Math 726: L-functions and modular forms | Fall 2011

Lecture 11 : Hecke Operators and Hecke theory

Instructor: Henri Darmon | *Notes written by: Celine Maistret*

We begin with an aside on Question 1 of assignment 1 :

If $\rho = Ind_K^{\mathbb{Q}} 1_K$ then we have the following facts :

- ρ can be identified with the permutation representation of $G_{\mathbb{Q}}$ acting on $Hom(K, \bar{\mathbb{Q}})$ which is a finite set of cardinality $d = [K : \mathbb{Q}]$.

It can therefore be viewed as the permutation representation of $G_{\mathbb{Q}}$ acting on the roots of the polynomial $F_\alpha(x)$, where $F_\alpha(x)$ is the monic characteristic polynomial of any primitive element $\alpha \in K$.

- If p is prime, we can choose $\alpha \in K$ such that $F_\alpha(x) \in \mathbb{Q}[x] \cap \mathbb{Z}_p[x]$ has p-integral coefficients and $\mathbb{Z}_p[x]/F_\alpha(x) = \mathcal{O}_K \otimes \mathbb{Z}_p$

Now, in the ring of integers, factor $F_\alpha(x)$ mod p :

$F_\alpha = F_1^{e_1}....F_r^{e_r}$ with $deg(F_j) = f_j$, $(p) = \wp_1^{e_1}....\wp_r^{e_r}$ and $N(\wp_j) = p^{f_j}$. This determines the factorisation of p in $\mathcal{O}_K$

Using this, we can see how the inertia group at p permutes among themselves the roots of F_α that reduce to a common root mod p. Hence V^{I_p} can be identified with the permutation representation of $G_{\mathbb{F}_p}$ acting on the roots of $F_1....F_r$ mod p.

Therefore, $det(1 - xFrob_p) = (1 - x^{f_1})(1 - x^{f_2})...(1 - x^{f_r})$ so that the Euler factor at p of $L(s, \rho)$ is

$$(1 - p^{-sf_1})(1 - p^{-sf_2})...(1 - p^{-sf_r})$$

but $N(\wp_i) = p^{f_i}$ hence

$$L(s, \rho) = \Pi_{\wp|p}(1 - N_\wp^{-s})^{-1}$$

Q.E.D.

Back to Hecke Operators in case of Modular Forms of Level 1.

A Modular Form of weight k can be viewed as a homogeneous function on Π , the space of lattices in $\mathbb{C}$, in the following way :

$$f \mapsto F_f(\Lambda) = \omega_2^{-k} f(\omega_1/\omega_2)$$

where ω_1, ω_2 are a set of integral generators of the lattice Λ, and were chosen such that their ratio belongs to the upper half plane.

Note that we want such functions F_f to be Modular/Cuspidal homogeneous functions on Π, ie we want to control the growth conditions such that when we consider the other direction we have :

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

with f_F holomorphic at τ and has the right behavior at ∞.

Once these conditions hold, we get a bijection between the two sets.

We can now define the Hecke Operator more naturally in terms of homogeneous functions on Π :

Definition 1. For all $n \geq 1$, the Hecke Operator T_n acting on the space of homogeneous functions of weight k on Π is defined by :

$$(T_n F)(\Lambda) = n^{k-1} \sum_{\substack{\Lambda' \subset \Lambda \\ [\Lambda/\Lambda'] = n}} F(\Lambda')$$

It is clear from this definition that the image of a homogeneous function of weight k on lattices is still a homogeneous function of weight k on lattices.

But we want to check that $T_n F$ preserves the image of the space of modular forms and hence that $T_n F$ induces an action on modular forms.

In order to do this, we make a previsional definition of T_n acting on $M_k(SL_2(\mathbb{Z}))$ and $S_k(SL_2(\mathbb{Z}))$:

Definition 2. $F_{T_n f} = T_n F_f$

Using Definition 2 we derive a precise formula :

$$T_n f(z) = n^{k-1} \sum_{\gamma \in SL_2(\mathbb{Z}) \backslash M_n} f(\gamma z)(cz+d)^{-k}$$

Where M_n is the set of matrices in $M_2(\mathbb{Z})$ of determinant n, on which $SL_2(\mathbb{Z})$ acts by left multiplication.

This is motivated by the fact that, in order to produce all the sublattices of (1,z) of index n, we apply to z various mӧbius tranformations corresponding to matrices of determinant n.

It is now clear that T_n preserves holomorphicity, it remains to show that it also preserves the growth properties.

THEOREM 3. *1) If $f = \sum_{m=0}^{\infty} a(m)q^m$ belongs to $M_k(SL_2(\mathbb{Z}))$, then*

$$T_n(f)(q) = \sum_{m=0}^{\infty} \sum_{d|(m,n)} d^{k-1} a(\frac{nm}{d^2}) q^m \tag{1}$$

In particular if $n = p$ prime, then

$$T_p(f)(q) = \sum_{m=0}^{\infty} a(mp)q^m + p^{k-1} \sum_{m=0}^{\infty} a(m)q^{mp}$$

2)

$$T_n T_m = \sum_{d|(m,n)} d^{k-1} T_{\frac{mn}{d^2}}$$

In particular, 1) shows that T_n preserves Modular and Cusp forms, and 2) implies :

$$T_n T_m = T_{nm} \; if \; (m,n) = 1$$

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

In order to prove Theorem 3 we need the following lemma :

LEMMA 1. *Every orbit $SL_2(\mathbb{Z}) \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z}) \setminus M_n$ has a unique representative of the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $ad = n$; $a, d > 0$; $0 \leq b < d$.*

Proof : Let $\gcd(a', c') = g$, and let $\alpha = \begin{pmatrix} * & * \\ -\frac{c'}{g} & \frac{a'}{g} \end{pmatrix} \in SL_2(\mathbb{Z})$
Then

$$\alpha \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \; with \; determinant = n$$
$$= \begin{pmatrix} a & * \\ 0 & d \end{pmatrix} with \; ad = n; ad > 0$$

Here we can assume by eventually multipying by $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ that $a, d > 0$

Also since $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b+td \\ 0 & d \end{pmatrix}$
there exists a unique $t \in \mathbb{Z}$ such that $b + td \in [0, d)$
Hence $SL_2(\mathbb{Z}) \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = SL_2(\mathbb{Z}) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $ad = n$; $a, d > 0$; $0 \leq b < d$. $\square$

Proof of theorem 3 :
1) We can rewrite (1) as

$$T_n(f)(z) = n^{k-1} \sum_{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2\mathbb{Z} \backslash M_n} (cz+d)^{-k} f(\frac{az+b}{cz+d})$$

which, using the lemma :

$$= n^{k-1} \sum_{\substack{a,d>0 \\ ad=n}} \sum_{b=0}^{d-1} d^{-k} f(\frac{az+b}{d})$$

By bringing in the Fourier expansion

$$= n^{k-1} \sum_{\substack{a,d>0 \\ ad=n}} \sum_{b=0}^{d-1} \sum_{m=0}^{\infty} d^{-k} a(m) e^{2\pi i m (\frac{az+b}{d})}$$

$$= n^{k-1} \sum_{\substack{a,d>0 \\ ad=n}} \sum_{b=0}^{d-1} \sum_{m=0}^{\infty} d^{-k} a(m) q^{ma/d} (e^{2\pi i m/d})^b$$

if we rearrange

$$= n^{k-1} \sum_{\substack{a,d>0 \\ ad=n}} d^{-k} \sum_{m=0}^{\infty} a(m) q^{ma/d} (\sum_{b=0}^{d-1} (e^{2\pi i m/d})^b)$$

Here we note that

$$\sum_{b=0}^{d-1} ((e^{2\pi i m/d})^b) = d \ if \ d|m \ and \ 0 \ otherwise$$

hence

$$= n^{k-1} \sum_{\substack{a,d>0 \\ ad=n}} d^{1-k} \sum_{d|m=0}^{\infty} q^{am/d}$$

by changing variables $m \to md$

$$= \sum_{\substack{a,d>0 \\ ad=n}} a^{k-1} \sum_{m=0}^{\infty} a(dm) q^{am}$$

finally we group terms

$$\begin{aligned} &= \sum_{m=0}^{\infty} \sum_{a|(m,n)} a^{k-1} a(\frac{mn}{a^2}) q^m \\ &= \sum_{m=0}^{\infty} \Big(\sum_{d|(m,n)} d^{k-1} a(\frac{mn}{d^2}) \Big) q^m \end{aligned}$$

2) Exercise

□