p(a) + d \cdot v_p(b).$$

Since

$$\operatorname{ord}(\chi(t)) = c \cdot v_p(a) + d \cdot v_p(b),$$

for $t \in D_2$, $\gamma(t)$ defined above satisfies the condition

$$\langle \gamma(t), \chi \rangle = \operatorname{ord}(\chi(t)).$$

Furthermore, because $v_p : \mathbb{Q}_p \mapsto \mathbb{Z}$ is a surjection, γ is a surjection. Because all elements in $\mathbb{Z}_p^\times$ has valuation zero, the sequence 5.9 with γ defined above forms an exact sequence as we wanted.

We could actually deduce more about the exact sequence 5.9. It in fact has a splitting,

$$\begin{tikzcd} 0 \arrow[r] & \underline{T}(\mathbb{Z}_p) \arrow[r] & \underline{T} \arrow[r, "\gamma"'] & X_\bullet(\underline{T}) \arrow[l, bend right, "\lambda"'] \arrow[r] & 0 \end{tikzcd} \tag{5.10}$$

where

$$\lambda : X_\bullet \to D_2$$

is defined by

$$\mu \longmapsto \mu(p).$$

Take $\mu = k_1e_1 + k_2e_2 \in X_\bullet(\underline{T})$,

$$\gamma(\lambda(\mu)) = \gamma\left(\begin{pmatrix} p^{k_1} & 0 \\ 0 & p^{k_2} \end{pmatrix}\right) : \mathbb{G}_m \to \underline{T}$$

$$g \longmapsto \begin{pmatrix} g^{k_1} & 0 \\ 0 & g^{k_2} \end{pmatrix}$$

implies that $\gamma(\lambda(\mu)) = k_1e_1 + k_2e_2 = \mu$. Hence, $\gamma\lambda = \mathrm{id}_{X_\bullet(\underline{T})}$ and the exact sequence 5.10 splits.

For G (in the definition of the Hecke ring) is T and K is $T(\mathbb{Z}_p)$ (the set of invertible diagonal 2-by-2 matrices onver $\mathbb{Z}_p$), because T is commutative, the double cosets $T(\mathbb{Z}_p)xT(\mathbb{Z}_p)$ are single cosets $xT(\mathbb{Z}_p)$. Thus, in $\mathcal{H}_T$,

$$c_\lambda \cdot c_\mu = c_{\lambda+\mu}. \tag{5.11}$$

By (5.11), the splitting of the exact sequence 5.10 and definition of the Hecke ring, we have an isomorphism of rings

$$\mathcal{H}_T \cong \mathbb{C}[X_\bullet(\underline{T})].$$

$$c_\lambda \leftrightarrow [\lambda].$$

This isomorphism is important when we discuss about the Satake transform.

5.2. **Satake Isomorphism.** Let N denote the set of unipotent matrix in GL_2, i.e.

$$N = \begin{pmatrix} 1 & \mathbb{Q}_p^\times \\ 0 & 1 \end{pmatrix}.$$

In particular, $T \subseteq B = T \cdot N \subset GL_2$. Let dn be the unique Haar measure on N which gives $\mathrm{vol}(N(\mathbb{Z}_p)) = 1$. Let

$$\delta : B \to \mathbb{R}_+^*$$

be the modular function on B, defined by the formula

$$d(bnb^{-1}) = \delta(b)dn.$$

By computation, for $m = bnb^{-1}$,

$$\int_N \mathbb{1}_N \ d(bnb^{-1}) = \int_N b^{-1}mb \ \mathbb{1}_N \ dm = \int_{b^{-1}Nb} \mathbb{1}_N \ dm = \mathrm{vol}(b^{-1}Nb) = \frac{\mathrm{vol}(N)}{[N : b^{-1}Nb]}.$$

This implies that

$$\delta(b) = \frac{1}{[N : b^{-1}Nb]}. \tag{5.12}$$

By (5.12), δ is trivial on N. Thus, we can define a character $\delta : T \to \mathbb{R}_+^*$ based on the definition of δ as the modular function on B. In particular, if $t = \mu(p)$ for $\mu \in X_\bullet(\underline{T})$,

$$\delta(t)^{\frac{1}{2}} = |\det(\mathrm{ad}t|\mathrm{Lie}(N))|_p{}^{\frac{1}{2}}. \tag{5.13}$$

From [2] (2.4), we have that

$$\det(\mathrm{ad}t|\mathrm{Lie}(N)) = 2\rho(t).$$

Substituting equation above into (5.13) gives us that

$$\begin{aligned} \delta(t)^{\frac{1}{2}} &= |p^{\langle \mu, 2\rho \rangle}|_p{}^{\frac{1}{2}} \\ &= p^{-\langle \mu, \rho \rangle} \in \mathbb{C}. \end{aligned}$$

Now we can define the Satake transform,

$$\mathcal{S} : \mathcal{H}_G \to \mathcal{H}_T$$
$$f \longmapsto \mathcal{S}f$$

where

$$\mathcal{S}f(t) = \delta(t)^{\frac{1}{2}} \cdot \int_N f(tn)dn.$$

The important result about the Satake transform is that the image of the Hecke ring $\mathcal{H}(GL_2, GL_2(\mathbb{Z}_p))$ lies in the subring

$${\mathcal{H}_T}^{S_2} = R(GL_2(\mathbb{C})) \otimes \mathbb{C}.$$

Given

$$R(GL_2(\mathbb{C})) = \mathbb{Z}[X_{\bullet}(\underline{T})] = \mathbb{Z}[e_1, e_2],$$

we have that

Proposition 5.14. *The Satake transform gives a ring isomorphism*

$$\mathcal{S} : \mathcal{H}_G \to \mathbb{C}[e_1, e_2]^{S_2}.$$

5.2.1. *Sample Computation for $\mathcal{S}(T_p)$.* We will now give a sample calculation using the Satake transform. In particular, we will compute what $\mathcal{S}(T_p)$ is on $t = \mu(p)$ for $\mu \in P^+$, i.e.

$$t = \begin{pmatrix} p^a & 0 \\ 0 & p^b \end{pmatrix}$$

with $a \geq b$. Applying the definition of the Satake transform gives us that

$$\mathcal{S}(T_p)(t) = p^{-\langle \mu, \rho \rangle} \cdot \int_N T_p(tn)dn.$$

Recall that we have a decomposition of the following double coset into right cosets from (5.7),

$$K \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K = \coprod_{k=0}^{p-1} \begin{pmatrix} p & j \\ 0 & 1 \end{pmatrix} K \coprod \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} K.$$

Thus,

$$\mathcal{S}(T_p)(t) = p^{-\langle \mu, \rho \rangle} \left(\sum_{i=0}^{p-1} \int_{N \cap t^{-1} \begin{pmatrix} p & j \\ 0 & 1 \end{pmatrix} K} 1dn + \int_{N \cap t^{-1} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} K} 1dn \right).$$

Let $x_i = \begin{pmatrix} p & i \\ 0 & 1 \end{pmatrix}$ for i between 0 and $p-1$ and x' be $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. Notice that the statement

$$N \cap t^{-1} x_i K \neq \varnothing \text{ or } N \cap t^{-1} x' K \neq \varnothing$$

is equivalent to

$$x_i^{-1} tN \cap K \neq \varnothing \text{ or } x'^{-1} tN \cap K \neq \varnothing. \tag{5.15}$$

Given x_i and x' are in $B = TN$, we could write $x_i = t(x_i)n(x_i)$ and $x' = t(x')n(x')$ for $t(x_i), t(x') \in T$ and $n(x_i), n(x') \in N$. Furthermore, given B normalizes N, (5.15) can be rewritten as

$$n(x_i)^{-1} N t(x_i)^{-1} t \cap K \neq \varnothing \text{ or } n(x')^{-1} N t(x')^{-1} t \cap K \neq \varnothing.$$

Given $n(x_i), n(x') \in N$, statement above is simplified as

$$Nt(x_i)^{-1}t \cap K \neq \varnothing \text{ or } Nt(x')^{-1}t \cap K \neq \varnothing.$$

This implies that in order for the intersection to be non-empty, $t^{-1}t(x_i) \in T(\mathbb{Z}_p)$ or $t^{-1}t(x') \in T(\mathbb{Z}_p)$. For $t^{-1}t(x_i) \in T(\mathbb{Z}_p)$ or $t^{-1}t(x') \in T(\mathbb{Z}_p)$, the intersection is equal to $N \cap K$. Thus, for $t^{-1}t(x_i) \in T(\mathbb{Z}_p)$,

$$\int_{N\cap t^{-1}\begin{pmatrix} p & j \\ 0 & 1\end{pmatrix} K} 1dn = \int_{N\cap K} 1dn = 1.$$

Therefore,

$$\mathcal{S}(T_p)(t) = p^{-\langle \mu,\rho\rangle}|\{x_i \text{ or } x' : t^{-1}t(x_i) \text{ or } t^{-1}t(x') \in T(\mathbb{Z}_p)\}|.$$

By computation, for all $0 \leq i < p$, $t(x_i) = \begin{pmatrix} p & 0 \\ 0 & 1\end{pmatrix}$ and $t(x') = \begin{pmatrix} 1 & 0 \\ 0 & p\end{pmatrix}$. For $\mu \in P^+$ and $t = \mu(p) = \begin{pmatrix} p^a & 0 \\ 0 & p^b\end{pmatrix}$ with $a \geq b$, in order for $t^{-1}t(x_i)$ to be contained in $T(\mathbb{Z}_p)$,

$$\begin{pmatrix} p^{-a} & 0 \\ 0 & p^{-b}\end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1\end{pmatrix} = \begin{pmatrix} p^{1-a} & 0 \\ 0 & p^{-b}\end{pmatrix}$$

must satisfy $1-a = 0$ and $-b = 0$. On the other hand, in order for $t^{-1}t(x') \in T(\mathbb{Z}_p)$,

$$\begin{pmatrix} p^{-a} & 0 \\ 0 & p^{-b}\end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & p\end{pmatrix} = \begin{pmatrix} p^{-a} & 0 \\ 0 & p^{1-b}\end{pmatrix}$$

must satisfy $-a = 0$ and $1-b = 0$. Therefore, for all $t = \mu(p)$ with $\mu \in P^+$, if $\mu \neq e_1$ or e_2, then $\mathcal{S}(T_p)(t) = 0$; otherwise, for $t = e_1(p) = \begin{pmatrix} p & 0 \\ 0 & 1\end{pmatrix}$, $t^{-1}t(x_i) = I \in T(\mathbb{Z}_p)$ but $t^{-1}t(x') \notin T(\mathbb{Z}_p)$. Given $\langle e_1, \rho\rangle = \frac{1}{2}$, computation gives us that

$$\mathcal{S}(T_p)(e_1(p)) = p^{-\frac{1}{2}} \cdot p = p^{\frac{1}{2}}.$$

On the other hand, for $t = e_2(p) = \begin{pmatrix} 1 & 0 \\ 0 & p\end{pmatrix}$, since only $t^{-1}t(x')$ is contained in $T(\mathbb{Z}_p)$ and $\langle e_2, \rho\rangle = -1/2$,

$$\mathcal{S}(T_p)(e_2(p)) = p^{\frac{1}{2}} \cdot 1 = p^{\frac{1}{2}}$$

This gives us that

$$\mathcal{S}(T_p) = p^{\frac{1}{2}} \cdot \left(\mathbb{1}_{e_1(p)T(\mathbb{Z}_p)} + \mathbb{1}_{e_2(p)T(\mathbb{Z}_p)}\right).$$

In fact, given $\mathcal{S}$ maps T_p from $\mathcal{H}_G$ to $R(GL_2(\mathbb{C})) \otimes \mathbb{C}$, according to [2] (3.9), in general, we have that

$$\mathcal{S}(T_p) = p^{\langle e_1,\rho\rangle}\chi_{e_1} + \sum_{\mu < e_1} a_{e_1}(\mu)\chi_\mu,$$

where $\chi_\mu = \mathrm{Trace}(V_\mu)$ and V_μ is the irreducible representation of $GL_2(\mathbb{C})$ with $\mu \in P^+$ is the highest weight for V_μ. Furthermore, given e_1 is a minuscule weight for $GL_2(\mathbb{C})$, i.e. there are no elements $\mu \in P^+$ with $\mu < e_1$, from [2] (3.14), we have

$$\mathcal{S}(T_p) = p^{\frac{1}{2}} \cdot \mathrm{Trace}(\mathbb{C}^2)$$

with $\mathbb{C}^2$ is the standard representation.

Moreover, from Proposition 5.14, it is clear that $\mathcal{H}_G$ is commutative as we wanted. As we can see from the previous section that multiplication in the Hecke ring is quite difficult. Given the Hecke ring is isomorphic to a polynomial ring, the multiplication of elements in the Hecke ring can therefore be identified with the multiplication of elements in the polynomial ring, thus making the computation of multiplication is easier.

Acknowledgement

I am particularly grateful for the continuous assistance and guidance given by my mentor, Hao (Billy) Lee on the readings and revisions of this paper. Much understanding of the materials mentioned in this paper come under his explanations during our weekly meeting.

In addition, I am also immensely thankful to Professor Peter May on organizing this REU. Without his support and making it possible as an online project, under such difficult condition due to the COVID pandemic, the REU wouldn't be possible, not mentioning how much new materials I learnt from the REU during this summer.

References

[1] Fred Diamond, Jerry Shurman, *A First Course in Modular Forms*, Springer-Verlag, New York, 2016, pp. 1-37, pp. 163-201

[2] Benedict H. Gross, *On the Satake Isomorphism*, In: *Galois Representations in Arithmetic Algebraic Geometry*, London Mathematical Society Lecture Note Series, **254**(1998), Cambridge University Press, pp. 223-238

[3] Benedict H. Gross, *Some Applications of Gelfand Pairs to Number Theory*, In: Bulletin of the American Mathematical Society, vol.24 no. 2, 1991

[4] Nicholas Dupré, *Subgroups of Linear Algebraic Groups* , `https://www.dpmms.cam.ac.uk/~nd332/alg_gps.pdf`.

[5] William Fulton, Joe Harris, *Representation Theory - A First Course*, Springer-Verlag, New York, 2004

[6] J. Tits, *Reductive groups over local fields*, In: *Automorphic forms, representations, and L-functions*, Proc. Symp. AMS **33** (1979), 29-69.