10

Modular Forms of Higher Level: 252, W. Stein, October 29

10.1 Modular Forms on $\Gamma_1(N)$

Fix integers $k \geq 0$ and $N \geq 1$. Recall that $\Gamma_1(N)$ is the subgroup of elements of $\mathrm{SL}_2(\mathbf{Z})$ that are of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ when reduced modulo N.

Definition 10.1.1 (Modular Forms). The space of *modular forms* of level N and weight k is

$$M_k(\Gamma_1(N)) = \left\{ f : f(\gamma\tau) = (c\tau + d)^k f(\tau) \text{ all } \gamma \in \Gamma_1(N) \right\},$$

where the f are assumed holomorphic on $\mathfrak{h} \cup \{\text{cusps}\}$ (see below for the precise meaning of this). The space of *cusp forms* of level N and weight k is the subspace $S_k(\Gamma_1(N))$ of $M_k(\Gamma_1(N))$ of modular forms that vanish at all cusps.

Suppose $f \in M_k(\Gamma_1(N))$. The group $\Gamma_1(N)$ contains the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, so

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

and for f to be holomorphic at infinity means that f has a Fourier expansion

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

To explain what it means for f to be holomorphic at all cusps, we introduce some additional notation. For $\alpha \in \mathrm{GL}_2^+(\mathbf{R})$ and $f : \mathfrak{h} \to \mathbf{C}$ define another function $f_{|[\alpha]_k}$ as follows:

$$f_{|[\alpha]_k}(z) = \det(\alpha)^{k-1}(cz + d)^{-k} f(\alpha z).$$

It is straightforward to check that $f_{|[\alpha\alpha']_k} = (f_{|[\alpha]_k})_{|[\alpha']_k}$. Note that we do not have to make sense of $f_{|[\alpha]_k}(\infty)$, since we only assume that f is a function on $\mathfrak{h}$ and not $\mathfrak{h}^*$.

Using our new notation, the transformation condition required for $f : \mathfrak{h} \to \mathbf{C}$ to be a modular form for $\Gamma_1(N)$ of weight k is simply that f be fixed by the $[\;]_k$-action of $\Gamma_1(N)$. Suppose $x \in \mathbf{P}^1(\mathbf{Q})$ is a cusp, and choose $\alpha \in \mathrm{SL}_2(\mathbf{Z})$ such that $\alpha(\infty) = x$. Then $g = f_{|[\alpha]_k}$ is fixed by the $[\;]_k$ action of $\alpha^{-1}\Gamma_1(N)\alpha$.

Lemma 10.1.2. *Let $\alpha \in \mathrm{SL}_2(\mathbf{Z})$. Then there exists a positive integer h such that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \alpha^{-1}\Gamma_1(N)\alpha$.*

Proof. This follows from the general fact that the set of congruence subgroups of $\mathrm{SL}_2(\mathbf{Z})$ is closed under conjugation by elements $\alpha \in \mathrm{SL}_2(\mathbf{Z})$, and every congruence subgroup contains an element of the form $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$. If G is a congruence subgroup, then $\Gamma(N) \subset G$ for some N, and $\alpha^{-1}\Gamma(N)\alpha = \Gamma(N)$, since $\Gamma(N)$ is normal, so $\Gamma(N) \subset \alpha^{-1}G\alpha$. □

Letting h be as in the lemma, we have $g(z + h) = g(z)$. Then the condition that f be holomorphic at the cusp x is that

$$g(z) = \sum_{n \geq 0} b_{n/h} q^{1/h}$$

on the upper half plane. We say that f vanishes at x if $b_{n/h} = 0$, so a cusp form is a form that vanishes at every cusp.

10.2 The Diamond Bracket and Hecke Operators

In this section we consider the spaces of modular forms $S_k(\Gamma_1(N), \varepsilon)$, for Dirichlet characters ε mod N, and explicitly describe the action of the Hecke operators on these spaces.

10.2.1 Diamond Bracket Operators

The group $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$, and the quotient $\Gamma_0(N)/\Gamma_1(N)$ is isomorphic to $(\mathbf{Z}/N\mathbf{Z})^*$. From this structure we obtain an action of $(\mathbf{Z}/N\mathbf{Z})^*$ on $S_k(\Gamma_1(N))$, and use it to decompose $S_k(\Gamma_1(N))$ as a direct sum of more manageable chunks $S_k(\Gamma_1(N), \varepsilon)$.

Definition 10.2.1 (Dirichlet character). A *Dirichlet character* ε modulo N is a homomorphism

$$\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*.$$

We extend ε to a map $\varepsilon : \mathbf{Z} \to \mathbf{C}$ by setting $\varepsilon(m) = 0$ if $(m, N) \neq 1$ and $\varepsilon(m) = \varepsilon(m \bmod N)$ otherwise. If $\varepsilon : \mathbf{Z} \to \mathbf{C}$ is a Dirichlet character, the *conductor* of ε is the smallest positive integer N such that ε arises from a homomorphism $(\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$.

Remarks 10.2.2.

1. If ε is a Dirichlet character modulo N and M is a multiple of N then ε induces a Dirichlet character mod M. If M is a divisor of N then ε is induced by a Dirichlet character modulo M if and only if M divides the conductor of ε.

2. The set of Dirichlet characters forms a group, which is non-canonically isomorphic to $(\mathbf{Z}/N\mathbf{Z})^*$ (it is the dual of this group).
3. The mod N Dirichlet characters all take values in $\mathbf{Q}(e^{2\pi i/e})$ where e is the exponent of $(\mathbf{Z}/N\mathbf{Z})^*$. When N is an odd prime power, the group $(\mathbf{Z}/N\mathbf{Z})^*$ is cyclic, so $e = \varphi(\varphi(N))$. This double-φ can sometimes cause confusion.
4. There are many ways to represent Dirichlet characters with a computer. I think the best way is also the simplest—fix generators for $(\mathbf{Z}/N\mathbf{Z})^*$ in any way you like and represent ε by the images of each of these generators. Assume for the moment that N is odd. To make the representation more "canonical", reduce to the prime power case by writing $(\mathbf{Z}/N\mathbf{Z})^*$ as a product of cyclic groups corresponding to prime divisors of N. A "canonical" generator for $(\mathbf{Z}/p^r\mathbf{Z})^*$ is then the smallest positive integer s such that $s \bmod p^r$ generates $(\mathbf{Z}/p^r\mathbf{Z})^*$. Store the character that sends s to $e^{2\pi i n/\varphi(\varphi(p^r))}$ by storing the integer n. For general N, store the list of integers n_p, one p for each prime divisor of N (unless $p = 2$, in which case you store two integers n_2 and n_2', where $n_2 \in \{0, 1\}$).

Definition 10.2.3. Let $\overline{d} \in (\mathbf{Z}/N\mathbf{Z})^*$ and $f \in S_k(\Gamma_1(N))$. The map $\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ is surjective, so there exists a matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ such that $d \equiv \overline{d} \pmod{N}$. The *diamond bracket d operator* is then

$$f(\tau)|\langle d\rangle = f_{|[\gamma]_k} = f(\gamma\tau)(c\tau + d)^{-k}.$$

Remark 10.2.4. Fred Diamond was named after diamond bracket operators.

The definition of $\langle d\rangle$ does not depend on the choice of lift matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, since any two lifts differ by an element of $\Gamma(N)$ and f is fixed by $\Gamma(N)$ since it is fixed by $\Gamma_1(N)$.

For each Dirichlet character ε mod N let

$$\begin{aligned} S_k(\Gamma_1(N), \varepsilon) &= \{f : f|\langle d\rangle = \varepsilon(d) f \text{ all } d \in (\mathbf{Z}/N\mathbf{Z})^*\} \\ &= \{f : f_{|[\gamma]_k} = \varepsilon(d_\gamma) f \text{ all } \gamma \in \Gamma_0(N)\}, \end{aligned}$$

where d_γ is the lower-left entry of γ.

When $f \in S_k(\Gamma_1(N), \varepsilon)$, we say that f has *Dirichlet character* ε. In the literature, sometimes f is said to be of "nebentypus" ε.

Lemma 10.2.5. *The operator $\langle d\rangle$ on the finite-dimensional vector space $S_k(\Gamma_1(N))$ is diagonalizable.*

Proof. There exists n such that $I = \langle 1\rangle = \langle d^n\rangle = \langle d\rangle^n$, so the characteristic polynomial of $\langle d\rangle$ divides the square-free polynomial $X^n - 1$. □

Note that $S_k(\Gamma_1(N), \varepsilon)$ is the $\varepsilon(d)$ eigenspace of $\langle d\rangle$. Thus we have a direct sum decomposition

$$S_k(\Gamma_1(N)) = \bigoplus_{\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*} S_k(\Gamma_1(N), \varepsilon).$$

We have $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \Gamma_0(N)$, so if $f \in S_k(\Gamma_1(N), \varepsilon)$, then

$$f(\tau)(-1)^{-k} = \varepsilon(-1) f(\tau).$$

Thus $S_k(\Gamma_1(N), \varepsilon) = 0$, unless $\varepsilon(-1) = (-1)^k$, so about half of the direct summands $S_k(\Gamma_1(N), \varepsilon)$ vanish.

10.2.2 Hecke Operators on q-expansions

Suppose

$$f = \sum_{n=1}^{\infty} a_n q^n \in S_k(\Gamma_1(N), \varepsilon),$$

and let p be a prime. Then

$$f|T_p = \begin{cases} \sum_{n=1}^{\infty} a_{np} q^n + p^{k-1}\varepsilon(p) \sum_{n=1}^{\infty} a_n q^{pn}, & p \nmid N \\ \sum_{n=1}^{\infty} a_{np} q^n + 0. & p \mid N. \end{cases}$$

Note that $\varepsilon(p) = 0$ when $p \mid N$, so the second part of the formula is redundant.

When $p \mid N$, T_p is often denoted U_p in the literature, but we will not do so here. Also, the ring $\mathbf{T}$ generated by the Hecke operators is commutative, so it is harmless, though potentially confusing, to write $T_p(f)$ instead of $f|T_p$.

We record the relations

$$T_m T_n = T_{mn}, \quad (m, n) = 1,$$
$$T_{p^k} = \begin{cases} (T_p)^k, & p \mid N \\ T_{p^{k-1}} T_p - \varepsilon(p) p^{k-1} T_{p^{k-2}}, & p \nmid N. \end{cases}$$

WARNING: When $p \mid N$, the operator T_p on $S_k(\Gamma_1(N), \varepsilon)$ need not be diagonalizable.

I will say more about the definition of Hecke operators on Friday.

10.3 Old and New Subspaces

Let M and N be positive integers such that $M \mid N$ and let $t \mid \frac{N}{M}$. If $f(\tau) \in S_k(\Gamma_1(M))$ then $f(t\tau) \in S_k(\Gamma_1(N))$. We thus have maps

$$S_k(\Gamma_1(M)) \to S_k(\Gamma_1(N))$$

for each divisor $t \mid \frac{N}{M}$. Combining these gives a map

$$\varphi_M : \bigoplus_{t|(N/M)} S_k(\Gamma_1(M)) \to S_k(\Gamma_1(N)).$$

Definition 10.3.1 (Old Subspace). The *old subspace* of $S_k(\Gamma_1(N))$ is the subspace generated by the images of the φ_M for all $M \mid N$ with $M \neq N$.

Definition 10.3.2 (New Subspace). The *new subspace* of $S_k(\Gamma_1(N))$ is the complement of the old subspace with respect to the Petersson inner product.

Since I haven't introduced the Petersson inner product yet, note that the new subspace of $S_k(\Gamma_1(N))$ is the largest subspace of $S_k(\Gamma_1(N))$ that is stable under the Hecke operators and has trivial intersection with the old subspace of $S_k(\Gamma_1(N))$.

Definition 10.3.3 (Newform). A *newform* is an element f of the new subspace of $S_k(\Gamma_1(N))$ that is an eigenvector for every Hecke operator, which is normalized so that the coefficient of q in f is 1.

If $f = \sum a_n q^n$ is a newform then the coefficient a_n are algebraic integers, which have deep arithmetic significance. For example, when f has weight 2, there is an associated abelian variety A_f over $\mathbf{Q}$ of dimension $[\mathbf{Q}(a_1, a_2, \ldots) : \mathbf{Q}]$ such that $\prod L(f^\sigma, s) = L(A_f, s)$, where the product is over the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-conjugates of F. The abelian variety A_f was constructed by Shimura as follows. Let $J_1(N)$ be the Jacobian of the modular curve $X_1(N)$. As we will see tomorrow, the ring $\mathbf{T}$ of Hecke operators acts naturally on $J_1(N)$. Let I_f be the kernel of the homomorphism $\mathbf{T} \to \mathbf{Z}[a_1, a_2, \ldots]$ that sends T_n to a_n. Then

$$A_f = J_1(N)/I_f J_1(N).$$

In the converse direction, it is a deep theorem of Breuil, Conrad, Diamond, Taylor, and Wiles that if E is any elliptic curve over $\mathbf{Q}$, then E is isogenous to A_f for some f of level equal to the conductor N of E.

When f has weight greater than 2, Scholl constructs, in an analogous way, a Grothendieck motive (=compatible collection of cohomology groups) $\mathcal{M}_f$ attached to f.