5.1 Hecke Operators.

Def. of $T(n)$:

Let E be a set and denote the free abelian group generated by E by $X_E = \{ \sum_{x \in E} n_x x : n_x \in \mathbb{Z} \}$, that is, X_E is the set of all the $\mathbb{Z}$-linear combinations with "basis elements" from E.

A correspondense on E (with integer coeff) is a homomorphism $T: X_E \longrightarrow X_E$. Note that T being an homomorphism implies $\mathbb{Z}$-linearity and also just as in the vector space case T is completely determined by its values on the basis elements:

$$T(x) = \sum_{y \in E} n_y(x)\, y \quad , \; n_y(x) \in \mathbb{Z} \tag{58}$$

$(n_y(x) = 0$ for almos all $y)$.

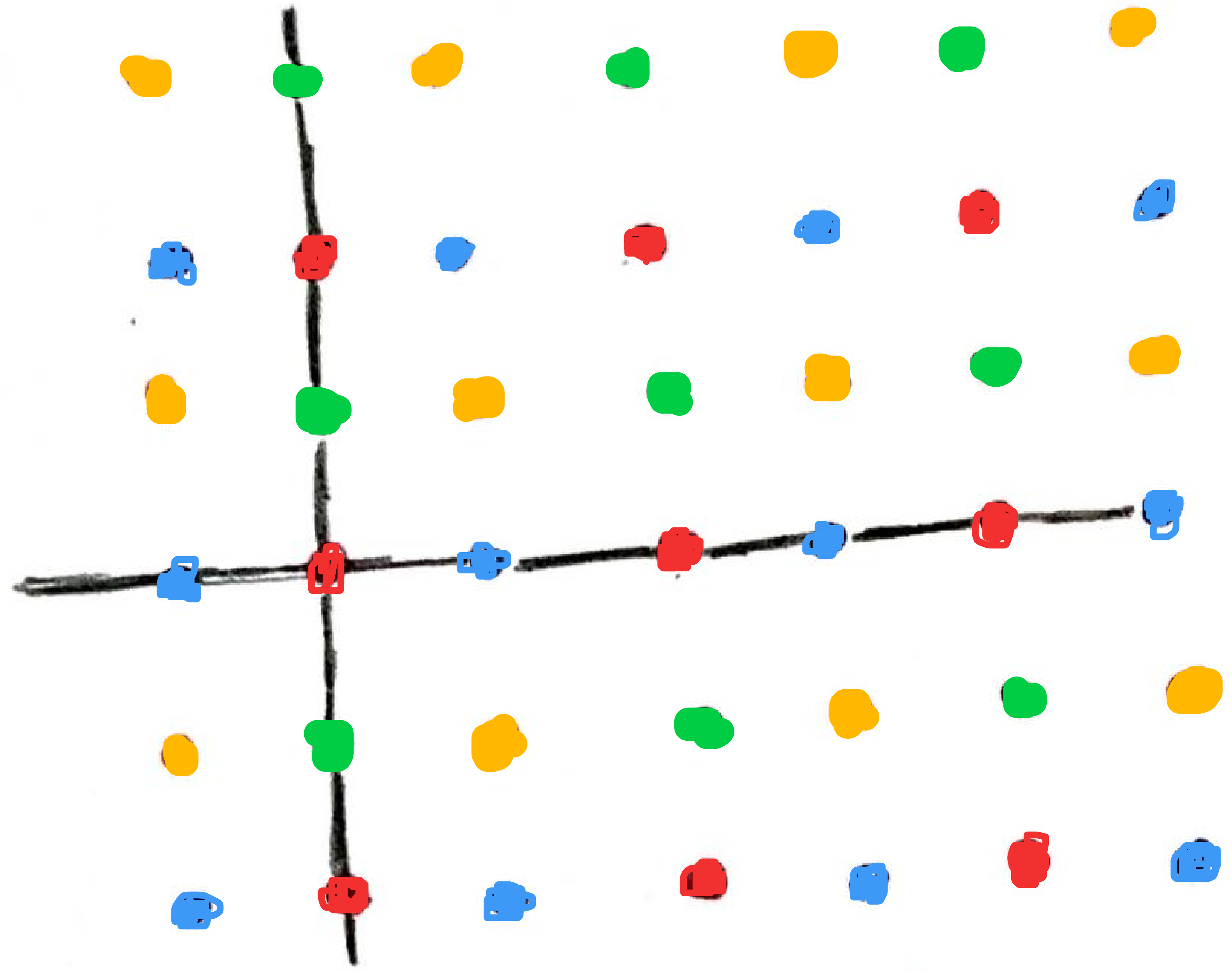
Any $\mathbb{Z}$-linear function $F: E \to \mathbb{Z}$ can be extended to a function $F: X_E \to \mathbb{Z}$. We denote TF the restriction to E of the function $F \circ T$, i.e.,

$$TF(x) = F(T(x)) = \sum_{y \in E} n_y(x) F(y). \tag{59}$$

Recall $R = \{\Lambda \text{ lattice of } \mathbb{C}\}$, let $n \geq 1$. We denote by $T(n)$ the correspondence on R: $T(n): X_R \to X_R$

$$T(n)\Lambda = \sum_{[\Lambda : \Lambda'] = n} \Lambda' \quad \text{for } \Lambda \in R, \tag{60}$$

where Λ' is a sub-lattice of Λ of index n. Note that $n\Lambda$ is contained in all the Λ', moreover, since $\Lambda \cong \mathbb{Z} \times \mathbb{Z}$ by definition Serre states that the sub-lattices Λ' of index n are the same number as the subgroups of order n of $\frac{\Lambda}{n\Lambda} \cong \frac{\mathbb{Z} \times \mathbb{Z}}{n\mathbb{Z} \times n\mathbb{Z}} = \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^2$



$\Lambda = \mathbb{Z}(1) \oplus \mathbb{Z}(i) \cong \mathbb{Z} \times \mathbb{Z}$

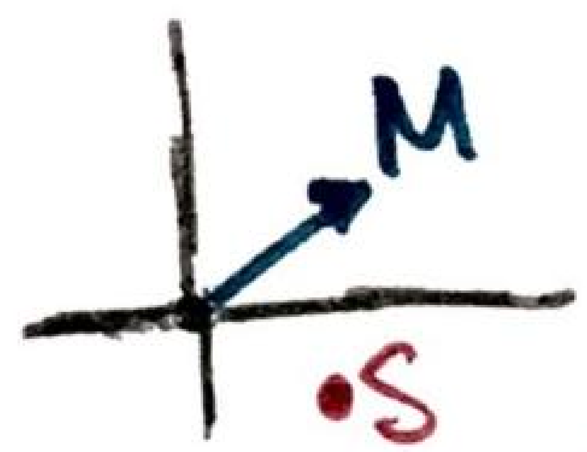
$2\Lambda = \mathbb{Z}(2) \oplus \mathbb{Z}(2i) \cong 2\mathbb{Z} \times 2\mathbb{Z}$

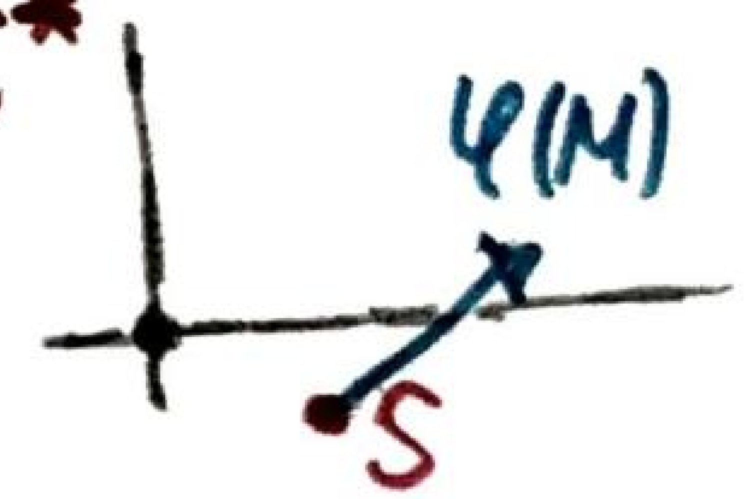
$[\Lambda : 2\Lambda] = 4 = 2^2.$

$\dfrac{\mathbb{Z} \times \mathbb{Z}}{2\mathbb{Z} \times 2\mathbb{Z}} = \left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^2 = 2^2.$

An homothety operator φ is a transformation on an affine space determined by a point S called center and for $\lambda \in \mathbb{C}^*$ called ratio

$$M \xmapsto{\varphi} S + \lambda \overrightarrow{SM}$$





Then, we set the homothety operators R_λ $\lambda \in \mathbb{C}^*$ by

(61) $$R_\lambda \Lambda = \lambda \Lambda \quad \text{for } \Delta \in R.$$

Proposition 10: The correspondences $T(n)$ and R_λ of $\mathcal{R}$ verify

$$(62) \qquad R_\lambda R_\mu = R_{\lambda\mu} \qquad (\lambda, \mu \in \mathbb{C}^*),$$

$$(63) \qquad R_\lambda T(n) = T(n) R_\lambda \qquad (n \geq 1,\ \lambda \in \mathbb{C}^*),$$

$$(64) \qquad T(m)T(n) = T(mn) \qquad \text{if } (m,n) = 1,$$

$$(65) \qquad T(p^n)T(p) = T(p^{n+1}) + p\,T(p^{n-1})R_p \qquad (p \text{ prime},\ n \geq 1).$$

Proof: (62) and (63) are trivial. To prove (64) let Λ'' a sublattice of Λ of index mn, then the abelian group Λ/Λ'', which is of order mn, has a unique decomposition as a direct sum

$$\Lambda/\Lambda'' = H_m \oplus H_n \quad \text{(F.T. of finite abelian groups)}$$

where H_m and H_n are subgroups of order m and n respectively.

$$\Rightarrow T(m)T(n)\Lambda = \sum_{[\Lambda:\Lambda']=n} T(m)\Lambda' = \sum_{\substack{[\Lambda:\Lambda']=n \\ [\Lambda':\Lambda'']=m}} \Lambda'' = \sum_{[\Lambda:\Lambda'']=mn} \Lambda'' = T(mn)\Lambda.$$

Unique for each Λ'

For (65), notice that each of the

$$T(p^n)T(p)\Lambda \; , \; T(p^{n+1})\Lambda \quad \text{and} \quad T(p^{n-1})R_p\Lambda$$

are lineal comb. of lattices contained in Λ. $([\Lambda : R_p\Lambda] = p^2)$,

By (65) we have to prove that for Λ'' s.t. $[\Lambda:\Lambda''] = p^{n+1}$ we have the coeffs. from the linear combination satisfying $a = b + pc$. By def. of $T(p^{n+1})$ we know $b = 1 \Rightarrow a = 1 + pc$

Case 1 (Λ'' is not contained in $p\Lambda$): Then $c = 0$ and a is the # of Λ' s.t. $[\Lambda:\Lambda'] = p$ and that Λ'' is a sub-lattice of Λ'.

Λ' contains $p\Lambda$ and the group $\Lambda/p\Lambda$ has order p^2.

Claim: The # of sub-lattices Λ' s.t. $[\Lambda:\Lambda'] = p$ are $p+1$ for p prime (Serre states that they are the # of points of the projective line over a field with p elements).

With this claim we can conclude that in $\Lambda/p\Lambda$ the image of Λ' is of index p and contains the image of Λ''.

In $\Delta/p\Delta$ the image of Δ'' is of order p, hence also of index p; thus there is only one Δ' with the desired properties. This gives $a=1$.

Case 2 ($\Delta'' \subset p\Delta$): We have $c=1$; since any lattice Δ' of index p contains $p\Delta$, thus they contain Δ''. This gives $a=p+1$ $(a=cp+1)$ by the red claim.

<u>Corollary 1.</u> The $T(p^n)$, $n>1$, are polynomials in $T(p)$ and R_p.
This follows from (65) by induction on n.

<u>Corollary 2.</u> The algebra generated by R_λ and the $T(p)$ for p prime is commutative; it contains all the $T(n)$.
This follows from (63), (65) and Corollary 1.

Action of $T(n)$ on functions of weight $2k$.

Let $F \in \mathcal{R}$ of weight $2k$ $\Rightarrow$ (66) $R_\lambda F = \lambda^{-2k} F \quad \forall \lambda \in \mathbb{C}^*$.

Formula (63) shows that $T(n)F$ is also of weight $2k$:

$$R_\lambda(T(n)F) = T(n)(R_\lambda F) = \lambda^{-2k}\, T(n)F.$$

5.2 A matrix lemma

Lemma 2. Let S_n be the set of integer matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $ad = n$, $a \geq 1$, $0 \leq b < d$. If $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ is contained in S_n, let Λ_σ be the sub-lattice of Λ having for basis

$$\omega_1' = a\omega_1 + b\omega_2, \quad \omega_2' = d\omega_2.$$

The map $\sigma \mapsto \Lambda_\sigma$ is a bijection of S_n onto the set $\Lambda(n)$ of sub-lattices of index n in Λ.

Λ_6 belongs to $\Lambda(n)$ because $\det(6) = ad = n$.

Conversely let $\Lambda' \in \Lambda(n)$, we want to assign uniquely a matrix $6(\Lambda') \in S_n$. Put

$$Y_1 = \Lambda / (\Lambda' + \mathbb{Z}\omega_2) \quad \text{and} \quad Y_2 = \mathbb{Z}\omega_2 / (\Lambda' \cap \mathbb{Z}\omega_2).$$

These are cyclic groups generated respectively by the images of ω_1 and ω_2, respectively. Which implies $\Lambda/\Lambda' \cong Y_1 \oplus Y_2$ and make this into an exact sequence:

$$0 \to Y_1 \to \Lambda/\Lambda' \to Y_2 \to 0.$$

Let a and d be the orders of Y_1 and Y_2 it proves that $ad = n$. (Splitting lemma for abelian groups)

If $\omega_2' = d\omega_2$, then $\omega_2' \in \Lambda'$. On the other hand there exists $\omega_1' \in \Lambda'$ s.t. $\omega_1' \equiv a\omega_1 \pmod{\mathbb{Z}\omega_2}$

Where ω_1' and ω_2' are a basis for Δ'. Moreover, we can write ω_1' uniquely by choosing $0 \leq b < d$ in this way

$$\omega_1' = a\omega_1 + b\omega_2,$$

which fixes ω_1' and then a, b, d which determines $\sigma(\Delta') \in S_n$.

The maps $\sigma \mapsto \Delta_\sigma$ and $\Delta' \mapsto \sigma(\Delta')$ are inverses to each other, that completes the proof.

Example: If p is prime, the elements of S_p are the $p+1$ matrices

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} \text{ with } 0 \leq b < p.$$

Which agrees with the fact that the # of sub-lattices Δ' s.t. $[\Delta : \Delta'] = p$ are $p+1$ (red claim).

5.3 Action of $T(n)$ on modular functions.

Let f be a weakly modular function of weight $2k$:

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) \quad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

and f meromorphic on H.

As we have seen f corresponds to a function F of weight $2k$ on $\mathcal{R}$ such that

$$(70) \quad F(\Lambda(\omega_1, \omega_2)) = \omega_2^{-2k} f(\omega_1/\omega_2) \quad \text{where } \omega_1/\omega_2 \in H.$$

We define $T(n)f$ as a function acting on F, given by

$$T(n)f(z) = n^{2k-1}\, T(n)\, F(\Lambda(z,1))$$

$$= n^{2k-1}\, T(n) \left(d^{-2k} f\left(\frac{az+b}{d}\right)\right)$$

By yesterdays lemma

$$= n^{2k-1} \sum_{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_n} d^{-2k} f\left(\frac{az+b}{d}\right)$$

$$\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_n \longmapsto \Lambda_\sigma(\omega_1', \omega_2')$$

is a bijection.

$$= n^{2k-1} \sum_{\substack{a \geq 1,\, ad = n \\ 0 \leq b < d}} d^{-2k} f\left(\frac{az+b}{d}\right) \quad (71)$$

Proposition 11: The function $T(n)f$ is weakly modular of weight $2k$. It is holomorphic on H if f is. We have:

$$(72) \quad T(m)T(n)f = T(mn)f \quad \text{if } (m,n)=1,$$

$$(73) \quad T(p)T(p^n)f = T(p^{n+1})f + p^{2k-1}T(p^{n-1})f \quad \text{if } p \text{ is prime}, n \geq 1.$$

Behaviour at infinity:

Suppose f is a modular function i.e. is meromorphic at ∞. Let

$$(74) \quad f(z) = \sum_{m \in \mathbb{Z}} c(m) q^m \qquad q = e^{2\pi i z}$$

Proposition 12: The function $T(n)f$ is a modular function. We have

$$(75) \quad T(n)f(z) = \sum_{m \in \mathbb{Z}} \gamma(m) q^m \quad \text{with}$$

$$(76) \quad \gamma(m) = \sum_{\substack{a \mid (n,m) \\ a \geq 1}} a^{2k-1} c\left(\frac{mn}{a^2}\right).$$

Proof: By def. we have: (71)

$$T(n)f(z) = n^{2k-1} \sum_{\substack{a\geq 1, ad=n \\ 0\leq b<d}} d^{-2k} \sum_{m\in\mathbb{Z}} c(m)\, e^{2\pi i m\left(\frac{az+b}{d}\right)}$$

, note that

the sum

$$\sum_{0\leq b<d} e^{2\pi i m b/d} = \begin{cases} d & \text{if } d \mid m \quad \left(\begin{array}{c}\text{Sum of } 1\\ d \text{ times}\end{array}\right) \\ 0 & \text{otherwise} \quad \left(\begin{array}{c}\text{Sum of the}\\ d \text{ roots of}\\ \text{unity } z^d=1.\end{array}\right)\end{cases}$$

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

$$T(n)f(z) = n^{2k-1} \sum_{\substack{ad=n \\ a\geq 1,\, m'\in\mathbb{Z}}} d^{-2k+1}\, c(m'd)\, q^{am'}.$$

Collecting powers of q by putting $am' = j$, gives:

$$T(n)f(z) = \sum_{j\in\mathbb{Z}} q^j \sum_{\substack{a \mid (n,j) \\ a\geq 1}} \left(\frac{n}{d}\right)^{2k-1} c\left(\frac{jd}{a}\right).$$

Since f is meromorphic at infinity $\exists N\geq 0$ s.t. $c(m)=0$ if $m\leq -N$.

$\Rightarrow c\left(\frac{jd}{a}\right)=0$ if $j\leq -\frac{aN}{d}$, which shows that $T(n)f$ is also meromorphic at infinity.

12

By Prop 11 it is weakly modular $\Rightarrow$ $T(n)f$ is a modular function. Doing the changes $n = ad$ and $j = m$ we get (76).

Corollary 1. $\gamma(0) = \sigma_{2k-1}(n)\, c(0)$ and $\gamma(1) = c(n)$. (just $a=1$)

Corollary 2. If $n=p$ with p prime, one has

$$\gamma(m) = \begin{cases} c(pm) & \text{if } m \not\equiv 0 \pmod p, \quad \text{(just the term } a=1\text{.)} \\ c(pm) + p^{2k-1} c(m/p) & \text{if } m \equiv 0 \pmod p. \quad \text{(just the terms } a=1 \text{ and } a=p\text{.)} \end{cases}$$

Corollary 3. If f is a modular form (resp a cusp form), so is $T(n)f$.

Thus, the $T(n)$ act on the spaces M_k and M_k^0, where the Hecke operators commute with each other and satisfy the identities (72) and (73).

5.4 Eigenfunctions of the $T(n)$.

A modular form f of weight $2k$ is an eigenfunction of all the $T(n)$ if

$$T(n)f = \lambda(n) f \quad \text{for all } n \geq 1 \text{ and } \lambda(n) \in \mathbb{C}. \tag{77}$$

Theorem 7. a) The coefficient $c(1)$ of q in f is $\neq 0$.

b) If f is normalized by the conditions $c(1) = 1$, then

$$c(n) = \lambda(n) \quad \text{for all } n > 1. \tag{78}$$

Proof: Let $f(z) = \sum_{n=0}^{\infty} c(n) q^n$, then Corollary 1 of Prop 12 implies the coefficient of q in $T(n)f$ is $c(n)$. On the other hand, by (77), it is also $\lambda(n)c(1)$ $\Rightarrow$ $c(n) = \lambda(n)c(1)$.

If $c(1)$ were zero, all the $c(n)$ would be zero for $n > 0$ and f would be constant. Hence a) and b) follows.

Corollary 1. Two modular forms of weight $2k$, $k>0$, which are eigenfunctions of the $T(n)$ with the same eigenvalues $\lambda(n)$, and which are normalized, coincide.

Corollary 2. Under the hypothesis of Theorem 7, b):

$$c(m)c(n) = c(mn) \quad \text{if } (m,n)=1 \tag{79}$$

$$c(p)c(p^n) = c(p^{n+1}) + p^{2k-1}c(p^{n-1}), \quad p \text{ prime.} \tag{80}$$

The result follows by $T(n)f = \lambda(n)f$ and the fact that $T(n)$ satisfies (72) and (73). Actually, from $c(n)=\lambda(n)$ we see that the same expressions are true for the normalized eigenvalues.

(79) and (80) canbe translated analytically in the following way:
Let the Dirichlet series defined by the $c(n)$

$$\Phi_f(s) = \sum_{n=1}^{\infty} c(n)/n^s \tag{81}$$

The Corollary of Th. 5 in page 94 tells us that $C(n) = O(n^{2K-1})$, which implies that (81) converges absolutely for $\mathrm{Re}(s) > 2K$.

Corollary 3. We have:

(82) $$\Phi_f(s) = \prod_{p \in P} \frac{1}{1 - c(p)p^{-s} + p^{2K-1-2s}}$$

Proof: We have seen that the associated Dirichlet series of a multiplicative function f satisfies.

$$\Phi_f(s) = \prod_{p \in P} (1 + f(p)p^{-s} + \ldots + f(p^m)p^{-ms} + \ldots) \quad \text{(Lemma 4) Page 69.}$$

By (79) $n \mapsto c(n)$ is multiplicative, then

$$\Phi_f(s) = \prod_{p \in P} \left(\sum_{n=0}^{\infty} c(p^n) p^{-ns} \right).$$

That is, putting $Q = p^{-s}$, we are required to prove.

(83) $$\sum_{n=0}^{\infty} c(p^n) Q^n = \frac{1}{1 - c(p)Q + p^{2K-1}Q^2}.$$

To do this, consider the series

$$\psi(Q)=\left(\sum_{n=0}^{\infty} c(p^n)Q^n\right)\left(1-c(p)Q+p^{2K-1}Q^2\right).$$

The coefficient of Q in ψ is $c(p)-c(p)=0$. The one for T^{n+1} for $n\geq 1$ is

$$c(p^{n+1})-c(p)c(p^n)+p^{2K-1}c(p^{n-1})=0 \quad \text{by (80)}.$$

Thus $\psi(Q)$ is reduced to its constant term $c(1)=1$, proving (83).

Remark Hecke has proved that Φ_f extends analytically to a meromorphic function on the whole plane and that the function

(84) $$X_f(s)=(2\pi)^{-s}\,\Gamma(s)\,\Phi_f(s)$$

satisfies the functional equation

(85) $$X_f(s)=(-1)^K X_f(2K-s).$$

The proof uses Mellin's formula

$$X_f(s)=\int_0^{\infty}(f(iy)-f(\infty))\,y^s\,\frac{dy}{y}$$

together with the identity $f(-1/z) = z^{2k} f(z)$. Hecke also proved a converse: every Dirichlet series Φ which satisfies a functional equation like (85) and some regularity and growth hyphotesis, comes from a modular form f of weight $2k$; moreover, f is normalized eigenfunction of the $T(n)$ if and only if Φ is a product of type (82) (Eulerian product).

5.6 Complements

5.6.1. The Petersson scalar product.

Let $f, g \in M_k^0$, the measure

$$\mu(f,g) = f(z)\overline{g(z)}\, y^{2k-2}\, dx\,dy \quad (x = \mathrm{Re}(z),\ y = \mathrm{Im}(z))$$

is invariant by $G = SL_2(\mathbb{Z})/\{\pm I\}$ the modular group. To check this, recall that G is generated by

$$S : z \longmapsto -1/z$$

$$T : z \longmapsto z+1 .$$

It is sufficient to check that $\mu(f,g)$ is invariant under S and T.

$\mu(fT, gT) = \mu(f,g)$ is trivially true since f is a weakly modular function of weight $2K$ if and only if

a) $f(z+1) = f(z)$

b) $f(-1/z) = z^{2K} f(z)$.

Then, since $\mathrm{Im}(Tz) = \mathrm{Im}(z) = y$ and $f(z+1) = f(z)$, $g(z+1) = g(z)$ one has the result. For S, note that $Sz = -\frac{1}{z} = -\frac{\bar{z}}{|z|^2} = \frac{-x}{|z|^2} + i\frac{y}{|z|^2}$

$\Rightarrow \mathrm{Im}(Sz) = y/|z|^2$ and

$$\mu(fS, gS) = f(Sz)\overline{g(Sz)}\,(y/|z|^2)^{2K-2}\,dx\,dy/|z|^4$$
$$= z^{2K} f(z)\,\bar{z}^{2K}\,\overline{g(z)}\,(y/|z|^2)^{2K-2}\,dx\,dy/|z|^4$$
$$= |z|^{4K} f(z)\overline{g(z)}\,y^{2K-2}\,|z|^{-4K+4}\,dx\,dy/|z|^4$$
$$= f(z)\bar{g}(z)\,y^{2K-2}\,dx\,dy$$
$$= \mu(f,g).$$

Then $\mu(f,g)$ is invariant under G, moreover, it is also bounded on the quotient H/G with fundamental domain D 

$$\langle f,g\rangle = \int_{H/G} \mu(f,g) = \int_{D} f(z)\,\overline{g(z)}\, y^{2k-2}\, dx\,dy$$

where $\langle\cdot,\cdot\rangle$ is positive and non-degenerate. One can check that

$$(88) \qquad \langle T(n) f, g\rangle = \langle f, T(n) g\rangle,$$

that follows by
$$T(n) f(z) = \sum_{j\in\mathbb{Z}} q^j \sum_{\substack{a\mid(n,j)\\ a\geq 1}} \left(\frac{n}{d}\right)^{2k-1} c\left(\frac{jd}{a}\right)$$

and the fact that $n \mapsto c(n)$ is multiplicative.

(88) means that the $T(n)$ are Hermitian operators with respect to $\langle f,g\rangle$. Since $T(n)$ and $T(m)$ commutes, then there exists an orthogonal basis of M_k^0 made of eigenvectors of $T(n)$ and that the eigenvalues on $T(n)$ are real numbers.

5.6.2 Integrability properties

Let $M_k(\mathbb{Z})$ be the set of modular forms of weight $2k$ whose coefficients $c(n) \in \mathbb{Z}$. One can prove that there exists a $\mathbb{Z}$-basis of $M_k(\mathbb{Z})$ which is a $\mathbb{C}$-basis of M_k.

Explicitely the following basis:

k even: The monomials $E_2^\alpha F^\beta$ where $\alpha, \beta \in \mathbb{N}$ s.t. $\alpha + 3\beta = k/2$;

k odd: The monomials $E_3 E_2^\alpha F^\beta$ where $\alpha + 3\beta = (k-3)/2$. (*)

where E_k is the Eisenstein's series of weight $2k$ and

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

Prop 12 and (76) shows that $T(n) f \in M_k(\mathbb{Z})$ for any $f \in M_k(\mathbb{Z})$ and $n \geq 1$. By the fact that (*) is a $\mathbb{C}$-basis of M_k, then the coefficients of the characteristic polynomial of the $T(n)$ acting on M_k are integers; which means that the eigenvalues are all algebraic integers.

J.6.3 The Ramanujan–Petersson conjecture.

Let $f = \sum_{n=1}^{\infty} c(n) q^n$, $c(1) = 1$ be a cusp form of weight $2k$ which is a normalized eigenfunction of the $T(n)$.

Let $\Phi_{f,p}(Q) = 1 - c(p)Q + p^{2k-1} Q^2$, p prime (appearing in (83)).

We can write

$\Phi_{f,p}(Q) = (1 - \alpha_p Q)(1 - \alpha_p' Q)$ with $\alpha_p + \alpha_p' = c(p)$, $\alpha_p \alpha_p' = p^{2k-1}$.

The Petersson conjecture is that α_p and α_p' are complex conjugate.

One can also express it by:

$$|\alpha_p| = |\alpha_p'| = p^{k-1/2} \quad \text{or} \quad |c(p)| \leq 2p^{k-1/2}$$

$$(|\alpha_p|^2 = p^{2k-1}) \qquad \text{(Triangular inequality)}$$

or $|c(n)| \leq n^{k-1/2} \sigma_0(n)$ for all $n \geq 1$.

For $k=6$, this is the Ramanujan conjecture: $|\tau(p)| \leq 2p^{11/2}$

where $F(z) = q \prod_{n=1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$.

These conjectures have been proved in 1973 by P. Deligne as consequence of the "Weil conjectures" about algebraic varieties over finite fields.