1 Lecture One

Instructor: Julia Gordon; gor@math.ubc.ca

Text: Modular Functions and Modular Forms, J. Milne

References to algebraic geometry will be only occasional, and can often be safely ignored. We closely follow Milne’s introduction to the subject.

We begin with a broad goal: to study all holomorphic (or meromorphic) functions on all Riemann surfaces. Recall that a Riemann surface is a one-dimensional complex manifold; that is, it is a connected, Hausdorff topological space \( X \) equipped with a family of charts \((U, \phi)\), with

\[ \phi : U \rightarrow \mathbb{C} \]

a homeomorphism onto an open subset of \( \mathbb{C} \), and for which, whenever \((U_1, \phi_1)\) and \((U_2, \phi_2)\) are charts with \( U_1 \cap U_2 \neq \emptyset \), the map

\[ \phi_2 \circ \phi_1^{-1} : \phi_1(U) \rightarrow \mathbb{C} \]

is holomorphic. Such a covering by charts is called a complex structure on \( X \).

Examples:

1. \( \mathbb{C} \), or any connected open subset of \( \mathbb{C} \).

2. The Riemann sphere \( \mathbb{P}^1(\mathbb{C}) \). We briefly review its construction: this is the set of dimension one subspaces in \( \mathbb{C}^2 \), described in homogeneous coordinates:

\[ aX + bY = 0 \text{ corresponds to } (a : b) \text{ corresponds to } (1 : \frac{b}{a}) \]

3. The standard torus. This (as we will soon see) admits infinitely many non-isomorphic complex structures.
2 Lecture Two

There will be extra classes Fridays at 16.00-17.30 on days when colloquium is off, or irrelevant. The first homework assignment has been posted.

The goal for this class is to carefully describe the affine modular curve $\Gamma \backslash H$, where $\Gamma$ is some group of interest, as:

1. a topological space;
2. a Riemann surface; and, later,
3. an algebraic variety.

We begin with some careful review of group actions. Let $G$ be a topological group; that is, a group which is a Hausdorff topological space, and for which the multiplication homomorphism $G \times G \to G$ and the inversion homomorphism $G \to G$ are continuous with respect to this topology. If $X$ is a topological space, we say that $G$ acts \textit{continuously} on $X$ if the map

$$G \times X \to X$$

$$(g, x) \mapsto g \cdot x$$

is continuous. From now on, we will assume that all actions of topological groups on topological spaces are continuous.

\textbf{Definition:} The \textbf{stabilizer} of $x \in X$ in $G$ is the subgroup

$$\text{Stab}_G(x) = \{g \in G : g \cdot x = x\}.$$ 

If $H \leq G$ is a subgroup of our topological group, then a topology (known as the \textbf{quotient topology}) is placed on the coset space $G/H$ by choosing the finest topology on $G/H$ for which the canonical projection $G \to G/H$ is continuous. More precisely: a subset $U \subseteq G/H$ is open in the quotient topology if and only if the union of cosets in $U$ is an open subset of $G$. In the same way, we can define a topology on the orbit space $G \setminus X$ of a topological space $X$ under a continuous action; this will be the finest topology on the space of orbits such that the map $X \to G \setminus X$ is continuous.

\textbf{Facts:} (to be solved as homework)

1. If $X$ is Hausdorff, then for all $x \in G$, $\text{Stab}_G(x)$ is a closed subgroup of $G$. 


2. The quotient $G/H$ is Hausdorff if and only if $H$ is closed in $G$ (as such, $G/H$ is a topological group if and only if $H$ is normal and closed).

3. Suppose the action of $G$ on $X$ is continuous and transitive (i.e., $X$ consists of a single orbit), and that $G$ is locally compact and second-countable; then the bijection $G/\text{Stab}_G(x) \to X$ is, in fact, a homeomorphism.

4. Assume further that $\text{Stab}_G(x)$ is compact in $G$ for all $x \in X$; then $\Gamma \subseteq G$ is discrete if and only if $\Gamma$ acts properly discontinuously on $X$.

5. With the same assumptions: if $\Gamma$ is discrete, then $\Gamma \backslash X$ is Hausdorff.

Aside: The dedicated reader should take the time to read pp. 16-18 in Milne’s notes, on the topic of “Riemann surfaces as ringed spaces.”

Thus, with $\Gamma = \text{SL}_2(\mathbb{Z})$ acting on $\mathbb{H}$, we see that $\Gamma \backslash \mathbb{H}$ is a Hausdorff topological space. If $\Gamma$, a discrete subgroup of $\text{SL}_2(\mathbb{R})$, or $\Gamma/\{\pm I\}$ acts freely on $\mathbb{H}$ (meaning that $\text{Stab}_\Gamma(x) = \{e\}$ for all $x \in \mathbb{H}$), then there is a unique complex structure on $\Gamma \backslash \mathbb{H}$ such that, for any open set $U \subseteq \mathbb{H}$, a function $f$ is holomorphic on $U$ if and only if $f \circ p$ is holomorphic on $\Gamma \backslash \mathbb{H}$, where $p : \mathbb{H} \to \Gamma \backslash \mathbb{H}$.

In our case, the group $\Gamma(1) = \text{SL}_2(\mathbb{Z})$ does not act freely on $\mathbb{H}$; however, we will still get a complex structure on $\Gamma \backslash \mathbb{H}$, and so we are motivated to study stabilizers. To do this, we want to:

1. Investigate $\text{Aut}(\mathbb{H})$;

2. Classify fractional linear transformations and study their fixed points; and

3. Find a fundamental domain for $\Gamma(1)$, and give it a complex structure.

Later, we will perform the same task for $\Gamma(N)$.

Aside: We take a moment to investigate the unusual origins of the fractional linear transformations. Consider the action of $\text{GL}_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$; this is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = \begin{pmatrix} az_0 + bz_1 \\ cz_0 + dz_1 \end{pmatrix}.$$ 

Suppose now that $\phi$ is one of the two standard charts on $\mathbb{P}^1(\mathbb{C})$, so that

$$\mathbb{C} \xrightarrow{\phi^{-1}} \mathbb{P}^1(\mathbb{C}) \setminus \{\text{pt.}\} \xrightarrow{\phi} \mathbb{C};$$
then, writing $z \in \mathbb{C}$ as $z_0/z_1$, we have

$$
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az_0 + b z_1}{cz_0 + d z_1} = \frac{a z + b}{c z + d},
$$

and we complete the picture by identifying the point $z_1 = 0$ with $\infty$, the “point at infinity” on the Riemann sphere.

Thus we are led to classify the fractional linear transformations

$$
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{a z + b}{c z + d}, \quad ad - bc \neq 0.
$$

Some are obvious: for $\lambda \in \mathbb{C}$, $\lambda \cdot \text{Id}$ acts trivially. Furthermore, we notice that, if $g \in \text{GL}_2(\mathbb{C})$ has fixed point $x$, then $h g h^{-1}$ has fixed point $h \cdot x$. As such, the Jordan canonical form guarantees that every linear fractional transformation is similar to one represented by one of the matrices

$$
\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}, \text{ or } \begin{pmatrix} \lambda & 0 \\ 1 & \mu \end{pmatrix}, \text{ with } \lambda \neq \mu.
$$

If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ gives rise to a linear fractional transformation similar to the first type, then we call $\gamma$ parabolic. If $\gamma$ gives rise to a linear fractional transformation similar to the second type, then we call $\gamma$ elliptic if $\lambda/\mu$ has absolute value one, hyperbolic if $\lambda = \mu$ is positive and real, and loxodromic otherwise. Typically, we will only be interested in parabolic, elliptic, and hyperbolic matrices.

Remark: Observe that the characteristic polynomial of $\gamma$ is $X^2 - \text{Tr}(\gamma) X + 1$, which has discriminant $\Delta = \text{Tr}(\gamma)^2 - 4$.

Exercise: Suppose $G = \text{SL}_2(\mathbb{C})$. Show that two non-scalar matrices are conjugate if and only if they have the same trace. Show that $\alpha \in G$ is:

1. parabolic if and only if $\text{Tr}(\alpha) = \pm 2$;
2. elliptic if and only if $\text{Tr}(\alpha) \in \mathbb{R}$ and $|\text{Tr}(\alpha)| < 2$;
3. hyperbolic if and only if $\text{Tr}(\alpha) \in \mathbb{R}$ and $|\text{Tr}(\alpha)| > 2$;
4. loxodromic if and only if $\text{Tr}(\alpha) \notin \mathbb{R}$.
If instead $G = \text{SL}_2(\mathbb{R})$, show that $\alpha \in G$ is parabolic if and only if it has a single fixed point on $\mathbb{R} \cup \{\infty\}$.

We remark on the usefulness of giving many perspectives on the objects that we work with. For instance, a fixed point on $\mathbb{P}^1(\mathbb{C})$ corresponds to a fixed line in $\mathbb{C}^2$, i.e., and eigenvector for the action of $\text{GL}_2(\mathbb{C})$ described above. The matrix $\begin{pmatrix} \lambda & 1 \\ \lambda & \end{pmatrix}$ has only one such eigenvector, up to scaling. In the case of a hyperbolic matrix $\begin{pmatrix} \lambda & \\ & \mu \end{pmatrix}$ with $\lambda, \mu \in \mathbb{R}$, we have two fixed points in $\mathbb{R}$. In the elliptic case, we have two eigenvectors which are complex conjugates; that is, there is a single fixed point in $\mathbb{H}$. 
3 Lecture Three

Last time, we saw that if $\Gamma \subseteq \text{SL}_2(\mathbb{R})$ is discrete (perhaps among other assumptions), then $\Gamma \backslash \mathbb{H}$ is a Hausdorff topological space, and we classified the action of an element of $\text{SL}_2(\mathbb{R})$ as elliptic, parabolic, or hyperbolic, according to their traces. Our goal today is to equip $\Gamma \backslash \mathbb{H}$ with a complex structure.

First, we will realize $\mathbb{H}$ as a quotient of $\text{SL}_2(\mathbb{R})$, and establish rigorously the fact that $\text{SL}_2(\mathbb{R})/\{\pm I\} \cong \text{Aut}(\mathbb{H})$.

where $\text{Aut}(\mathbb{H})$ denotes the set of (biholomorphic) automorphisms of $\mathbb{H}$. We will then find a fundamental domain for the action of $\text{SL}_2(\mathbb{Z})$ on $\mathbb{H}$.

**Proposition 3.1.** One has:

1. The action of $\text{SL}_2(\mathbb{R})$ on $\mathbb{H}$ is transitive.

2. There is an isomorphism $\text{SL}_2(\mathbb{R})/\{\pm I\} \cong \text{Aut}(\mathbb{H})$.

3. There is a bijection $\text{Stab}_{\text{SL}_2(\mathbb{R})}(i) = \text{SO}_2(\mathbb{R})$, where $i = \sqrt{-1}$.

4. The map $\text{SL}_2(\mathbb{R})/\text{SO}_2(\mathbb{R}) \rightarrow \mathbb{H}$ given by $[\alpha] \mapsto \alpha(i)$ is a homeomorphism.

We recall that $\text{SO}_2(\mathbb{R})$ consists of all linear transformations of $\mathbb{R}^2$ which preserve orientation and inner products, and so in particular can be written

$$\text{SO}_2(\mathbb{R}) = \{ \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} : \theta \in \mathbb{R} \}.$$

**Proof.** Let $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{R})$.

1. It suffices to show, for all $z = x + iy \in \mathbb{H}$, that there exists $\alpha \in \text{SL}_2(\mathbb{R})$ such that $\alpha \cdot i = z$. Because $y$ is assumed positive, we can take $\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \in \text{SL}_2(\mathbb{R})$, and we are done.

2. A quick calculation shows that $\text{Im}(\alpha \cdot z) = \frac{\text{Im}(z)}{|cz + d|^2}$, so there exists a homomorphism $\text{SL}_2(\mathbb{R}) \rightarrow \text{Aut}(\mathbb{H})$ which descends to a homomorphism $\text{SL}_2(\mathbb{R})/\{\pm I\} \rightarrow$
Another easy calculation shows that this latter map is injective; thus, it suffices to show that it is surjective.

Suppose $\gamma \in \text{Aut}(\mathbb{H})$; we from from above that there exists $\alpha \in \text{SL}_2(\mathbb{R})$ such that $\alpha \cdot i = \gamma \cdot i$. Thus, replacing $\gamma$ with $\gamma \circ \alpha^{-1}$, we can assume that $\gamma$ stabilizes $i$. The homomorphism $\rho(z) = \frac{z-i}{z+i}$ maps $\mathbb{H}$ to the unit disc, $i$ to 0, and the real line to the unit circle; as such, $\rho \circ \gamma \circ \rho^{-1}$ is an automorphism of the unit disc, which fixes zero. By the Schwarz lemma, it follows that $|\rho \circ \gamma \circ \rho^{-1}(z)| \leq |z|$ for all $z, |z| < 1$. The same argument applies \textit{mutatis mutandis} to the automorphism $\rho^{-1} \circ \gamma \circ \rho$, from which it follows that $|\rho \circ \gamma \circ \rho^{-1}(z)| = |z|$ whenever $|z| \leq 1$;

from this, the Schwarz lemma gives the existence of some $\lambda \in \mathbb{C}, |\lambda| = 1$ such that $\rho \circ \gamma \circ \rho^{-1}(z) = e^{2\pi i \theta} z$ for some $\theta \in \mathbb{R}$.

It follows that $\gamma \in \text{SO}_2(\mathbb{R})$.

3. This is immediate from the previous part; it can also be proven using the orbit-stabilizer theorem.

4. Because $\text{SO}_2(\mathbb{R})$ is the stabilizer of an element of a space with a continuous group action, we know it is a closed subgroup of $\text{SO}_2(\mathbb{R})$; the result now follows immediately from the associated homework problem.

\[\square\]

**Definition:** Let $\Gamma$ be a discrete subgroup of $\text{SL}_2(\mathbb{R})$. A \textbf{fundamental domain} for $\Gamma$ in $\mathbb{H}$ is a connected, open set $D$ such that:

1. For any $z \neq z' \in D$, there is no $\gamma \in \Gamma$ such that $\gamma z = z'$, and

2. One has

$$\bigcup_{\gamma \in \Gamma} \gamma \overline{D} = \mathbb{H},$$

where $\overline{D}$ is the topological closure of $D$. 8
It is a fact that a fundamental domain always exists for any discrete subgroup of \( \text{SL}_2(\mathbb{R}) \); we will prove this fact only for the congruence subgroups. Today, we will prove that there exists a fundamental domain for the action of \( \Gamma(1) \).

We note the important fact that the group \( \text{SL}_2(\mathbb{Z})/\{\pm I\} \) is generated by the elements

\[
S = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.
\]

Observe that, for \( z \in \mathbb{H} \), we have \( S \cdot z = \frac{-1}{z} \) and \( T \cdot z = z + 1 \).

**Theorem 3.2.** A fundamental domain for the action of \( \Gamma(1) \) on \( \mathbb{H} \) is given by the set

\[
D = \{ z \in \mathbb{H} : |z| > 1 \} \cap \{ z \in \mathbb{H} : -\frac{1}{2} \Re(z) < \frac{1}{2} \},
\]

whose boundary consists of the two vertical rays

\[
\{ \frac{1}{2} + iy : y > \frac{\sqrt{5}}{2} \} \quad \text{and} \quad \{ -\frac{1}{2} + iy : y > \frac{\sqrt{5}}{2} \},
\]

as well as the arc

\[
\{ e^{i\theta} : \frac{\pi}{3} < \theta < \frac{2\pi}{3} \}.
\]

Furthermore, if \( \gamma z = z' \) for some \( \gamma \in \text{SL}_2(\mathbb{Z}), z \neq z' \in \overline{D} \), then \( \Re(z) = \pm \frac{1}{2} \) and \( z' = \mp 1 \), or \( |z| = 1 \) and \( z' = S \cdot z \); in particular, if the stabilizer of \( z \) is not \( \{ \pm I \} \), then \( z = i, \rho, \) or \( \rho^2 \), where \( \rho^2 = e^{i\pi/3} \), and the respective stabilizers are \( \langle S \rangle, \langle TS \rangle \), or \( \langle ST \rangle \). Finally, \( \Gamma(1) = \langle T, S \rangle \), and \( \text{SL}_2(\mathbb{Z}) \) has presentation

\[
\text{SL}_2(\mathbb{Z}) = \langle S, T | S^2 = (ST)^3 = I \rangle;
\]

thus, \( \text{SL}_2(\mathbb{Z}) \) is the free product of two cyclic groups of prime order.

**Proof.** Let \( \Gamma' \) be the subgroup of \( \Gamma(1) \) generated by \( S \) and \( T \); we will show first that \( D \) is a fundamental domain for \( \Gamma' \).

Observe that, if \( z = x + iy \in \mathbb{H} \) and \( N \) is some fixed positive integer, then there are only finitely many pairs of integers \( (c, d) \) such that \( |cz + d| < N \). Indeed, if this is so, then \( |c| \leq \frac{N^2}{y} \) is satisfied by only finitely many integers, and the claim is now obvious. It follows from this that, in the orbit of \( z \) under \( \Gamma' \), there exists an element \( \alpha \cdot z \) with minimal imaginary part.

We now claim that there exists some \( \gamma \in \Gamma' \) and some \( z' \in \overline{D} \) such that \( \gamma z' = z \). Clearly there exists some integer \( n \in \mathbb{Z} \) such that \( -\frac{1}{2} \leq \Re(T^n)(\alpha \cdot z) \leq \frac{1}{2} \); write
$z'$ for $T^n(\alpha \cdot z)$. We must now have $|z'| \geq 1$; otherwise, we apply $S$ and we have $|Sz'| \geq 1$, and repeat (clean this up later).

Finally, let $z \neq z' \in \overline{D}$ and suppose that $\gamma \in \Gamma(1)$ has $z' = \gamma \cdot z$. Without loss of generality, we will assume $\text{Im}(z) \leq \text{Im}(z')$; then

$$|cz + d| = (cx + d)^2 + c^2y^2 \leq 1;$$

in $D$ we must have $y^2 \geq \frac{3}{4}$, and so we can only have $c = 0$ or $\pm 1$. If $c = 0$ we have $d = \pm 1$ and so $\gamma = T^{\pm 1}$, and $z, z'$ lie on the parallel rays which make up the boundary of $D$; if $c = 1$ we must have $|z + d| \leq 1$ and so $\pm 1$ and $z = \rho$ or $\rho^2$, or $d = 0$.

It remains only to show that $\Gamma' = \Gamma(1)$, and the rest of the theorem will be proven. Let $\gamma \in \Gamma(1)$ and choose $z_0 \in D$; we know from our above work that $\Gamma' \cdot \overline{D} = H$, and so there exist $\gamma' \in \Gamma'$, $z' \in \overline{D}$ such that

$$\gamma'z' = \gamma z_0.$$

Consider the point $(\gamma')^{-1}z_0 = z' \in \overline{D}$: the only way both $z_0$ and $z'$ lie in $\overline{D}$ is if $z_0$ lies on the boundary, which is not the case (clean this up later). ∎
4 Lecture Four

We briefly return to correct an error in the last lecture: we recall that the minimum value of $|cz + d|$ corresponds to the maximum value of $\text{Im}(yz)$. The element $\gamma_0$ should have been chosen to give this maximum value $\text{Im}(\gamma z_0)$.

Today we will talk about the complex structure on modular curves, and compactify the upper half-plane; we begin with two guiding examples.

Let $D$ denote the unit disc, and consider the group $\text{Aut}(D, 0)$ of automorphisms of $D$ fixing zero. As we saw last time, the Schwarz lemma implies that every element of $\text{Aut}(D, 0)$ is a rotation of the form $z \mapsto \xi z$, where $\xi \in \mathbb{C}, |\xi| = 1$. Let $\Delta$ be a finite group acting by automorphisms on $D$, assuming that no nontrivial subgroup of $\Delta$ acts trivially on $D$. Because there is an inclusion $\Delta \hookrightarrow S^1 \cong \mathbb{R}/\mathbb{Z}$, we know that $\Delta$ has to be cyclic; its image will be the group of roots of unity of some degree $m$ (say).

Let $\xi_0$ be a generator of $\Delta$; we want to place a complex structure on $\Delta \backslash D$. Equivalently, we want to determine which functions on $\Delta \backslash D$ are holomorphic. We note that the maps $z \mapsto z^m, m \in \mathbb{Z}$, are holomorphic on $D$ which are invariant under $\Delta$, and so by the universal property of quotients they descend to a “holomorphic” map on $\Delta \backslash D$.

Note that the map $\Delta \backslash D \to D, z \mapsto z^m$ is a homeomorphism. First of all, it is well-defined: $[z_1] = [z_2]$ in $\Delta \backslash D$ if and only if $z_1 = \xi_0^k z_2$ for some $k \in \mathbb{Z}$, and so $z_1^m = z_2^m$. It is also injective: if $z_1^m = z_2^m$ in $D$, then $|z_1| = |z_2|$, and so there exists some $\xi \in S^1, \xi^m = 1$ such that $z_1 = \xi z_2$, hence

$$z_1^m = \xi^m z_2^m.$$

If $z_1 = z_2 = 0$ then we are done; otherwise we must have $\xi \in \Delta$, and the claim is proven. Surjectivity is clear, and is left as an exercise.

Thus we can define a complex structure on $\Delta \backslash D$ via the atlas consisting of the single chart

$$\Delta \backslash D \to D, z \mapsto z^m,$$

where holomorphic functions on $\Delta \backslash D$ are holomorphic functions of $z^m$.

For our second example, we put

$$X = \{z \in \mathbb{C} : \text{Im}(z) > c \geq 0\},$$

and we fix $h \in \mathbb{Z}$. Let $\mathbb{Z}$ act on $X$ by translations:

$$n.z = z + nh.$$
We add to $X$ a point $\infty$, called the “point at infinity,” to get a new space $X^* = X \cup \{\infty\}$; the action of $\mathbb{Z}$ on $X$ is extended to $X^*$ via $n.\infty = \infty$. We can topologize $X^*$ as follows: for $x \in X$, a fundamental system of neighbourhoods giving its topology in $X$, and a base of neighbourhoods of $\infty$ is given by the open sets $U_N = \{\text{Im}(z) > N\}$ for $N \in \mathbb{Z}_{\geq 0}$. With this new topology, the action of $\mathbb{Z}$ on $X^*$ is continuous.

We obtain a map $q$ from $X^*$ to the open disc of radius $e^{-2\pi c/h}$ which is $\mathbb{Z}$-periodic by defining

$$q(z) = \begin{cases} e^{2\pi iz/h} & \text{if } z \neq \infty, \\ 0 & \text{if } z = \infty. \end{cases}$$

Then $q$ is in fact a homeomorphism, which we can use as the coordinate function on $\mathbb{Z}\backslash X^*$, so that again holomorphic functions on $\mathbb{Z}\backslash X^*$ are holomorphic functions of $q(z)$.

With these two examples in mind, we can now define a complex structure on $\Gamma \backslash \mathbb{H}$ and $\Gamma \backslash \mathbb{H}^*$, where $\Gamma = \text{SL}_2(\mathbb{Z})$. First, denote by $p$ the projection map $\mathbb{H} \to \Gamma \backslash \mathbb{H}$, let $P \in \Gamma \backslash \mathbb{H}$, and let $Q \in p^{-1}(P)$. If $Q$ is not an elliptic point, then $p$ is a local homeomorphism around $Q$. If $Q \sim i$ (that is, $Q$ is in the same orbit as $i$), then take $Q = i$ for simplicity. The map

$$\rho(z) := \frac{z - i}{z + i}$$

sends $\mathbb{H}$ to the unit disc and maps $i$ to $0$. If $D'$ is some neighbourhood of $0$ in the unit disc, then $D'' = \rho^{-1}(D')$ is some neighbourhood of $i$ in $\mathbb{H}$ which is invariant under the action of $S \in \Gamma, S(z) = \frac{-1}{z}$; this is to be checked as an exercise, with the hint that $\rho^{-1} \circ S \circ \rho$ is the map $z \mapsto -z$ on the unit disc. We can therefore equip $\langle S \rangle \backslash D''$ with a complex structure, with chart

$$z \mapsto \left(\frac{z - i}{z + i}\right)^2.$$

We will play the same game near the points $\rho$ and $\rho^2$ in $\mathbb{H}$: for $\rho^2$ we choose coordinate chart

$$z \mapsto \left(\frac{z + \rho^2}{z + \rho^2}\right)^3$$

which is a conformal map sending $\mathbb{H}$ to the unit disc and $\rho^2$ to $0$. The exponent of $3$ takes care of the action of $ST$, the stabilizer of $\rho^2$. 

12
We claim next that $\Gamma \backslash \mathbb{H}$ is, in fact, the Riemann sphere minus one point. More precisely, we will show that $\Gamma \backslash \mathbb{H}$ admits a one-point compactification which has the structure of a Riemann sphere.

As in example 2: let $\mathbb{H}^* = \mathbb{H} \cup \{\infty\}$ and topologize $\mathbb{H}^*$ in the same way. As in that case, we have $T \cdot \infty = \infty$, and also $S \cdot \infty = 0$ (which we will explain in a moment). The complex structure on $\Gamma \backslash \mathbb{H}^*$ is constructed in the same way as example 2 for the co-ordinate chart near $\infty$.

More precisely: a point $s \in \mathbb{R} \cup \{\infty\}$ is called a cusp for some discrete subgroup $\Gamma$ of $\text{SL}_2(\mathbb{R})$ if it is the fixed point of some (parabolic) element of $\Gamma$.

**Exercise:** The cusps of $\Gamma(1)$ are $\mathbb{Q} \cup \{\infty\}$; moreover, they all lie in the same orbit under $\Gamma(1)$.

Thus motivated, we choose instead to define $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$; then $\Gamma \backslash \mathbb{H}^*$ is compact, and has the complex structure of the Riemann sphere.

Next time, we will discuss differences that arise when we replace $\Gamma(1)$ with $\Gamma(N)$. 

13
5 Lecture Five

Last time, we closed by putting a complex structure on $\Gamma(1)\backslash \mathbb{H}^*$. Today we will do the same for $\Gamma(N)\backslash \mathbb{H}^*$, where $N$ is arbitrary.

**Proposition 5.1.** Let $\Gamma'$ be a finite-index subgroup of a discrete subgroup $\Gamma$ of $\text{SL}_2(\mathbb{R})$, let $D$ be a fundamental domain for $\Gamma$, and let $\gamma_1, \ldots, \gamma_m \in \Gamma$ be a complete set of coset representatives for cosets of $\Gamma'/\{\pm I\}$ in $\Gamma/\{\pm I\}$; then

$$D' := \bigcup_{i=1}^m \gamma_i D$$

is a fundamental domain for $\Gamma'$.

**Proof.** Exercise. \qed

It does not follow that the set $D'$ is connected, but it is possible to show that the interior of the closure of $D'$ is connected.

For the moment we will leave aside the cusps, and consider the complex structure on $\Gamma(N)\backslash \mathbb{H}$: it is that which arises from $\mathbb{H}$. Indeed, if $N > 1$, the points $i, \rho$, and $\rho^2$, which were elliptic in the case $N = 1$, are not fixed by any elements of $\Gamma(N)$ except $\{\pm I\}$, and so there are no elliptic points in the $N > 1$ case, and $\Gamma(N)$ is a normal subgroup of $\Gamma(1)$.

However, there is more than one orbit $P_1 / Q$ under $\Gamma(N)$ when $N > 1$, giving finitely many inequivalent cusps; the exact number of such cusps we will compute next time.

There is a natural covering map (with possible branch points)

$$\Gamma(N)\backslash \mathbb{H}^* \to \Gamma(1)\backslash \mathbb{H}^*$$

of the Riemann sphere by $\Gamma(N)\backslash \mathbb{H}^*$; this map is $m$-to-one, where $m = [\Gamma(1) : \Gamma(N)]$, away from branch points.

We now take an aside, per Milne, to discuss Riemann surfaces as ringed spaces. Let $k$ be a field.

**Definition:** By a ringed space is meant a pair $(X, \mathcal{O}_X)$ consisting of a topological space $X$ and a sheaf $\mathcal{O}_X$ of $k$-algebras on $X$. We recall that this means that $\mathcal{O}_X$ is a functor from the category of open subsets of $X$, whose morphisms are inclusions, to
the category of \( k \)-algebras, satisfying the sheaf axiom: If \( U = U_i U_i \) is an open cover of some open subset \( U \) of \( X \), and \( f_i \in \mathcal{O}_X(U_i) \) is a collection of sections such that
\[
f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j},
\]
for every \( i \), then there exists some unique \( f \in \mathcal{O}_X(U) \) such that \( f|_{U_i} = f_i \) for every \( i \).

For this course, we will use the following convention: If \( V \subseteq \mathbb{C} \) is open and \( U \subseteq V \) any open subset, the symbol \( \mathcal{O}_V(U) \) will denote the set of holomorphic function \( f : U \rightarrow \mathbb{C} \). The pair \( (V, \mathcal{O}_V) \) will be called the standard ringed space.

It should now be clear that to give a complex structure on a topological space \( X \) is to give a sheaf of \( \mathbb{C} \)-algebras on \( X \) satisfying the condition that there exists an open cover \( \{U_i\} \) of \( X \) such that each ringed space \( (U_i, \mathcal{O}_X|_{U_i}) \) is isomorphic to a standard ringed space. Here, \( \mathcal{O}_X|_{U_i} \) denotes the sheaf \( U \mapsto \mathcal{O}_X(U) \), when \( U \subseteq U_i \).

The next terminology we introduce will be that of differential forms. Let \( U \subseteq \mathbb{C} \) be an open subset; a differential (one)-form on \( U \) is an expression of the form \( \omega = f(z) dz \). To a (meromorphic, say) function \( f : U \rightarrow \mathbb{C} \) we associate the one-form \( \omega_f := f'(z) dz \). If \( \phi : U \rightarrow W \) is a holomorphic map between open subsets of \( \mathbb{C} \), then the pullback of the form (on \( W \)) \( \omega = f(w) dw \) is the one-form (on \( U \))
\[
\phi^*(\omega) := f(\phi(z))\phi'(z) dz.
\]
Note that, if \( U \) has \( z \)-co-ordinates and \( W \) has \( w \)-co-ordinates, then we can write
\[
dw = \phi'(z) dz.
\]

More generally: Let \( X \) be a Riemann surface and let \( (U_i, z_i) \) be a co-ordinate covering. A differential one-form on \( X \) is a collection \( (\omega_i)_i \) of differential one-forms on the subsets \( U_i \) such that, if
\[
\omega_i = f_i(z_i) dz_i \text{ and } z_i = \phi_{ij}(z_j),
\]
then \( \phi_{ij}^*(\omega_i) = \omega_j \); that is,
\[
f_j(z_j) dz_j = f_i(\phi_{ij}(z_j)) \phi_{ij}'(z_j) dz_j.
\]

Exercise: Phrase this observation as a statement of sheaves of differential forms and \( \mathcal{O}_X \)-modules.

We emphasize the contrast between the transformation of functions with that of differential forms. We mention here also the fact that a compact, complex manifold can be realized as the \( \mathbb{C} \)-points of a projective algebraic variety.
Example: What are the meromorphic functions on $S = \mathbb{P}^1(\mathbb{C})$? By Liouville’s theorem, we know that the only holomorphic functions on $S$ are constants. Working with co-ordinates makes it clear that, to be meromorphic on $S$, a function $f(z)$ on $\mathbb{C}$ must be meromorphic in $z$, and also meromorphic in $\frac{1}{z}$. From this it is clear that the only rational functions on $S$ are the rational functions.

We might ask the same question about differentials on $S$? The same analysis tells us that a meromorphic one-form on $S$ must have both $f(z)$ meromorphic and $-\frac{f(1/z)}{z^2}$ meromorphic, whenever $z \neq 0$. 
6 Lecture Six

It is a fact that a meromorphic function \( f \) on a compact Riemann surface \( X \) has the same number of poles as it has zeroes, counting multiplicity. If \( \omega \) is a one-form on \( X \), then the sum of the residues of \( \omega \) at its poles will be zero.

The sketch of the proof is as follows: one can triangulate \( X \) in such a way that no pole lies on a vertex or an edge. On each face \( F \) of the triangulation, we will have by Cauchy the equation

\[
\int_{\partial F} = 2\pi i \sum \text{poles } p \in F \text{ Res}(\omega; p). 
\]

From this, it follows that

\[
\sum \text{all poles } p \text{ Res}(\omega; p) = \frac{1}{2\pi i} \sum F \int_{\partial F} \omega. 
\]

The first statement follows from the second by setting \( \omega = \frac{df}{f} \).

**Proposition 6.1.** Let \( f \) be a non-constant, meromorphic function on a compact Riemann surface \( X \). Then \( f \) attains every value in its range exactly \( n \) times (counting multiplicity), where \( n \) is the sum of the orders of the poles of \( f \). This value is known as the **valence** of \( f \).

**Proof.** (sketch) Let \( c \in \mathbb{C} \) be a constant, and apply the previous statement to the function \( f - c \). The argument will then show, as a corollary, that the range of \( f \) must be all of \( \mathbb{C} \). \( \Box \)

Thus, the statement that \( f \) has valence \( n \) is the same as the statement that the induced map \( f : X \to S \) onto the Riemann sphere is an \( n \)-to-one algebraic cover.

**Definition:** A point \( p \in S \) is called a **ramification point** for the function \( f : X \to S \) if \( f^{-1}(p) \) contains fewer than \( n \) distinct points.

Now, recall that the meromorphic functions on \( S \) are precisely the rational functions \( \mathbb{C}(z) \).

**Proposition 6.2.** If \( X \) is some compact Riemann surface and \( f : X \to S \) is some given meromorphic function of valence \( n \), then every meromorphic function on \( X \) is the root of a polynomial of degree at most \( n \), with coefficients in \( \mathbb{C}(z) \).
Proof. (sketch) Let \( c \in S \) be a point for which \( f^{-1}(c) \) has exactly \( n \) points (that is, \( c \) is not a ramification point), and label
\[
f^{-1}(c) = \{P_1(c), \ldots, P_n(c)\}.
\]
Let \( z \in X \) be some value such that \( f(z) = c \), and let \( g : X \to \mathbb{C} \) be meromorphic. Then
\[
\prod_{i=1}^{n} (g(z) - g(P_i(c))) = 0
\]
by construction; expanding the product gives
\[
g(z)^n + r_1(c)g(z)^{n-1} + \cdots + r_n(c) = 0,
\]
where \( r_i(c) \) are (symmetric) polynomials in \( g(P_i(c)) \). Considered as functions of \( c \), therefore, we see that \( g(P_i(c)) \) and \( r_i(c) \) are both meromorphic functions on \( S \), and so in particular the \( r_i(c) \) are rational functions on \( S \). The proof now follows when we take \( c = f(z) \).

Another definition: a divisor on \( X \) is a formal finite sum of the form
\[
D = \sum_{P \in X} n_P \cdot P,
\]
where \( n_P \in \mathbb{Z} \) and \( n_P = 0 \) for all but finitely many \( P \). Denote by \( \text{Div}(X) \) the free abelian group on the points of \( X \), and define a homomorphism of groups
\[
\deg : \text{Div}(X) \to \mathbb{Z}
\]
via
\[
\deg \left( \sum_{P \in X} n_P \cdot P \right) = \sum_{P \in X} n_P.
\]
A divisor can be attached to any meromorphic function \( f \) on \( X \) via
\[
D(f) = \sum_{P \in X} \text{ord}_P(f) \cdot P;
\]
a divisor \( D \) is called principal if it equals \( D(f) \) for some meromorphic function \( f \). Our work above implies that \( \deg D(f) = 0 \) whenever \( X \) is compact. Two divisors \( D_1, D_2 \) are called linearly equivalent if \( D_1 - D_2 \) is a principal divisor, and a divisor is called effective (denoted \( D \geq 0 \)) if all its coefficients \( n_P \) are nonnegative.
Now, let $\omega$ be a differential on $X$. We can associate to $\omega$ a differential in another way, namely: for each $P \in X$ we can take a chart $(U_i, z_i)$ containing $P$ in which $\omega$ has co-ordinates $f(z_i)\, dz_i$; we then define
\[
\text{ord}_P(\omega) = \text{ord}_P(f_i).
\]
This map is well-defined: if $\phi_{ij}(z)$ is some transition function on the appropriate chart, then
\[
d\omega = \phi'_{ij}(z)f_j(z)\, dz,
\]
with $\phi'_{ij}(z) \neq 0$ anywhere.

**Fact:** If $\omega$ is a nonzero (meromorphic) differential on the compact Riemann surface $X$, then every other differential on $X$ has the form $f \cdot \omega$, where $f$ is some meromorphic function on $X$. It follows from this that all divisors on $X$ are linearly equivalent. The equivalence class of the divisor associated to $\omega$ is denoted $K$, and is called the **canonical divisor** of $X$.

For an example: when $X = \mathbb{P}^1(\mathbb{C})$, the differential $dz$ on the usual chart corresponds to the differential $dw = -\frac{dz}{z^2}$ on the chart which identifies $w = \frac{1}{z}$. This differential has a pole of order 2 at $\infty$, and so in this case we will have $K = -2 \cdot \{\infty\}$. Obviously, the canonical divisor in this case has degree 2.

**Definition:** If $D$ is a divisor on $X$, put
\[
L(D) = \{\text{meromorphic } f : X \to \mathbb{C} : \text{div}(f) + D \geq 0\} \cup \{0\};
\]
then $L(D)$ is a vector space, of finite dimension $\ell(D)$, and its dimension depends only on the linear equivalence class of $D$. We can now state the important theorem of our lecture.

**Theorem 6.3** (Riemann-Roch theorem). Let $X$ be a compact Riemann surface. There exists an integer $g \in \mathbb{Z}_{\geq 0}$ such that, for all $D \in \text{Div}(X)$, one has
\[
\ell(D) = \deg(D) + 1 - g + \ell(K - D),
\]
where $K$ is the canonical divisor of $X$.

The quantity $g$ occurring in the theorem is called the **genus** of $X$.

This theorem is very useful in certain special cases. For instance, if $\deg(D) < 0$, then $\ell(D) = 0$; indeed, $f \in L(D)$ if and only if $\text{div}(f) + D \geq 0$. But $\deg(\text{div}(f)) + \deg(D) = \deg(D) < 0$, so the divisor cannot possibly be effective.
Example: Let $D = m \cdot \{\infty\}$ on $S = \mathbb{P}^1(\mathbb{C})$, with $m > 0$. Then $\text{div}(f) + D \geq 0$ implies that the only possible pole of $f$ is at $\infty$, of order at most $m$, and so $f$ must be a polynomial of degree at most $m$; this condition is also sufficient. Thus

$$\ell(D) = m + 1 = \deg(D) + 1.$$  

We also have $K - D = -(m + 2) \cdot \{\infty\}$, so $\ell(K - D) = 0$ by the same argument; it follows that $g = 0$ works for this divisor $D$. Because all divisors on $S$ are linearly equivalent, this shows that $g = 0$ generally.

Corollaries:

1. Taking $D = 0$ gives $\ell(D) = 1$ and $L(D)$ equals the space of constant functions. In this case, Riemann-Roch yields the equation

$$1 = \ell(0) = 0 + 1 - g + \ell(K) \implies g = \ell(K).$$

From this it follows that the dimension of the space of holomorphic one-forms on a compact Riemann surface $X$ of genus $g$, is $g$ itself.

2. Taking $D = K$ gives the equation

$$\ell(K) = g = \deg(K) + 1 - g + \ell(0) \implies \deg(K) = 2g - 2.$$  

An important point in all of this discussion is this: if $X$ is a compact Riemann surface, then there exists a nonconstant meromorphic function $f : X \to S$; the corresponding statement is not true in higher dimensions.

We close with a more general topological statement: let $X$ be a topological space and let $\chi(X)$ be the Euler-Poincaré characteristic (or topological genus), which is the (well-defined) quantity

$$\chi(E) = V + F - E,$$

where $V$, $F$, and $E$ denote respectively the number of vertices, faces, and edges in a given triangulation of $X$. It is a fact that the topological genus equals the genus $g$ from the Riemann-Roch theorem, as we will see next time.
7 Lecture Seven

We finish our discussion on genus, from Friday. We saw in that lecture the statement of the Riemann-Roch theorem, and saw some examples of its computational usefulness. Today, we begin with the Riemann-Hurwitz formula.

**Theorem 7.1.** Let \( f : Y \to X \) be a holomorphic surjection of compact Riemann surfaces, that is \( m \)-to-one, counting multiplicity (that is, ramification points are permitted); assume without loss of generality that there are only finitely many ramification points. For \( P \in Y \), let \( e_P \) be the multiplicity of \( P \) in the fibre over \( F(P) \): then

\[
2g(Y) - 2 = m(2g(X) - 2) + \sum_{P \in Y} (e_P - 1),
\]

the sum taken over all points of \( Y \).

An example of the situation that arises in the theorem comes from considering the map from the unit disc \( D \) to itself, \( z \mapsto z^e \). If \( w = z^e \), then \( dw = ez^{e-1}dz \), hence

\[ f^*(dw) = ez^{e-1}dz \]

has a zero of order \( e - 1 \) at zero.

**Proof.** Choose a differential \( \omega \) on \( X \) such that \( \omega \) has no zero or pole at any ramification point of \( f \); then \( f^*\omega \) has at every pre-image of a zero or pole of \( \omega \), a zero or pole respectively of the same order. From this discussion, if we put \( D_\omega \) for the divisor associated to \( \omega \), we see that

\[
\deg(D_{f^*\omega}) = m \deg D_\omega + \sum_{\text{P over a ramification point}} (e_P - 1).
\]

The result is now immediate from the Riemann-Roch theorem. \( \square \)

Now: let \( \Gamma \subseteq \Gamma(1) \) be a discrete subgroup. Recall that \( X(\Gamma) = \Gamma \backslash \Gamma \), and the map \( p : H^* \to X(\Gamma(1)) \); let \( \phi : X(\Gamma) \to X(\Gamma(1)) \) be the induced map. Ignoring cusps, the map \( p \) ramifies only over \( p(i) \) and \( p(\rho) = p(\rho^2) \), with respective ramification
indices 2 and 3 (this is the cardinality of the stabilizer subgroup). As such, \( \phi \) can only possibly ramify at \( p(i), p(\rho) \), or at the cusps.
Theorem 7.2. Suppose $[\Gamma(1) : \Gamma] = m$. Let $v_2$ be the number of $\Gamma$-inequivalent points of order 2 in $H$, which are elliptic for $\Gamma$ (i.e., $|\text{Stab}_{\Gamma/\{\pm I\}}(z_0)| = 2$), and let $v_3$ be the corresponding number of points of order 3. Similarly, let $v_\infty$ be the number of $\Gamma$-inequivalent cusps, which is exactly the number of orbits of $\Gamma$ in $Q \cup \{\infty\}$. Then the genus of $X(\Gamma)$ is

$$g = 1 + \frac{m}{12} - \frac{v_2}{4} - \frac{v_3}{3} - \frac{v_\infty}{2}.$$ 

Proof. See Milne, pp. 37-38. \hfill \Box

If we lighten notation by writing $X(N)$ for $\Gamma(N) \backslash H^*$, then the above theorem allows us to calculate the genus of $X(N)$.

Facts:

1. One has

$$[\Gamma(1) : \Gamma(N)] = N^3 \prod_{p|N} (1 - p^{-2}),$$

the product taken over all primes $p$ which divide $N$.

2. If $N \neq 2$, then

$$[\tilde{\Gamma}(1) : \tilde{\Gamma}(N)] = \frac{1}{2} [\Gamma(1) : \Gamma(N)],$$

where $\tilde{\Gamma}(N) = \Gamma(N)/\{\pm I\}$. Moreover, $[\tilde{\Gamma}(1) : \tilde{\Gamma}(2)] = 6$.

3. Put $\mu_N = [\tilde{\Gamma}(1) : \tilde{\Gamma}(N)]$; then

$$g(X(N)) = 1 + \mu_N \frac{(N - 6)}{12N}.$$ 

The proofs are left as homework exercises.

Now: to every pair of complex numbers $\omega_1, \omega_2$ which are linearly independent over $\mathbb{R}$, we can associate the lattice $\Lambda(\omega_1, \omega_2) = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Assuming without loss of generality that the quotient $\tau = \frac{\omega_1}{\omega_2}$ has positive imaginary part, we will normalize our lattices so that we have the association

$$\Lambda(\tau) = \mathbb{Z} + \mathbb{Z} \tau.$$
We might ask when two different bases will yield the same lattice? Clearly, \((\omega_1, \omega_2)\) generates the same lattice as \((\omega'_1, \omega'_2)\) if and only if there exist integers \(a, b, c, d\) with \(ad - bc = \pm 1\), such that
\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix}.
\]
As such, we deduce that \(\Lambda(\tau) = \Lambda(\tau')\) (with \(\tau \in \mathbb{H}\)) if and only if \(\tau\) and \(\tau'\) are \(\Gamma(1)\)-equivalent. It follows that the points of \(\Gamma(1) \backslash \mathbb{H}\) are in one-to-one correspondence with the set of all lattices \(\Lambda(\tau)\).

Given a lattice \(\Lambda\), we can consider the complex torus \(\mathbb{C}/\Lambda\). This quotient inherits the structure of a Riemann surface; as we will see, different lattices will inherit different complex structures. In fact, it is possible to equip each Riemann surface \(\mathbb{C}/\Lambda(\tau)\) with the structure of an elliptic curve.

As we will see, a meromorphic function on the quotient \(\mathbb{C}/\Lambda\) corresponds to a meromorphic function on \(\mathbb{C}\) which is doubly periodic, under both generators of \(\Lambda\). The field of such functions is \(\mathbb{C}(\wp(z), \wp'(z))\), where \(\wp\) is the Weierstrass \(\wp\)-function attached to the lattice, and the functions satisfy the equation
\[
\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3,
\]
where \(g_2\) and \(g_3\) are (known) constants.
8 Lecture Eight

Let $\Gamma = \Gamma(1)$. Recall from before our identification of real manifolds

$$\Gamma \setminus \text{SL}_2(\mathbb{R}) / \text{SO}_2(\mathbb{R}) \leftrightarrow \Gamma \setminus \mathbb{H};$$

as a Riemann surface, $\Gamma \setminus \mathbb{H}$ has the structure of a Riemann sphere minus a point, and so it has the structure of an algebraic variety. We also saw a one-to-one correspondence between $\Gamma \setminus \mathbb{H}$ and the set of full-rank lattices in $\mathbb{C}$; if $\Lambda_\tau$ is the lattice in $\mathbb{C}$ generated by 1 and $\tau$, then the correspondence is given by $[\tau] \leftrightarrow \Lambda_\tau$. The quotient space $\mathbb{C}/\Lambda_\tau$ is in every case a Riemann surface of genus one. Today, we will give $\mathbb{C}/\Lambda_\tau$ the structure of an elliptic curve.

By a doubly periodic function on $\mathbb{C}$ is meant a meromorphic function $f : \mathbb{C} \to \mathbb{C}$ for which there exists a full-rank lattice $\Lambda$ in $\mathbb{C}$ such that

$$f(z + \lambda) = f(z) \text{ for all } \lambda \in \Lambda.$$

The function $f$ is said to be doubly periodic with respect to $\Lambda$. By Liouville’s theorem, the only holomorphic doubly periodic functions are constants.

**Proposition 8.1.** Let $f(z)$ be a nonzero, doubly periodic function, and let $D$ be a fundamental parallelogram such that $f$ has neither poles nor zeroes on the boundary; then

$$\sum_{P \in D} \text{ord}_P(f) = \sum_{\text{poles } p} \text{Res}(f; p) = 0,$$

and $\sum_{P \in D} \text{ord}_P(f) \cdot P \equiv 0 \text{ mod } \Lambda$.

**Proof.** We proved all but the last statement before; for this, we consider the differential $\omega = \frac{f'(z)}{f(z)}$, and apply our result [ref] from above. \qed

**Corollary:** A non-constant, doubly periodic function has at least two poles, counting multiplicity.

Given these restrictions, we will attempt to create a doubly periodic function with respect to a given lattice $\Lambda = \Lambda_\tau$. First of all: let $G$ be a finite group acting on the set $X$. A $G$-invariant function on $X$ arises from any function $f$ on $X$, via

$$h(x) := \sum_{g \in G} f(g \cdot x).$$
Indeed,

\[ h(g_0 \cdot x) = \sum_{g \in G} f(g \cdot (g_0 \cdot x)) = \sum_{g \in G} f((gg_0) \cdot x) = \sum_{g' \in G} f(g' \cdot x) = h(x), \]

where the last sum has been re-indexed via \( g' = gg_0 \); notice that the terms in the summation have been reordered. An analogous construction will therefore extend to infinite groups as long as the sum over \( g \in G \) converges absolutely. Moreover, the sum will be meromorphic if it converges absolutely and uniformly on compact sets. We will attempt this with the function \( f(z) = \frac{1}{z^2} \); define the function

\[ h(z) = \frac{1}{z^2} + \sum_{(m,n) \in \mathbb{Z}^2, (m,n) \neq (0,0)} \frac{1}{(m\tau + n + z)^2}, \]

which does not converge absolutely. However, replacing the exponent in the denominator by a 3 does give an absolutely convergent series; thus we define

\[ g'_\Lambda(z) := -2 \sum_{\lambda \in \Lambda, \lambda \neq 0} \frac{1}{(z - \omega)^3}, \]

which is meromorphic, and therefore admits an antiderivative, viz.

\[ g_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda, \lambda \neq 0} \left( \frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right). \]

This is known as the Weierstraß \( \wp \)-function.

**Fact:** Consider the map \( \mathbb{C}/\Lambda \rightarrow \mathbb{P}^2(\mathbb{C}) \) given by

\[ z \mapsto \begin{cases} (\wp(z) : \wp'(z) : 1) & \text{if } z \neq 0, \\ (0 : 1 : 0) & \text{if } z = 0. \end{cases} \]

The image of this map is the curve with equation

\[ Y^2Z = 4X - g_2XZ^2 - g_3Z^3, \]

where \( g_2 \) and \( g_3 \) are constants defined in the homework; that is, \( \wp \) satisfies the differential equation

\[ (\wp')^2 = 4\wp^3 - g_2\wp - g_3. \]
Now, let \( k \in \mathbb{N} \), and write
\[
G_k(\Lambda) = \sum_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} \lambda^{-2k};
\]
then \( G_k(z) \) gives us a function on \( \mathbb{H} \) by defining \( G_k(\tau) = G_k(\Lambda \tau) \). This function is
known as the **Eisenstein series** associated to \( \Lambda \).

**Proposition 8.2.** For \( k > 1 \), the function \( G_k(z) \) converges to a holomorphic function on \( \mathbb{H} \), and takes the value \( 2\zeta(2k) \) at \( \infty \).

**Proof.** We compute
\[
\lim_{\tau \to i\infty} \sum_{\lambda \in \Lambda} \lambda^{-2k} = \sum_{\lambda \in \Lambda} \lim_{\tau \to i\infty} \lambda^{-2k} = \sum_{(m,n) \in \mathbb{Z}^2} \lim_{\tau \to i\infty} \frac{1}{(m\tau + n)^{2k}} = \sum_{n \in \mathbb{Z}} \frac{1}{n^{2k}} = 2\zeta(2k).
\]

We will write \( g_2 = 60G_2(\Lambda) \) and \( g_3 = 140G_3(\Lambda) \).

**Theorem 8.3.** One has \( (\wp')^2 = 4\wp^3 - g_2\wp - g_3 \), and the field of \( \Lambda \)-doubly periodic functions is \( \mathbb{C}(\wp, \wp') \).

**Proof.** We prove only the last statement, leaving the first as an exercise.

Suppose \( f \) is an even, meromorphic function with a zero or pole of order \( m \) at \( z_0 \); then \( f \) also has a zero or pole of the same order at \( -z_0 \). We consider the two cases \( z_0 \equiv -z_0 \mod \Lambda \) and \( z_0 \not\equiv -z_0 \mod \Lambda \). In the first case, because the odd derivatives of \( f \) are odd functions, we get the equation
\[
f^{(2k+1)}(z) = -f^{(2k+1)}(-z),
\]
from which it follows that \( m \) is even. Then consider the function
\[
g(z) = \prod_{z_i} (\wp(z) - \wp(z_i))^{m_i} \prod_{z_i \equiv -z_i \mod \Lambda} (\wp(z) - \wp(z_i))^{m_i/2},
\]
where the first product is taken over all zeroes and poles \( z_i \) of \( f(z) \) for which \( z_i \not\equiv -z_i \mod \Lambda \); then \( f/g \) is a constant, and the result is now immediate.
As we consider elliptic curves, we will assume that the characteristic of our base field is not 2 or 3. For the moment, we will also assume our field is algebraically closed. From the Riemann-Roch theorem, we know that projective curves over that field have an associated value \( g \) (the genus). Let \( E \) be such a curve, and consider the divisor \( D = 2 \cdot \{0\} \); as usual, \( K \) denotes the canonical divisor. We know from Riemann-Roch that

\[
\deg(K) = 2g - 2,
\]

which vanishes when \( g = 1 \). We have

\[
\ell(D) = \dim\{ f : \text{div}(f) + D \geq 0 \} = \deg(D) + 1 - g + \ell(K - D).
\]

As \( g = 1 \) and \( \deg D > 0 \), this equation reduces to \( \ell(D) = \deg(D) = 2 \). It follows that the space of functions which have a pole of order at most 2 at zero, is two. One function, call it \( X \), will have a pole of order 2 at zero; another function \( Y \) has a pole of order 3. Consider the functions

\[
1, X, Y, XY, X^2, Y^2, X^3;
\]

because there are seven functions, and the dimension of \( L(6\{0\}) \) is six, we know there must be a linear relation between the functions. We will explore this further next time.
9 Lecture Nine

We continue from last time. If $\Lambda, \Lambda'$ are two full-rank matrices in $\mathbb{C}$, then we say that $\Lambda$ is \textbf{equivalent} to $\Lambda'$ and write $\Lambda \sim \Lambda'$ if there exists some $c \in \mathbb{C}^\times$ such that $\Lambda = c\Lambda'$.

\textbf{Fact:} there is a one-to-one correspondence between the set of equivalence classes of full-rank lattices in $\mathbb{C}$ and $\Gamma(1) \backslash \mathbb{H}$.

We saw last time how, given a lattice $\Lambda$, we can equip the quotient space $\mathbb{C}/\Lambda$ with the structure of a Riemann surface. It is a fact that

$$\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda' \iff \Lambda \sim \Lambda'.$$

We begin by discussing endomorphisms of the quotient $\mathbb{C}/\Lambda$, by which we mean a group homomorphism which is also holomorphic. Suppose $\Lambda'$ is a lattice satisfying

$$\alpha\Lambda \subseteq \Lambda', \text{ some } \alpha \in \mathbb{C}^\times;$$

then there is a homomorphism

$$\phi_\alpha : \mathbb{C}/\Lambda \rightarrow \mathbb{C}/\Lambda'$$

sending the class of $z$ to the class of $\alpha z$. Clearly, $\phi_\alpha([0]_\Lambda) = [0]_{\Lambda'}$.

\textbf{Proposition 9.1.} Every holomorphic map $\phi : \mathbb{C}/\Lambda \rightarrow \mathbb{C}/\Lambda'$ such that $\phi([0]_\Lambda) = [0]_{\Lambda'}$ equals $\phi_\alpha$ for some $\alpha$.

\textbf{Proof.} From topology, we know there exists a continuous function $\tilde{\phi} : \mathbb{C} \rightarrow \mathbb{C}$ satisfying $\tilde{\phi}(0) = 0$. Because the projection maps

$$\mathbb{C} \rightarrow \mathbb{C}/\Lambda \text{ and } \mathbb{C} \rightarrow \mathbb{C}/\Lambda'$$

are local isomorphisms, it follows that $\tilde{\phi}$ is holomorphic.

Take $\lambda \in \Lambda$; then $\tilde{\phi}(z + \lambda) - \tilde{\phi}(z)$ takes values in $\Lambda'$, and so by Liouville's theorem must be constant. Thus $\tilde{\phi}'$ is doubly-periodic with respect to $\Lambda$; by our work from the previous lecture, it must be a constant itself. That is, $\tilde{\phi}'(z) = \alpha z$ for some $\alpha, \beta \in \mathbb{C}$, and the result is now clear.

\textbf{Corollary:} There is an isomorphism of Riemann surfaces $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$ if and only if there exists some $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda = \Lambda'$.
Proposition 9.2. One has:

1. \( \text{End}(\mathbb{C}/\Lambda) \supseteq \mathbb{Z} \);

2. if \( \text{End}(\mathbb{C}/\Lambda) \neq \mathbb{Z} \), then there exists a quadratic extension \( K \) of \( \mathbb{Q} \) with ring of integers \( \mathcal{O}_K \), and \( \text{End}(\mathbb{C}/\Lambda) \) is a subring of \( \mathcal{O}_K \), of rank 2 over \( \mathbb{Z} \).

Proof. Write \( \Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \), and put \( \tau = \omega_1/\omega_2 \). If \( \alpha \in \mathbb{C} \) has \( \alpha\Lambda \subseteq \Lambda \), then there exist integers \( a, b, c, d \) such that

\[
\alpha \omega_1 = a\omega_1 + b\omega_2 \quad \text{and} \quad \alpha \omega_2 = c\omega_1 + d\omega_2;
\]

that is,

\[
\alpha \tau = a\tau + b \quad \text{and} \quad \alpha = c\tau + d.
\]

Thus

\[
c\tau^2 + (d - a)\tau - b = 0 = a^2 - (a + d)\alpha + (ad - bc) = 0,
\]

and the result now follows. \qed

Theorem 9.3. There are natural equivalences between any pair of the following three categories:

- The category of full-rank lattices \( \Lambda \subseteq \mathbb{C} \) whose morphisms are

\[
\text{Hom}(\Lambda, \Lambda') = \{ \alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda' \}.
\]

- The category of compact Riemann surfaces of genus 1 and distinguished basepoint 0, whose morphisms are holomorphic maps satisfying \( 0 \mapsto 0 \).

- The category of elliptic curves over \( \mathbb{C} \) with basepoint, i.e. projective, smooth algebraic curves of (algebraic) genus 1 with distinguished point 0, whose morphisms are regular maps satisfying \( 0 \mapsto 0 \).

Proof. Exercise. \qed
We have already done most of the work involved in this proof; there is a single missing ingredient, namely how elliptic curves arise from lattices, which we will discuss now. Suppose $E$ is the elliptic curve defined by the equation $y^2 = 4x^3 - g_2x - g_3$, and let $\Delta = g_2^3 - 27g_3^2$. Then, up to some multiplicative constant, we have

$$\Delta = \prod_{i \neq j} (x_i - x_j)^2 = \text{Res}(f, f'),$$

where the product is taken over all roots of the polynomial $f(x) = y^2$, and $\text{Res}$ denotes the resultant. It is a fact that $E$ is nonsingular if and only if $\Delta \neq 0$.

**Definition:** If $E$ is defined by the equation $y^2 = 4x^3 - ax - b$, define the associated $j$-invariant to be

$$j(E) = \frac{1728a^3}{\Delta}.$$

It is a fact that, if $E$ and $E'$ are two elliptic curves defined over an algebraically closed field, then $j(E) = j(E')$ if and only if $E$ and $E'$ are isomorphic. We will show now that the induced function $j : \mathbb{H} \to \mathbb{C}$ is surjective.

Recall that if $\Gamma$ is a subgroup of finite index in $\Gamma(1)$, then a **modular function** for $\Gamma$ is a function on $\mathbb{H}$ which is $\Gamma$-invariant, meromorphic, and meromorphic at the cusps, where the last condition means that the function

$$z \mapsto f(e^{2\pi iz/h})$$

is holomorphic as $z \to i\infty$. Here, $h$ is the width of the cusp at infinity, which we define to be the unique positive integer such that the stabilizer of $i\infty$ in $\Gamma$ is generated by the matrix $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$.

**Definition:** A **modular form** of weight $2k$ for $\Gamma$ is a function $f(z)$ on $\mathbb{H}$ which is holomorphic on $\mathbb{H}$, holomorphic at all cusps of $\Gamma$, and which satisfies

$$f(\gamma \cdot z) = (cz + d)^{2k} f(z)$$

(the so-called automorphy condition) for every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and $z \in \mathbb{H}$. The notion of “holomorphy at the cusps” is similarly contrived to our above construction of “meromorphy at [the cusp] infinity.”

We note that modular functions coincide exactly with the meromorphic functions on $\Gamma \backslash \mathbb{H}^*$, whereas modular forms coincide with holomorphic differentials on $\Gamma \backslash \mathbb{H}$.
Observe also that the quotient of two modular forms of a given weight is a modular function.

**Example:** Consider the Eisenstein series we introduced above; recall we defined

\[ G_{2k}(z) = \sum_{\lambda \in \Lambda_z \atop \lambda \neq 0} \frac{1}{\lambda^{2k}}. \]

An easy calculation shows that

\[ G_{2k}(\alpha z) = \alpha^{-2k} G_{2k}(z) \]

for any \( \alpha \in \mathbb{C}^\times \); then \( G_{2k}(z) \) is a weakly modular function, meaning it satisfies the automorphy condition, for the full modular group. This is an immediate consequence of the following

**Lemma:** Let \( F \) be a function on lattices of weight \( 2k \), so that

\[ F(\alpha \Lambda) = \alpha^{-2k} F(\Lambda) \]

for any \( \alpha \in \mathbb{C}^\times \); then \( f(z) := F(\Lambda z) \) is a weakly modular function of weight \( 2k \), and all weakly modular functions of weight \( 2k \) are of this form.

**Proof.** We have, for any \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \), that

\[ F(\Lambda(\omega_1, \omega_2)) = F(\Lambda(\alpha \omega_1 + b \omega_2, c \omega_1 + d \omega_2)). \]

Put \( \tau = \omega_1/\omega_2 \), and put \( f(\tau) = F(\tau, 1) = \omega_2^{2k} F(\omega_1, \omega_2) \). Then

\[
 f \left( \frac{a \tau + b}{c \tau + d} \right) = F \left( \Lambda \left( \frac{a \omega_1 + b \omega_2}{c \omega_1 + d \omega_2}, 1 \right) \right) \\
 = (c \omega_1 + d \omega_2)^{2k} F(\Lambda(\omega_1, \omega_2)) = (c \omega_1 + d \omega_2)^{2k} F(\Lambda(\omega_1, \omega_2)) \\
 = (c \omega_1 + d \omega_2)^{2k} \omega_2^{-2k} F(\Lambda(\tau, 1)) = (c \tau + d)^{2k} f(\tau),
\]

and the result is clear. \( \square \)

**Definition:** By a cusp form is meant a modular form which vanishes at every cusp. We denote by \( \mathcal{M}_k(\Gamma) \) the space of weight \( k \) modular forms for \( \Gamma \), and by \( \mathcal{S}_k(\Gamma) \) the subspace of cusp forms. Note that

\[ \mathcal{M}_k(\Gamma).\mathcal{M}_n(\Gamma) = \mathcal{M}_{k+n}(\Gamma). \]
The ring of modular forms \( \mathcal{M}(\Gamma) \) for \( \Gamma \) is therefore graded by weight:

\[
\mathcal{M}(\Gamma) = \bigoplus_k \mathcal{M}_k(\Gamma).
\]

**Example:** Recall from above the \( j \)-invariant, defined

\[
j(z) = \frac{1728g_2^3}{\Delta}, \text{ where } \Delta = g_2^3 - g_3^2.
\]

We showed \( g_2 = 60G_2 \) and \( g_3 = 140G_3 \) to be modular forms for \( \Gamma(1) \) already, of respective weight 4 and 6, from which it follows that \( \Delta \) is a modular form for \( \Gamma(1) \) of weight 12. Because the numerator is as well, we must have that \( j(z) \) is a modular function.

As we will see soon, \( \Delta \) has no zeroes on \( \mathbb{H} \) and has only a simple zero at the cusp (exercise: show that this fact implies that \( 8\xi(4)^3 - 108\xi(6)^2 = 0 \)) Thus, the \( j \)-invariant has a single pole on \( \Gamma(1) \backslash \mathbb{H}^\ast \), and so has valence 1. It follows that it takes every complex value exactly once.
10 Lecture Ten

Last time, we saw the $j$-invariant, and its isomorphism from $\Gamma(1) \backslash \mathbb{H}^*$ to the Riemann sphere. We proved almost everything, except for the fact that $\Delta(z)$ has a simple zero at $i\infty$; we will prove this today.

We begin with a warm-up calculation. Consider the meromorphic differential $\omega = f(z) \, dz$ on $\mathbb{H}$, and suppose $\Gamma \leq \Gamma(1)$ is a finite-index subgroup. When is $\omega$ invariant under the action of $\Gamma$? That is: When does $\omega$ descend to a meromorphic differential on the modular curve $\Gamma \backslash \mathbb{H}$? Write

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

so that

$$\gamma(z) = \frac{az + b}{cz + d};$$

then

$$\gamma^* \omega = f(\gamma(z)) \, d(\gamma(z)) = f(\gamma(z))(cz + d)^{-2} \, dz.$$

It follows that $\omega$ gives a differential on $\Gamma \backslash \mathbb{H}$ if and only if $f(z)$ is weakly modular of weight 2 for $\Gamma$. Therefore we have one-to-one correspondences between each of the following sets:

- the set of meromorphic modular forms on $\Gamma \backslash \mathbb{H}^*$;
- the set of meromorphic differential forms on $\mathbb{H}^*$ which are invariant under $\Gamma$;
- the set of meromorphic modular forms of weight 2 for $\Gamma$.

Now: by a $k$-fold differential on a Riemann surface is meant a formal expression in local co-ordinates of the form $\omega = f(z) \, (dz)^k$, where $k \leq 1$ is an integer. If we take new co-ordinates $u = u(z)$, then $\omega$ transforms under the co-ordinate change via

$$u^* \omega = f(u(z)) \, (du)^k = f(u(z))(u'(z))^k \, (dz)^k.$$

Note that if $\Omega$ is the sheaf of differentials on our Riemann surface, then $k$-fold differentials are sections of $\Omega^{\otimes k}$. The same analysis establishes a correspondence between the set of meromorphic modular forms of weight $2k$ for $\Gamma$, and the set of meromorphic $k$-fold differentials on $\Gamma \backslash \mathbb{H}^*$.

We note that the order of a zero or pole at $P \in \Gamma \backslash \mathbb{H}^*$ is well defined for a $k$-fold differential, because $u'(z) \neq 0$ anywhere. We might reasonably ask therefore: how
do the zeroes and poles of a modular form relate to the zeroes and poles of the corresponding differential?

**Example:** Consider the map $w$ from the unit disc $D$ to itself, defined $w(z) = z^e$; we will investigate what becomes of the differential around zero. If $f : D \to \mathbb{C}$ is any function, then $w^*(f) = f(z^e)$; so, if $f$ has Laurent series $f(w) = a_n w^n + \cdots$, it follows that

$$w^* f(z) = a_n z^{en} + \cdots$$

Thus, the order at zero of $w^* f$ is $e \text{ord}_0 (f)$. If $\omega$ is a $k$-fold differential on the codomain $D$, then $\omega = f(w) (dw)^k$ for some function $f(w)$, and so

$$\omega^* := w^* \omega = f(z^e) (d(z^e))^k = f(z^e) (ez^{e-1})^k (dz)^k;$$

thus

$$\text{ord}_0 (\omega^*) = e \text{ord}_0 (\omega) + k(e - 1).$$

**Proposition 10.1.** Let $f$ be a meromorphic modular form of weight $2k$ for some subgroup finite-index subgroup $\Gamma \leq \Gamma(1)$, and let $\omega$ be the corresponding $k$-fold differential on $\Gamma \backslash \mathbb{H}^*$. If $Q \in \mathbb{H}^*$ lies above $P \in \Gamma \backslash \mathbb{H}^*$ with multiplicity $e$, then:

1. If $Q$ is elliptic, then $\text{ord}_Q (f) = e \text{ord}_P (\omega) + k(e - 1)$;
2. If $Q$ is a cusp, then $\text{ord}_Q (f) = \text{ord}_P (\omega) + k$; and
3. In any other case, $\text{ord}_Q (f) = \text{ord}_P (\omega)$.

Recall that the *multiplicity* of $P$ above $Q$ is 1 if $Q$ is a cusp, and otherwise is the order of the stabilizer of $Q$ in $\Gamma$.

**Proof.** The first and third claim are clear in light of our calculations above; as such, it remains only to prove the second point. Consider the image of the cusp $Q$ in $\Gamma \backslash \mathbb{H}$, and let $U$ be a neighbourhood containing this cusp. A map $\Gamma \backslash \mathbb{H}$ to the punctured unit disc $D^\times$ is given by $q = q(z) = \exp(2\pi i z/h)$, as in the previous lecture. If $\omega$ is a $k$-fold differential on $D^\times$, we can write in local co-ordinates

$$\omega = g(q) (dq)^k,$$

hence $\omega^* = g(q(z)) \left( \frac{2\pi i}{h} q(z) \right)^k (dz)^k$.

The result is now obvious. \qed
We now investigate higher-weight modular forms. We know that $f \in M_{2k}(\Gamma)$ if and only if:

- $e_P \text{ord}_P(\omega_f) + k(e_P - 1) \geq 0$ for all point $P$;
- $\text{ord}_P(\omega) + k \geq 0$ at every cusp $P$; and
- $\omega_f$ is holomorphic elsewhere.

If we fix some $k$-fold differential $\omega_0$ on $\Gamma \backslash \mathbf{H}^*$; then any $\omega$ will be of the form $h(z) \cdot \omega_0$, where $h(z)$ is some meromorphic function. With this notation, our conditions above are equivalent to the conditions:

- $\text{ord}_P(h) + \text{ord}_P(\omega_0) + k(1 - 1/e_P) \geq 0$ at all elliptic points $P$;
- $\text{ord}_P(h) + \text{ord}_P(\omega_0) + k \geq 0$ at every cusp $P$; and
- $\text{ord}_P(h) + \text{ord}_P(\omega_0) \geq 0$ at every other point $P$.

We can reformulate these conditions once again to the equivalent statement: $f \in M_{2k}(\Gamma)$ if and only if $\text{div}(h) + D \geq 0$, where

$$D = \text{div}(\omega_0) + \sum_{\text{cusps}} k \cdot P_i + \sum_{\text{elliptic points}} \left[ k(1 - 1/e_P) \right] P_i,$$

and $[x]$ is the greatest integer part of $x$.

**Theorem 10.2.** Suppose $\Gamma \leq \Gamma(1)$ has finite index; then

$$\dim(M_{2k}(\Gamma)) = \begin{cases} 
0 & \text{if } k \leq -1, \\
1 & \text{if } k = 0, \\
1 - g + k(2g - 2) + k v_\infty + \sum_P [k(1 - 1/e_P)] & \text{if } k \geq 1,
\end{cases}$$

where in the last case $g$ is the genus of $X(\Gamma) = \Gamma \backslash \mathbf{H}^*$, and $v_\infty$ is the number of $\Gamma$-inequivalent cusps.

**Proof.** (sketch) We use the Riemann-Roch theorem, using the fact that $\ell(K - D) = 0$ because $\text{deg}(K - D) < 0$. 

\[\square\]
In the special case $\Gamma = \Gamma(1)$, this formula simplifies considerably: we have

$$\dim(\mathcal{M}_{2k}) = 1 - k + \left\lfloor \frac{k}{2} \right\rfloor + \left\lfloor \frac{2k}{3} \right\rfloor = \begin{cases} \left\lfloor \frac{k}{6} \right\rfloor & \text{if } k \equiv 1 \mod 6, \\ 1 + \left\lfloor \frac{k}{6} \right\rfloor & \text{if } k \not\equiv 1 \mod 6, \end{cases}$$

whenever $k \geq 0$.

This formula allows us easily to compute the dimensions of the various spaces $\mathcal{M}_{2k}$, and our previous work will give us generators.

<table>
<thead>
<tr>
<th>$k$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>weight</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>12</td>
<td>14</td>
</tr>
<tr>
<td>dimension</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>generator(s)</td>
<td>0</td>
<td>$G_2$</td>
<td>$G_3$</td>
<td>$G_2^2$</td>
<td>$G_2G_3$</td>
<td>$G_3^2$, $G_3^2$</td>
<td>$G_2^2G_3$</td>
</tr>
</tbody>
</table>

Indeed, it may be shown that, as a ring, $\mathcal{M}_{2k}$ is generated by $G_2$ and $G_3$.

We close with a few words on the zeroes of modular forms. With $\deg(D) = k(2g-2)$, we have

$$\sum_Q \left( \text{ord}_Q(f) \frac{1}{e_Q} - k(1 - \frac{1}{e_Q}) \right) = k(2g-2) + kv_\infty$$

where the sum is taken over a set of representatives $Q$ of zeroes, poles, and cusps of $f$ in $\Gamma \backslash \mathbb{H}$. For $\Gamma(1)$, this becomes

$$\text{ord}_i(f) + \frac{1}{2} \text{ord}_i(f) + \frac{1}{3} \text{ord}_\rho(f) + \sum_Q \text{ord}_Q(f) = \frac{k}{6},$$

where the sum is taken over the set of all points $Q$ on the interior of a fundamental domain for $\Gamma(1)$. For $G_2$, we have a simple pole at $\rho$, and no others; for $G_3$, we have a simple zero at $i$, and no others; for $\Delta$, which has no zero in $\mathbb{H}$, has a simple zero at $i\infty$. 

36
11 Lecture Eleven

Recall that, at the end of the last lecture, we calculated the dimensions of \( \mathcal{M}_{2k} = \mathcal{M}_{2k}(\Gamma(1)) \). Today, we will show that

\[
\mathcal{M} := \bigoplus_{k \geq 1} \mathcal{M}_{2k} = \mathbb{C}[G_2, G_3],
\]

where \( G_2 \) and \( G_3 \) are the Eisenstein series from before.

**Lemma 1.** The map \( f \mapsto f\Delta \) is an isomorphism of \( \mathcal{M}_{2k} \) onto \( \mathcal{S}_{2k+12} \).

**Proof.** That this map is a homomorphism is clear, and injectivity is similarly obvious; thus it suffices to show surjectivity. Let \( g \in \mathcal{S}_{2k+12} \), and consider the quotient \( \frac{g}{\Delta} \); because \( \Delta \) has no zeroes in \( \mathbb{H} \) and has only a simple zero at \( i\infty \), it is easy to see that \( \frac{g}{\Delta} \in \mathcal{M}_{2k} \). This completes the proof. \( \square \)

This lemma will make it easy to prove that \( G_2 \) and \( G_3 \) generate \( \mathcal{M} \). We will use induction on \( k \), the cases \( k \leq 6 \) having already been established. If \( k > 6 \), we will write \( k = 2n + 3m \) (with \( m, n \geq 0 \)) and consider the modular form \( h = G_2^n G_3^m \), which has weight \( 2k \). It is nonzero at \( i\infty \); in fact, it can be shown that its value there is

\[
(2\zeta(4))^n (2\zeta(6))^m \neq 0.
\]

Now, for any \( f \in \mathcal{M}_{2k} \), we will put

\[
\tilde{f} = f - \frac{f(i\infty)}{h(i\infty)} h \in \mathbb{C}[G_2, G_3].
\]

And this... completes the proof? (Clean this up)

We now want to prove that \( G_2 \) and \( G_3 \) are algebraically independent; we will do this by proving directly that \( G_2^2 \) and \( G_3^2 \) are algebraically independent, from which our desired result will follow. We begin with another

**Lemma 2.** Let \( f, g \in \mathcal{M}_{2k} \); then either \( f \) and \( g \) are proportional, or they are algebraically independent.

We know that \( G_2 \) vanishes at \( \rho \) while \( G_3 \) does not.
Proof. Suppose \( P(f, g) = 0 \) for some polynomial \( P(X, Y) \in \mathbb{C}[X, Y] \), and write \( P_d \) for the degree \( d \) homogeneous component of \( P \); then \( P_d(f, g) \) is a modular form of weight \( dk \). Writing
\[
P = \sum_{d \geq 0} P_d,
\]
we see that \( P_d(f, g) = 0 \) for every \( d \). We define a function of a single variable via
\[
p(f/g) := \frac{P_d(f, g)}{g^d},
\]
which must then be identically zero as well. Because \( p \) is a nonconstant polynomial, it follows that we must have that \( f/g \) is a constant, and so \( f \) and \( g \) are proportional, as claimed.

We remark here that our \( j \)-invariant from before, defined
\[
j(z) = \frac{1728g_2^3(z)}{\Delta(z)},
\]
gives an isomorphism \( \Gamma(1) \backslash \mathbb{H}^* \to S \), where \( S \) is the unit sphere. Indeed: \( j \) is the unique isomorphism \( \Gamma(1) \backslash \mathbb{H}^* \to S \) satisfying
\[
j(i) = 1728, j(p) = 0, j(i \infty) = \infty.
\]
We now discuss Fourier expansions. Suppose \( \Gamma \leq \Gamma(1) \) has finite index, and recall the generator \( T \in \Gamma(1) \). For some positive integer \( h \) (the width of the cusp, defined above), we will have \( T^h \in \Gamma \), and so we have for any modular form \( f \in \mathcal{M}_{2k}(\Gamma) \) the identity
\[
f(z + h) = f(z),
\]
and so \( f \) is periodic with period \( h \). It follows that we can take its Fourier series expansion. For the moment, we restrict our attention to \( \Gamma = \Gamma(1) \). Writing \( q = \exp(2\pi i z) \) as before, we will obtain the series expansion
\[
f(z) = \sum_{n \geq 0} a_n q^n,
\]
for some \( a_n \in \mathbb{C} \); that the series has nonnegative coefficients follows from the holomorphy of \( f \) at the cusp. We will compute the Fourier series expansion for \( G_{2k} \).
We have the identity

$$\pi \cot(\pi z) = \lim_{N \to \infty} \sum_{n=-N}^{N} \frac{1}{z+n};$$

we call the expression on the right the *principal value* of the (not absolutely convergent) series \( \sum_{n \in \mathbb{Z}} (z+n)^{-1} \); thus

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \left( \frac{1}{z+n} + \frac{1}{z-n} \right) = \frac{1}{z} + 2 \sum_{n=1}^{\infty} \frac{z}{z^2-n^2}. $$

We have also the Weierstrass factorization

$$\sin(\pi x) = \pi x \prod_{n=1}^{\infty} \left( 1 - \frac{x^2}{n^2} \right);$$

in fact, the first identity is a consequence of the second, by taking logarithmic derivatives.

We will prove the first identity: \( \pi \cot(\pi z) \) has simple poles (with residue one) at all integers, and nowhere else. The series

$$\frac{1}{z} + \sum_{n=1}^{\infty} \left( \frac{1}{z+n} + \frac{1}{z-n} \right)$$

also has simple poles with residue one at each integer. Moreover, both functions are clearly periodic, with period one, and are holomorphic away from the poles; it may also be shown that both functions are bounded in vertical strips. It follows that their difference is holomorphic on all of \( \mathbb{C} \), which is bounded everywhere, and must therefore be a constant. The value of this constant is shown to be zero by evaluating both functions at \( \frac{1}{2} \).

Now: an easy calculation (left as an exercise) shows that

$$\cot(z) = i \frac{e^{2iz} + 1}{e^{2iz} - 1} = i + \frac{2i}{e^{2iz} - 1}. $$

**Proposition 11.1.** For \( k \geq 2 \), one has

$$G_k(z) = 2\zeta(2k) + 2 \frac{(2\pi)^{2k}}{(2k-1)!} \sum_{n \geq 1} \sigma_{2k-1}(n) q^n, $$

where \( \sigma_\ell(n) \) is the \( \ell \)-th power sum-of-divisors function

$$\sigma_\ell(n) = \sum_{d \mid n} d^\ell.$$
Proof. We have

\[
\pi \cot(\pi z) = \pi i - 2\pi i \sum_{n=1}^{\infty} \frac{q^n}{z} = \frac{1}{z} + \sum_{n=1}^{\infty} \left( \frac{1}{z+n} + \frac{1}{z-n} \right);
\]

differentiating both sides \(k-1\) times (with respect to \(z\)) gives

\[
\frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^n = \sum_{n \in \mathbb{Z}} \frac{1}{(n+z)^k}.
\]

Thus

\[
G_k(z) = \sum_{(m,n) \neq (0,0)} \frac{1}{(mz+n)^{2k}} = 2\zeta(2k) + 2 \sum_{n=1}^{\infty} \sum_{m \in \mathbb{Z}} \frac{1}{(n+zm)^{2k}},
\]

\[
= \frac{(-2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} m^{2k-1} q^{mn} = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} m^{2k-1} q^{mn};
\]

careful rearrangement of the last series then yield the result.

We close with an application. Define constants \(B_k\) by the equation

\[
\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{x^{2k}}{(2k)!};
\]

then Euler was able to show

\[
\zeta(2k) = \frac{2^{2k-1}}{(2k)!} B_k \pi^{2k}.
\]
12 Lecture Twelve

Last time, we closed by introducing the Bernoulli numbers and evaluating the Riemann zeta function at even positive integers. It is an easy consequence of the proposition that closed the last lecture, that \( \frac{1}{2\pi i} G_k \) has rational Fourier coefficients; with more work, it can be shown that

\[
\Delta(z) = (2\pi)^{12}(q - 24q^2 + 252q^3 - 1472q^4 + \cdots)
\]

In fact, it may be shown that \( \Delta \) admits an infinite product factorization: as we will prove later,

\[
\Delta(z) = (2\pi)^{12}q \prod_{n=1}^{\infty} (1 - q^n)^{24},
\]

which itself proves that \( \frac{\Delta}{(2\pi)^{12}} \) has integer Fourier coefficients.

**Definition:** the Ramanujan \( \tau \)-function is the arithmetic function \( \tau : \mathbb{N} \to \mathbb{C} \) defined by

\[
\Delta(z) = (2\pi)^{12}q \prod_{n=1}^{\infty} \tau(n)q^n.
\]

Ramanujan conjectured several properties of the \( \tau \)-function:

- it is multiplicative; that is, \( \tau(mn) = \tau(m)\tau(n) \) if \( (m, n) = 1 \);
- if \( p \) is a prime and \( k \geq 1 \), then \( \tau(p^{k+1}) = \tau(p)\tau(p^k) - p^1\tau(p^{k-1}) \); and
- if \( p \) is prime, then \( |\tau(p)| \leq 2p^{11/2} \).

None of these facts are obviously true from the definition of the function. The first two conjectures were proven by Mordell in 1917; the last was proven by Deligne in 1976, as part of his proof of the Weil conjectures.

To \( \tau \), and other functions more generally, we can associate a series. Indeed, if \( f \) is a modular form with Fourier expansion

\[
f(z) = \sum_{n=0}^{\infty} a_n q^n,
\]

then we can define a Dirichlet series

\[
L_f(s) = \sum_{n=0}^{\infty} \frac{a_n}{n^s};
\]
bounds on the coefficients \(a_n\) can then be found by investigating the analytic properties of \(L_f\). The Shimura-Taniyama-Weil conjecture (now proven) provides a correspondence between such \(L\)-functions and the zeta function \(\zeta_E\) attached to elliptic curves over finite fields; the conjectured properties of such \(\zeta_E\) were ultimately proven by Wiles in his proof of Fermat’s last theorem. We hope to focus on the details of this work during the remainder of the course.

For the moment, consider our modular function \(j = \frac{1728g_2^3}{\Delta}\) as a formal power series in \(q\); we know
\[
\Delta(z) = (2\pi)^{12}q(1 + \cdots),
\]
and similarly that
\[
g_2^3(z) = (2\pi)^{12}(1 + \cdots),
\]
from which it follows that
\[
\frac{1728g_2^3}{\Delta} = q^{-1} + c + \cdots
\]
for some constant \(c\). In fact, the first few coefficients are known:
\[
j(z) = q^{-1} + 744 + 196884q + \cdots
\]

Of course, we observe that 196884 is one greater than the dimension of the smallest nontrivial irreducible representation of the Monster group.

Recall the correspondence we established between \(Y(1)\), i.e. the affine modular curve \(\Gamma(1)\backslash \mathcal{H}\), and the set of equivalence classes of elliptic curves over \(\mathbb{C}\); namely, \(j^{-1}\). If \(L/\mathbb{Q}\) is an algebraic extension of \(\mathbb{Q}\) in \(\mathbb{C}\), and an elliptic curve \(E\) is defined by the equation
\[
y^2 = 4x^3 - ax - b,
\]
with \(a, b \in L\), then the restriction of \(j^{-1}\) to the set of (equivalence classes of) elliptic curves defined over \(L\) defines a bijection onto the set \(Y(1)(L)\) of \(L\)-points of \(Y(1)\). If we take \(\tau \in \mathcal{H}\) with \([\mathbb{Q}(\tau) : \mathbb{Q}] = 2\), then it will follow from these observations that \(j(\tau) \in \mathbb{Q}(\tau)\).

**Theorem 12.1.** Let \(\tau \in \mathcal{H}\) be a quadratic irrational number; then \(j(\tau)\) is algebraic, and \(\tau\) together with \(j(\tau)\) generates the Hilbert class field of \(\mathbb{Q}(\tau)\). That is, \([\mathbb{Q}(\tau, j(\tau)) : \mathbb{Q}] = 2h\), where \(h\) is the class number of \(\mathbb{Q}(\tau)\).

**Proof.** Omitted. \(\square\)
In fact, more can be said: suppose we know that, for some particular \( \tau \in \mathbb{H} \), the value \( j(\tau) \) is algebraic; then \( \tau \) is itself imaginary quadratic.

We pause now to see how the \( j \)-invariant helps us to approximate \( \pi \): if \( L = \mathbb{Q}(\tau) \) is some quadratic extension with class number 1, then \( j(\tau) \in \mathbb{Q} \); for instance, if \( \tau = \frac{1+i\sqrt{163}}{2} \), then

\[
q = \exp(2\pi i \tau) = \exp(i\pi - \pi \sqrt{163}) = -e^{-\pi \sqrt{163}},
\]

and so \( j(\tau) = q^{-1} + 744 + q + \cdots \approx 744 + q^{-1} \). Apparently, this... lets us approximate \( \pi \)?

What we want to prove now is the following: the function

\[
f(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}
\]

is a cusp form of weight 12, and so the product is absolutely convergent everywhere on \( \mathbb{H} \). Observe that \( z \in \mathbb{H} \) implies \( |q| < 1 \), and therefore that \( f(z) \) converges absolutely on \( \mathbb{H} \), and it suffices to check the transformation property. Periodicity is clear, and it remains only to check that \( f(-1/z) = z^{12} f(z) \).

At the same time, we will consider the “quasi-Eisenstein series”

\[
G_1(z) = \sum_{n \geq 1} \frac{1}{n^{2k}} + \sum_{m \neq 0} \frac{1}{(mz + n)^2};
\]

this series converges, but not absolutely, for \( z \in \mathbb{H} \). We avoid this problem by redefining \( G_1 \) according to the general Fourier expansion of \( G_k \) we found before:

\[
G_1(z) = (2\pi i)^2 \left( -\frac{B_1}{4} + \sum_{n=1}^{\infty} \sigma(n)q^n \right),
\]

which has constant term \( \xi(2) = \frac{\pi^2}{6} \). We simplify notation by defining generally:

\[
E_k = \frac{1}{G_k(0)} G_k;
\]

then \( E_k(z) \) has constant term 1.

**Proposition 12.2.** For any \( a, b, c, d \in \mathbb{Z} \) with \( ad - bc = 1 \), we have

\[
G_1 \left( \frac{az + b}{cz + d} \right) = (cz + d)^2 G_1(z) - \pi ic(cz + d).
\]
We will consider the proof next time. With this knowledge in hand, however, we can compute
\[
\frac{1}{2\pi i} \log f(z) = 1 - 24 \sum_{n=1}^{\infty} \frac{ne^{2\pi i n z}}{1 - e^{2\pi i n z}} = E_1(z).
\]
13 Lecture Thirteen

Today we will introduce the Petersson inner product. We begin by placing a metric on $H$.

Recall that $H$ is isomorphic to the Poincaré disc $D$; this is the open unit disc, whose geometry is given by the Euclidean axioms, apart from the parallel postulate, which is replaced by the axiom:

- Given a line $L$ and a point $p$ not on $L$, there exist more than one line passing through $p$ which do not meet $L$.

The resulting geometry has, for its straight lines, all diameters of the disc, as well as all arcs of Euclidean circles contained in $D$, which are orthogonal to the boundary of $D$. We then transform this under the correct Möbius transformation to obtain the metric on $H$.

Alternatively, we can define the geometry on $H$ by defining its metric. For $z_1, z_2 \in H$, let $\infty_1, \infty_2$ be the points on $\mathbb{R}$ which intersect the (hyperbolic) line joining $z_1$ and $z_2$; assume without loss of generality that the points can be traversed in the order $\infty_1, z_1, z_2, \infty_2$. Define the cross-ratio of $z_1, z_2, z_3, z_4$ to be

$$D(z_1, z_2, z_3, z_4) = \frac{(z_1 - z_3)(z_2 - z_4)}{(z_2 - z_3)(z_1 - z_4)};$$

we can then define the metric on $H$ via

$$d(z_1, z_2) = \log D(z_1, z_2, \infty_1, \infty_2)$$

(a simple calculation shows that $D(z_1, z_2, \infty_1, \infty_2)$ is real and positive). Locally, the measure on $H$ is given by

$$ds^2 = \frac{dx^2 + dy^2}{y^2},$$

considered as a real manifold. The group $\text{PSL}_2(\mathbb{R})$ acts naturally on this manifold, and the cross-ratio is invariant under this transformation. The corresponding $\text{PSL}_2(\mathbb{R})$-invariant volume form on $H$ is $\frac{dx dy}{y^2}$; this follows (as an exercise) from the isomorphism

$$\text{SL}_2(\mathbb{R}) = NAK,$$

where $K = \text{SO}_2(\mathbb{R})$, $A$ is the subgroup of diagonal matrices, and $N$ is the subgroup of upper- (or lower-) triangular matrices.
With this volume form, we can compute the (finite) volume of $\Gamma \backslash \mathbb{H}$: for $\Gamma = \Gamma(1)$, we have

$$\text{vol}(\Gamma(1) \backslash \mathbb{H}) = \int_D \frac{dx \, dy}{y^2} = \int_{-1/2}^{1/2} \int_{\sqrt{1-x^2}}^{\infty} \frac{dy}{y^2} \, dx = [\arcsin(x)]_{x=-1/2}^{1/2} = \frac{\pi}{3}.$$ 

For more general $\Gamma$, we have by Stokes’ theorem (exercise)

$$\int_{\Gamma \backslash \mathbb{H}} \frac{dx \, dy}{y^2} = 2\pi \left( 2g - 2 + v_\infty + \sum_p (1 - 1/e_p) \right).$$

Moreover, if $f$ is a modular form of weight $2k$ for $\Gamma$, then the number of zeroes of $f$ counted with multiplicity equals $\frac{k \text{vol}(\Gamma \backslash \mathbb{H})}{4\pi}$. We remark that the ubiquitous factor $\frac{1}{12}$ appears here as the quotient of $\text{vol}(\Gamma(1) \backslash \mathbb{H})$ by $4\pi$, i.e. the normalized volume of the 2-sphere.

We will now place an inner product on the space $\mathcal{M}_{2k}(\Gamma)$, for some arbitrary finite-index subgroup $\Gamma$ of $\Gamma(1)$.

**Proposition 13.1.** Let $z = x + iy$, and suppose $f, g \in \mathcal{M}_{2k}(\Gamma)$; then

$$f(z)\overline{g(z)} y^{2k-2} dx \, dy = f(z)\overline{g(z)} \text{Im}(z)^{2k-2} dx \, dy$$

is invariant under the transformation $z \mapsto \gamma z, \gamma \in \Gamma$.

**Proof.** For $\gamma \in \Gamma$, write $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$; then

$$\text{Im}(\gamma z) = \frac{1}{|cz + d|^2} \text{Im}(z),$$

and since

$$\frac{d}{dz}(\gamma z) = \frac{1}{(cz + d)^2},$$

we know that

$$f(\gamma z) = (cz + d)^{2k} f(z), \quad g(\gamma z) = (cz + d)^{2k} g(z).$$

An easy calculation (exercise; see p. 64 in Milne) shows that

$$\gamma^*(dx \, dy) = \frac{dx \, dy}{|cz + d|^4}.$$ 

The result is now immediate. \qed
We remark that the case $k = 0$ and $f = g = 1$ gives a proof of the invariance of the metric $\frac{dx \, dy}{y^2}$.

**Proposition 13.2.** If $f$ is a cusp form for $\Gamma(1)$, then

$$|f(x + iy)| = O(e^{-2\pi y})$$

as $y \to \infty$.

*Proof.* (sketch) We use the Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a_n q^n,$$

with $q = \exp(2\pi i z) = \exp(-2\pi y) \exp(2\pi i x)$. The absolute value of the dominant term is thus clearly $\exp(-2\pi y)$.

A more general result exists for cusp forms of arbitrary level, which we will see later. Retaining the above notation for the Fourier expansion, we can also obtain growth estimates for the coefficients $a_n$.

**Proposition 13.3.** If $f$ is a cusp form of weight $2k$ for $\Gamma(1)$, then

$$|a_n| \leq cn^k$$

for some (absolute) constant $c$.

*Proof.* It is clear from our above remarks that the map $z \mapsto |f(z)|(\text{Im} z)^k$ is $\Gamma(1)$-invariant, and therefore bounded on $\mathbb{H}$. It follows that there exists a constant $c$ such that

$$|f(z)| \leq \frac{c}{y^k} \text{ for all } z = x + iy \in \mathbb{H}.$$

We compute the Fourier coefficients by the definition: we have

$$e^{-2\pi ny} a_n = \int_0^1 f(x + iy)e^{-2\pi inx} \, dx,$$

and taking $y = \frac{1}{n}$ gives

$$e^{-2\pi |a_n|} = \left| \int_0^1 f(x + i/n)e^{2\pi inx} \right|.$$

The integrand is dominated by $\frac{c}{y^2}$, as remarked above, and so the left-hand side is dominated by $cn^k$. \qed

47
Now: we define the Petersson inner product of \( f, g \in \mathcal{M}_2k(\Gamma) \) by the formula

\[
\langle f, g \rangle = \int_D f(z)\overline{g(z)}y^{2k-2}dx\,dy,
\]

where \( D \) is a fundamental domain for the action of \( \Gamma \) on \( \mathbb{H} \), and one of \( f, g \) is a cusp form.

**Proposition 13.4.** The Petersson inner-product is a positive-definite Hermitian product; thus, \( \mathcal{M}_{2k}(\Gamma) \) is a finite-dimensional Hilbert space.

Tomorrow, we will discuss Hecke operators.
14 Lecture Fourteen

Today, we define the Hecke operators. Recall that we have already seen the relationship between modular forms and functions on lattices; we will define operators on lattices, and thereby obtain an action on modular forms. Let \( \mathcal{D} \) be the free abelian group on the set of full-rank lattices

\[
\Lambda(\omega_1, \omega_2) = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2;
\]

an element of \( \mathcal{D} \) therefore can be written

\[
\sum_{i=1}^{m} n_i[\Lambda_i],
\]

with \( n_i \in \mathbb{Z} \). We remark that \([\Lambda]\) is not an equivalence class, and that this notation is used only to emphasize the lattice \( \Lambda \) as an element of \( \mathcal{D} \).

**Definition:** for \( n \in \mathbb{N} \), define the operator

\[
T(n) : \mathcal{D} \to \mathcal{D}
\]

by the formula

\[
T(n)([\Lambda]) = \sum_{\substack{\Lambda' \subseteq \Lambda \\ [\Lambda : \Lambda'] = n}} [\Lambda'].
\]

We also define the operator \( R(n) : \mathcal{D} \to \mathcal{D} \) via \( R(n)([\Lambda]) = [n\Lambda] \).

**Proposition 14.1.** Let \( T(n), R(n) \) be as above; then

- one has \( T(m) \circ T(n) = T(mn) \) if \( (m, n) = 1 \); and
- if \( p \) is a prime and \( n \geq 1 \), then

\[
T(p^n) \circ T(p) = T(p^{n+1}) + pR(p) \circ T(p^{n-1}).
\]

We remark that an immediate corollary of this proposition is the fact that the \( T(p) \) (with \( p \) prime) generate the same algebra as \( \{T(n)\} \).

**Proof.** By the correspondence theorem, every index \( mn \) sublattice is an index sublattice of a unique index \( m \) sublattice, when \( m \) and \( n \) are coprime. From this, we deduce that

\[
\Lambda/\Lambda' \cong \mathbb{Z}/(mn)\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z} ) \oplus (\mathbb{Z}/n\mathbb{Z}),
\]
and the result now follows. For the second point: we know that both left- and right-hand sides are formal sums of sublattices of index $p^{n+1}$. If $\Lambda'$ is an index $p^{n+1}$ sublattice of $\Lambda$, we can compare its multiplicities on both sides of the equation.

In the first case, we have $\Lambda' \subseteq p\Lambda = R(p)([\Lambda])$; we know $[\Lambda : p\Lambda] = p^2$. So on the right-hand side, $\Lambda'$ occurs with multiplicity $p + 1$. On the left-hand side, because $\Lambda'$ is contained in $p\Lambda$, it must lie in every sublattice of index $p$. Therefore, the multiplicity of $\Lambda'$ on the left-hand side is the number of sublattices of index $p$ in $\Lambda$; we have

$$\Lambda / p\Lambda \cong \mathbb{Z} / p\mathbb{Z} \oplus \mathbb{Z} / p\mathbb{Z} \cong \mathbb{F}_p^2.$$  

The number of sublattices of index $p$ in $\Lambda$ is precisely the number of lines in $\mathbb{F}_p^2$, which is exactly

$$\frac{p^2 - 1}{p - 1} = p + 1,$$

and the fact is proven.

In the second case, when $\Lambda' \not\subseteq p\Lambda$, then $\Lambda'$ appears not at all in the second term on the right-hand side, and with multiplicity one in the first term. On the left-hand side, we claim that there is only a single index $p$ sublattice of $\Lambda$ which contains $\Lambda'$; indeed, suppose $\Lambda_1, \Lambda_2$ both contain $\Lambda'$; then

$$\Lambda' \subseteq \Lambda_1 \cap \Lambda_2 = p\Lambda,$$

which is a contradiction, and the result is proven.

We remark that $R(p)$ and $T(p)$ commute for every prime $p$, and also that $T(p^n)$ and $T(p)$ commute for every $p$. It follows that the algebra generated by the $T(n)$ is commutative. Today, we will build an algebra of Hecke operators acting on $M_k(\Gamma(1))$ for every $k$; in general, this can be done for arbitrary subgroups.

For the rest of this lecture, we fix $\Gamma = \Gamma(1)$. Recall that we established a correspondence between weakly modular functions $f(z)$ of weight $2k$, and weighted functions on lattices $F(\Lambda), F(\lambda\Lambda) = \lambda^{-2k} F(\Lambda)$. If $T$ is an operator on lattices, define the action of $T$ on the set of functions of lattices via

$$(T \cdot F)(\Lambda) = F(T(\Lambda));$$

then

$$T(n) \cdot F = \sum_{\Lambda' \subseteq \Lambda} F(\Lambda') \text{ and } R(n) \cdot F = n^{-2k} F.$$
We will continue to normalize our lattices so that one generator is 1, and the other has positive imaginary part:

$$\Lambda(\omega_1, \omega_2) = \Lambda\left(1, \frac{\omega_1}{\omega_2}\right) = \Lambda(1, z) =: \Lambda_z.$$ 

To the weakly modular function $f$ we define the function $F$ on lattices by the formula $F(\Lambda_z) = f(z)$; it is an exercise to show that this is well-defined.

**Definition:** Define the action of Hecke operators $T(n)$ on the set of weakly modular functions $f$ by the equation

$$T(n) \cdot f(z) := n^{2k-1} T(n) \cdot F(\Lambda_z).$$

It is easy to check that $T(n) \cdot f$ is also weakly modular of weight $2k$.

Now, we claim that

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

where the sum is taken over all triples $(a, b, d)$ such that

$$ad = n, a \geq 1, \text{ and } 0 \leq b < d.$$ 

We give a rough justification: the formula arises from an explicit description of sub-lattices of $\Lambda$ of index $n$. Such a lattice is the image of $\Lambda$ under the action of some element $\gamma \in M_2(\mathbb{Z})$ of determinant $\pm n$. It may be shown that the set $M_2(n)$ of all $2 \times 2$ matrices with integer entries and determinant $n$ has decomposition

$$M_2(n) = \coprod_{a,b,d} SL_2(\mathbb{Z}) \begin{pmatrix} a & b \\ d & 0 \end{pmatrix},$$

the coproduct taken over the same index as above. Thus, taking the quotient of $M_2(n)$ by the action (by left-multiplication) of $SL_2(\mathbb{Z})$ gives, as a set of coset representatives, our set of triples $(a, b, d)$ from before.

Having introduced the Hecke operators on the space of weakly modular functions, we might ask: how do Hecke operators affect Fourier expansions? Recall our operators $T(N)$ acting on $\mathcal{M}_{2k}(\Gamma(1))$.

**Theorem 14.2.** Fix a weight $k$ and let $f \in \mathcal{M}_{2k}(\Gamma(1))$ have Fourier expansion

$$f(z) = \sum_{m=0}^{\infty} c_m q^m.$$ 

51
Then
\[ T(n) \cdot f(z) = \sum_{m=0}^{\infty} \gamma_m q^m, \]
where
\[ \gamma_m = \sum_{d \mid (m,n)} d^{2k-1} c_{mn/d^2}. \]

Proof. Omitted. (see Milne, proposition 5.16(b)) \qed

**Corollary 1:** The constant term of the Fourier expansion of \( T(n) \cdot f \) is \( c_0 \cdot \sigma_{2k-1}(n) \), and the coefficient of the linear term is \( c_n \).

**Corollary 2:** If \( n = p \) is prime, then
\[ \gamma_m = \begin{cases} c_{pm} & \text{if } p \nmid m; \\ c_{pm} + p^{2k-1} c_{m/p} & \text{if } p \mid m. \end{cases} \]

**Corollary 3:** Every \( T(n) \) maps cusp forms to cusp forms.

**Fact:** For \( \Gamma = \Gamma(1) \), the Hecke operators \( T(n) \) are Hermitian with respect to the Petersson inner product; hence, the space \( \{T(n)\} \) have a common basis of eigenforms on \( \mathcal{S}_k \).

We close now with the motivation for our next lecture: if \( f \in \mathcal{M}_{2k}(\Gamma(1)) \) is a nonzero eigenform for \( T(n) \), and has Fourier expansion
\[ f(z) = \sum_{n=0}^{\infty} c_n q^n, \]
then we have \( c_n = \lambda(n)c_1 \), where \( \lambda(n) \) is the eigenvalue of \( T(n) \) on \( f \). In particular, the Ramanujan \( \tau \)-function from Lecture Twelve is multiplicative (because \( \mathcal{S}_{12} \) is one-dimensional). We will pick up here next time.
15 Lecture Fifteen

Last time, we introduced the Hecke operators \( T(n) \) for \( \mathcal{M}_{2k}(\Gamma(1)) \), and saw that it satisfied various properties. In particular, we saw how the Fourier coefficients of Hecke eigenforms are determined by its eigenvalues and constant term.

**Proposition 15.1.** Let \( G_k \) be the Eisenstein series of weight \( 2k \) for \( \Gamma(1) \); then \( G_k \) is an eigenform of \( T(p) \) with eigenvalue \( \sigma_{2k-1}(p) = p^{2k-1} + 1 \).

*Proof.* Omitted. \( \square \)

**Proposition 15.2.** Let \( \mathcal{S}_k \) be the space of cusp forms of weight \( 2k \) for \( \Gamma(1) \); then

\[
\langle f, G_k \rangle = 0 \text{ for all } f \in \mathcal{S}_k,
\]

where \( \langle , \rangle \) is the Petersson inner product.

These results mean that we have a direct sum decomposition

\[
\mathcal{M}_{2k}(\Gamma(1)) = \mathcal{S}_k \oplus \langle G_k \rangle;
\]

we also recall our isomorphism

\[
\bigoplus_k \mathcal{M}_{2k}(\Gamma(1)) = C[E_2, E_3],
\]

where \( E_k = (2\zeta(2k))^{-1}G_k \) are the normalized Eisenstein series.

**Theorem 15.3.** Let \( \mathcal{M}_{2k}(\mathbb{Z}) \) be the \( \mathbb{Z} \)-submodule of \( \mathcal{M}_{2k}(\Gamma(1)) \) consisting of modular forms with integer Fourier coefficients; then

\[
\bigoplus_k \mathcal{M}_{2k}(\mathbb{Z}) = \mathbb{Z}[E_2, E_3].
\]

*Proof.* We have shown that the \( E_k \) are Hecke eigenforms, and we know that every \( T(p) \) has eigenvalues in \( \mathbb{Z} \) on \( E_k \); hence, every \( T(n) \) has eigenvalues in \( \mathbb{Z} \), and so it follows from our work in the previous lecture that the Fourier coefficients of \( E_k \) must be integers.

We also know that \( \Delta \) has eigenvalues in \( \mathbb{Z} \), and that \( f \mapsto f\Delta \) gives an isomorphism \( \mathcal{M}_{2k} \to \mathcal{S}_{2k+12} \); the result is now immediate. \( \square \)
We remark that, as the action of each $T(n)$ on $\mathcal{S}_{2k}(\Gamma(1))$ is Hermitian, then $T(n)$ must have real eigenvalues. **Corollary:** The eigenvalues of $T(n)$ are algebraic integers, and so lie in a totally real finite extension of $\mathbb{Q}$.

**Proof.** The action of $T(n)$ on $\mathcal{M}_{2k}(\Gamma(1))$ preserves the lattice $\mathcal{M}_{2k}(\mathbb{Z})$; thus, it acts by a matrix with $\mathbb{Z}$ coefficients once we have chosen a basis arising from this lattice. In particular, if the Fourier expansion is normalized so that the coefficient of $q$ is 1, then all coefficients must be algebraic integers. 

We will now change our perspective slightly, and consider modular forms for general congruence subgroups. Recall that we have defined the **principal congruence subgroups**

$$\Gamma(N) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \gamma \equiv I \mod N \right\};$$

we showed in homework that $\Gamma(N)$ is normal in $\text{SL}_2(\mathbb{Z})$, and that

$$\text{SL}_2(\mathbb{Z})/\Gamma(N) \cong \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

has cardinality $N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$. We called a **congruence subgroup** any subgroup $\Gamma$ of $\Gamma(1)$ of finite index which contains some $\Gamma(N)$. We have also established that the cusps of $\Gamma\backslash \mathbb{H}$ (for an arbitrary congruence subgroup $\Gamma$) are in one-to-one correspondence with the $\Gamma$-orbits of $\mathbb{P}^1(\mathbb{Q})$.

We used the Riemann-Roch theorem to prove that

$$\dim \mathcal{M}_{2k}(\Gamma) = (2k - 1)(g - 1) + \left\lfloor \frac{k}{2} \right\rfloor \varepsilon_2 + \left\lfloor \frac{2k}{3} \right\rfloor + k \nu_\infty,$$

where $g$ is the genus of $\Gamma\backslash \mathbb{H}$, $\varepsilon_{\ell}$ is the number of $\ell$-elliptic points (for $\ell = 2, 3$), and $\nu_\infty$ is the number of $\Gamma$-inequivalent cusps of $\mathbb{H}$. If $\Gamma$ denotes the image of $\Gamma$ in $\text{PSL}_2(\mathbb{Z})$, then

$$\nu_\infty = \ldots$$

The stabilizer $P$ of $i\infty$ in $\Gamma(1)$ is generated by $\begin{pmatrix} 1 & 1 \\ \end{pmatrix}$, while the stabilizer of $i\infty$ in $\Gamma$ is generated by $\begin{pmatrix} 1 & h \\ \end{pmatrix}$ for some positive integer $h$. These observations give a bijection

$$\Gamma\backslash \text{SL}_2(\mathbb{Z})/P \to \{\text{cusps of } \Gamma\}$$
via
\[ \Gamma \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) P \mapsto \Gamma \cdot \left( \frac{a}{c} \right). \]

**Fact:** When \( k \geq 2 \), one has
\[ \dim \mathcal{S}_{2k}(\Gamma) = \dim \mathcal{M}_{2k}(\Gamma) - \nu_\infty, \]
while
\[ \dim \mathcal{S}_2(\Gamma) = \dim \mathcal{M}_2(\Gamma) - (\nu_\infty - 1). \]

In the remainder of today’s lecture, we will compute the Eisenstein series associated to a given cusp for \( \Gamma \) (for \( k \geq 2 \)); this will be nonzero at our distinguished cusp, and zero at every other cusp. In every case, the Eisenstein series we construct will be orthogonal (with respect to the Petersson inner product) to the space of cusp forms.

In the \( \Gamma(1) \) case, we have from the definition
\[
G_k(z) = \sum_{(c,d) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(cz + d)^{2k}} = \sum_{m \in \mathbb{Z}} \sum_{(c,d) \in \mathbb{Z}^2} \frac{1}{\gcd(c,d)=m} \frac{1}{(cz + d)^{2k}}
\]
\[
= \sum_{m \geq 1} \frac{1}{m^{2k}} \sum_{\gcd(c,d)=1} \frac{1}{(cz + d)^{2k}} = \zeta(2k) \sum_{\gcd(c,d)=1} \frac{1}{(cz + d)^{2k}}.
\]
That is,
\[
E_{2k}(z) = \frac{1}{2\zeta(2k)} G_k(z) = \frac{1}{2} \sum_{\gcd(c,d)=1} \frac{1}{(cz + d)^{2k}}.
\]
where \( E_{2k} \) from now on denotes the normalized Eisenstein series of weight \( 2k \). For general \( \Gamma(N) \), let \( \tilde{v} \in (\mathbb{Z}/N\mathbb{Z})^2 \) be an element of order \( N \); we will consider \( \tilde{v} \) as a row vector \([\tilde{c}_v, \tilde{d}_v]\), where \( \tilde{a} \) is the image of \( a \) modulo \( N \). Let
\[
\delta = \begin{pmatrix} a & b \\ c_v & d_v \end{pmatrix} \in \text{SL}_2(\mathbb{Z});
\]
we know that some such \( \delta \) must exist because \( \tilde{v} \) has order \( N \). We now introduce two important pieces of notation.

**Definition:** The **automorphy factor** \( j(\gamma, z) \) is the function
\[
j : \text{SL}_2(\mathbb{Z}) \times \mathbb{H} \rightarrow \mathbb{C}
\]

55
defined
\[ j(\gamma, z) = cz + d \quad \text{for} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \]
(our notation is from Diamond-Shurman; Milne has \( j(\gamma, z) = (cz + d)^2 \) instead). A simple calculation shows that the automorphy factor satisfies the cocycle relation
\[ j(\gamma \gamma', z) = j(\gamma, \gamma' \cdot z) j(\gamma', z) \quad \text{for all} \quad z \in \mathbb{H}, \gamma, \gamma' \in \text{SL}_2(\mathbb{Z}). \]

We pause here for a moment to remark that the modularity condition (of weight \( 2k \)) can be written as the statement that
\[ f(\gamma \cdot z) = j(\gamma, z)^{2k} f(z) \quad \text{for all} \quad \gamma \in \text{SL}_2(\mathbb{Z}), z \in \mathbb{H}; \]
in fact, any function \( j(\gamma, z) \) satisfying the cocycle condition leads to a reasonable theory.

**Definition:** Suppose \( f \) is a complex-valued function on \( \mathbb{H} \), and let \( \gamma \in \text{SL}_2(\mathbb{Z}) \). A right action of \( \text{SL}_2(\mathbb{Z}) \) on \( f \) is given by
\[ (f[\gamma])_k(z) = j(\gamma, z)^{-k} f(\gamma(z)); \]
clearly, \( f \) is a modular form of weight \( k \) for \( \Gamma(1) \) if and only if it is holomorphic on \( \mathbb{H} \), and \([\gamma]_k \) acts trivially on \( f \) for all \( \gamma \in \text{SL}_2(\mathbb{Z}) \).

Having established these notations, we will begin the next lecture by constructing the previously-promised Eisenstein series for \( \Gamma(N) \). Our method will be to take an arbitrary function on \( \mathbb{H} \), sum over its values on \( \Gamma \)-translations (weighted by the automorphy factor).
16 Lecture Sixteen

We continue with the construction of Eisenstein series associated to the principal congruence subgroups $\Gamma(N)$. Let $\bar{v} \in (\mathbb{Z}/N\mathbb{Z})^2$ have order $N$, and write $\bar{v} = (\bar{c}_v, \bar{d}_v)$ with $c_v, d_v \in \mathbb{Z}$; then there exists a matrix

$$\delta = \begin{pmatrix} a & b \\ c_v & d_v \end{pmatrix} \in \text{SL}_2(\mathbb{Z}).$$

We define a function (per Milne’s notation): for $k \geq 2$, let

$$E_k(\bar{v})(z) = \varepsilon_N \sum_{\substack{\gcd(c, d) = 1 \\ (c, d) \equiv v \mod N}} (cz + d)^{-2k},$$

where $\varepsilon_N = \frac{1}{2}$ if $N = 1, 2$, and equals 1 otherwise (Diamond-Shurman would call this function $E_{2k}^\bar{v}$). We can also write

$$E_k(\bar{v})(z) = \sum_{\gamma \in P_+ \cap \Gamma(N) \setminus \Gamma(N)\delta} j(\gamma, z)^{-2k},$$

where

$$P_+ = (T) = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}$$

and $j(\gamma, z) = (cz + d)$ is the automorphy factor we introduced last time. A proof similar to the last time will show that this series converges absolutely and uniformly on compact subsets.

**Proposition 16.1.** For $\gamma \in \text{SL}_2(\mathbb{Z})$, one has

$$(E_k[\gamma]_{2k})(z) = E_k^{(\gamma z)}(z),$$

where $(f[\gamma]_{2k}) = j(\gamma, z)^{-k} f(\gamma z)$ as before.

*Proof.* Omitted. \hfill \square

**Corollary:** One has $E_k^{\bar{v}} \in \mathcal{M}_{2k}(\Gamma(N))$.

**Proposition 16.2.** One has

$$\lim_{\text{Im}(z) \to \infty} E_k^{\bar{v}}(z) = \begin{cases} 1 & \text{if } \bar{v} \equiv \pm (0, 1), \\ 0 & \text{otherwise}. \end{cases}$$
Corollary: The value of $E_{nk}^\tilde{\nu}(z)$ at the cusp corresponding to $\tilde{\nu}$ is 1, and is zero at every other cusp.

We outline the proof of the corollary: let $\delta = \left( \begin{array}{cc} a & b \\ c_v & d_v \end{array} \right)$ as before, and let $s = \frac{a'}{c'}$ be a cusp for $\Gamma(N)$. Then there exists a Möbius transformation

$$\alpha = \left( \begin{array}{cc} a' & b' \\ c' & d' \end{array} \right)$$

that sends $i\infty$ to $s$. The behaviour of $E_{nk}^\tilde{\nu}(z)$ at $s$ is therefore determined by $E_{nk}[\alpha]_{2k}(z)$ at $i\infty$; but

$$E_{nk}[\alpha]_{2k}(z) = E_k(\alpha \sigma \tau)(z) = E_{k}^{(0,1)\delta\alpha}(z),$$

which is nonzero at $i\infty$ if and only if

$$\overline{(0, 1)\delta\alpha} = \pm(0, 1),$$

if and only if

$$\left( \frac{d'}{c'} \right) \equiv \pm \left( \frac{-d_v}{c_v} \right) \mod N,$$

if and only if $\Gamma(N)s = \Gamma(N)(-d_v/c_v)$. It follows that the cusps of $\Gamma(N)$ are in bijection with the orbits of $\Gamma(N)$ on $\mathbb{Q} \cup \{i\infty\}$. We have a decomposition, orthogonal with respect to the Petersson inner product, for $k \geq 2$:

$$\mathcal{M}_{2k}(\Gamma(N)) = \bigoplus_{\tilde{\nu} \in (\mathbb{Z}/N\mathbb{Z})^2 \atop \text{ord}(\tilde{\nu})=N} \mathbb{C} \cdot E_{nk}^\tilde{\nu} \oplus \mathcal{S}_{2k}(\Gamma(N)).$$

Parts of this statement are obvious (e.g. that $E_{nk}^\tilde{\nu}$ is a modular form), other parts are known, and the rest will just be believed.

We will now generalize our earlier construction of the Hecke operators. Let $\Gamma_1, \Gamma_2$ be two congruence subgroups of $\Gamma(1)$; they can also be considered as subgroups of $\text{GL}_2^+(\mathbb{Q})$ (i.e. rational matrices with positive determinant). We want to consider the double coset

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

where $\alpha \in \text{GL}_2^+(\mathbb{Q})$. Consider the space $\Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2$ of left $\Gamma_1$-orbits; we have the decomposition

$$\Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2 = \bigsqcup_{\beta_i \in \Gamma_2} \alpha \beta_i.$$
Each double coset $\Gamma_1 \alpha \Gamma_2$ will give us an operator acting on $\mathcal{M}_k(\Gamma_1(N))$, where $\Gamma_1(N)$ is a particular congruence subgroup which we will define below. As we saw in the case of the full modular group, the double-coset decomposition will give relations between the Hecke operators we will construct.

Now: there is a one-to-one correspondence between orbit spaces

$$\Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2 \leftrightarrow ((\alpha^{-1} \Gamma_1 \alpha) \cap \Gamma_2) \backslash \Gamma_2;$$

the proof of this fact is an easy exercise. The action of $\text{SL}_2(\mathbb{Z})$ on functions $f : \mathbb{H} \to \mathbb{C}$ is extended to an action of $\text{GL}_2^+(\mathbb{Q})$ via

$$(f[\alpha]_k)(z) = (\operatorname{det} \alpha)^{k-1} j(\alpha, z)^{-k} f(\alpha \cdot z);$$

notice that the condition that $\operatorname{det} \alpha > 0$ means that $f[\alpha]_k$ is indeed a function on $\mathbb{H}$, and not on $\hat{\mathbb{H}}$.

**Definition:** The weight $k$ double coset operator of $\Gamma_1 \alpha \Gamma_2$ on function $f : \mathbb{H} \to \mathbb{C}$ is defined

$$f[\Gamma_1 \alpha \Gamma_2]_k = \sum_{j} f[\beta_j]_k,$$

where the sum runs over a complete set of coset representatives

$$\Gamma_1 \alpha \Gamma_2 = \bigsqcup_{j} \Gamma_1 \beta_j.$$

We first claim that there are only finitely many coset representatives $\beta_j$; our correspondence above shows that it is enough to show that there are only finitely many cosets $\alpha^{-1} \Gamma_1 \alpha \cap \Gamma_2 \backslash \Gamma_1$, which is clear because $\alpha^{-1} \Gamma_1 \alpha$ is a congruence subgroup of $\Gamma(1)$ which contains $\Gamma_2$.

**Fact:** Any two congruence subgroups are commensurable, meaning that their intersection has finite index in both.

Moreover, the function does not depend on choice of coset representatives: this is clear in the case $f \in \mathcal{M}_{2k}(\Gamma(1))$. The general case is left as an exercise.

**Proposition 16.3.** The action $[\Gamma_1 \alpha \Gamma_2]$ is a map $\mathcal{M}_{2k}(\Gamma_1) \to \mathcal{M}_{2k}(\Gamma_2)$.

**Proof.** (sketch) We check the condition of weak modularity. Take $\gamma_2 \in \Gamma_2$; then if $\{\beta_j\}$ are a set of representatives for the $\Gamma_1$ orbits, then $\{\beta_j \gamma_2\}$ is also a set of representatives, and $\beta_1 \gamma_2, \beta_2 \gamma_2$ must lie in different $\Gamma_1$-cosets. This is the case if and only if $\beta_1, \beta_2$ lie in different $\Gamma_1$-cosets. It follows that the action of $\gamma_2$ permutes the terms in our sum.
In the special case $\Gamma_1 \supset \Gamma_2$, we obtain an inclusion
\[ [\Gamma_1 \Gamma_2] : \mathcal{M}_k(\Gamma_1) \hookrightarrow \mathcal{M}_k(\Gamma_2) \]
by taking $\alpha = \text{id}$. In the special case $\alpha^{-1}\Gamma_1\alpha = \Gamma_2$, we obtain an isomorphism
\[ [\Gamma_1\alpha\Gamma_2] : \mathcal{M}_k(\Gamma_1) \cong \mathcal{M}_k(\Gamma_2). \]
Finally, if $\Gamma_1 \subset \Gamma_2$, we again take $\alpha = \text{id}$, and our sums are indexed by the cosets $\Gamma_1 \backslash \Gamma_2$. Then $[\Gamma_1\Gamma_2]$ is a projection
\[ [\Gamma_1\Gamma_2] : \mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2). \]
In general, any operator $[\Gamma_1\alpha\Gamma_2]$ can be written as a composition of these three maps: inside $\Gamma_1$ is the subgroup $\Gamma_1 \cap \alpha\Gamma_2\alpha^{-1}$, whose modular forms are isomorphic to those of $\alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$, which lives inside $\Gamma_2$. Thus:
\[ ([\alpha^{-1}\Gamma_1\alpha\cap\Gamma_2]\Gamma_2][(\Gamma_1\cap\alpha\Gamma_2\alpha^{-1})\alpha^{-1}\Gamma_1\alpha\cap\Gamma_2][\Gamma_1(\Gamma_1\cap\alpha\Gamma_2\alpha^{-1})] : \mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2). \]
Now: define the subgroups
\[ \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbf{Z}) : c \equiv 0 \mod N \right\} \]
and
\[ \Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbf{Z}) : a \equiv b \equiv 1 \mod N \text{ and } c \equiv 0 \mod N \right\}; \]
clearly we have inclusions
\[ \Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N). \]
Consider the homomorphism $\Gamma_0(N) \to (\mathbf{Z}/N\mathbf{Z})^\times$ sending $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $d \mod N$; this is a surjective homomorphism with kernel $\Gamma_1(N)$, and so $\Gamma_1(N)$ is normal in $\Gamma_0(N)$, and has quotient
\[ \Gamma_0(N)/\Gamma_1(N) \cong (\mathbf{Z}/N\mathbf{Z})^\times. \]
The double-coset operators we have just constructed give us an action of $\Gamma_0(N)$ on $\mathcal{M}_k(\Gamma_1(N))$: take $\alpha \in \Gamma_0(N)$, and consider the operator $[\Gamma_1(N)\alpha\Gamma_1(N)]_k$. Because $\Gamma_1$ is normal in $\Gamma_0$ (in fact, $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbf{Z}/N\mathbf{Z})^\times$), we know that
\[ [\Gamma_1(N)\alpha\Gamma_1(N)]_k : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N)). \]
Moreover, this depends only on the image of \( \alpha \in \Gamma_0/\Gamma_1 \); that is, only on the image of \( d \) modulo \( N \). We therefore have an action of \( (\mathbb{Z}/N\mathbb{Z})^\times \) on the finite-dimensional complex vector space \( \mathcal{M}_k(\Gamma_1(N)) \), and so there is an orthogonal decomposition

\[
\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_{\chi \in (\mathbb{Z}/N\mathbb{Z})^\times} \mathcal{M}_k(\Gamma_1(N), \chi),
\]

where \( \mathcal{M}_k(\Gamma_1(N), \chi) \) is the subspace of \( \mathcal{M}_k(\Gamma_1(N)) \) on which \( \Gamma_0 \) acts by the character \( \chi \). Note that we have slightly abused notation by considering \( \chi \) as a Dirichlet character

\[
\chi: (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times.
\]

We will pick up here next time.
17 Lecture Seventeen

We can define an operator \( \langle d \rangle : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N)) \) via
\[
\langle d \rangle f = f[\alpha]_k,
\]
where
\[
\alpha = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N), \quad \delta \equiv d \mod N.
\]
This is known as the diamond operator; in this case, the operator \([\alpha]_k\) coincides with the operator \([\Gamma_1(N)\alpha\Gamma_1(N)]_k\). This allows us to rewrite our subspaces from last lecture via
\[
\mathcal{M}_k(N, \chi) = \{ f \in \mathcal{M}_k(\Gamma_1(N)) : \langle d \rangle f = \chi(d) f \}.
\]

We will now construct another sort of Hecke operator: take \( \alpha = \begin{pmatrix} 1 & \ast \\ \cdot & \cdot \end{pmatrix} \in \text{GL}_2^+(\mathbb{Q}) \), with \( p \) prime, and put \( \Gamma_1 = \Gamma_2 = \Gamma_1(N) \). We define an operator
\[
T_p : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))
\]
by putting \( T_p f = [\Gamma_1(N) \begin{pmatrix} 1 & \ast \\ \cdot & \cdot \end{pmatrix} \Gamma_1(N)]_k \).

**Proposition 17.1.** If \( p | N \), then
\[
T_p f = \sum_{j=0}^{p-1} f \left[ \left( \begin{array}{c} 1 \\ \cdot \end{array} \right)_j \right]_k,
\]
and otherwise
\[
T_p f = \sum_{j=0}^{p-1} f \left[ \left( \begin{array}{c} 1 \\ \cdot \end{array} \right)_j \right]_k + f \left[ \left( \frac{m}{N} \frac{n}{p} \right) \left( \begin{array}{c} 1 \\ \cdot \end{array} \right) \right]_k.
\]
where \( mp - Nn = 1 \).

The proof follows from the fact that
\[
\Gamma_1(N) \begin{pmatrix} 1 \\ \cdot \end{pmatrix} \Gamma_1(N) \equiv \begin{pmatrix} 1 \\ x \end{pmatrix} \mod N
\]
for some $x$ modulo $N$, and hence

$$\Gamma_1(N) \begin{pmatrix} 1 \\ p \end{pmatrix} \Gamma_1(N) = \bigcup_j \Gamma_1(N) \beta_j$$

for an appropriate set $\{\beta_j\}$ of coset representatives (we will skip the details).

We compare the operators $T_p$ with the operators $T(p)$ on $\mathcal{M}_k(\Gamma(1))$ from before: the sum over $j$ for $T_p$ is the same as what we had for $T(p)$, and of course if $N = 1$ then $p \nmid N$ for all $p$, and so the extra term $\binom{p}{1}$ does indeed appear. We state without proof the following properties of the operators $T_p$:

- Suppose $f \in \mathcal{M}_k(\Gamma_0(N)) = \mathcal{M}_k(N, 1)$ (where 1 denotes the trivial character). If $a_n(f)$ denotes the $n$th Fourier coefficient of the function $f$, then $a_n(T_p f) = a_{np}(f) + \mathbb{1}_N(p)p^{k-1}a_{n/p}(\langle p \rangle f)$, where $\mathbb{1}_N(p)$ is 1 if $p|N$ and is zero otherwise.

- The operators $\langle d \rangle$ and $T_p$ commute, and for $p \neq q$ both prime, we have $T_p \cdot T_q = T_{pq}$.

**Definition:** Suppose $n \in \mathbb{N}$; then define an operator on $\mathcal{M}_k(\Gamma_1(N))$ via

$$T_n f = \begin{cases} (n \mod N) & \text{if } (n, N) = 1, \\ 0 & \text{if } (n, N) > 1. \end{cases}$$

It may be easily shown from our properties above that

$$T_m \cdot T_n = T_{mn} \text{ if } (m, n) = 1$$

and

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

whenever $r \geq 2$. Moreover, if $f \in \mathcal{M}_k(\Gamma_1(N))$, then

$$a_m(T_n f) = \sum_{d | (m, n)} d^{k-1}a_{mn/d^2}(\langle d \rangle f);$$

in particular, if $f \in \mathcal{M}_k(N, \chi)$, then

$$a_m(T_n f) = \sum_{d | (m, n)} \chi(d) d^{k-1}a_{mn/d^2}(f).$$

63
We remark that \( M_k(N, \chi) \) can be thought of as the \( \chi \)-eigenspace of \( \langle d \rangle \) in \( M_k(\Gamma_1(N)) \).

By construction, the algebra of operators generated by all \( T_n \) and \( \langle m \rangle \) is commutative. Finally, the algebra of Hecke operators preserves \( S_k(\Gamma_1(N)) \).

We now return briefly to the Petersson inner product, viz.

\[
(f, g)_{\Gamma} = \frac{1}{\text{vol}(\Gamma)} \int_{\Gamma \backslash \mathbb{H}} f(z) \bar{g}(z) y(z)^k \frac{dx dy}{y^2},
\]

where

\[
\text{vol}(\Gamma) = [\bar{\Gamma}(1) : \bar{\Gamma}] \cdot \text{vol}(\Gamma(1) \backslash \mathbb{H}),
\]

and \( \bar{\Gamma} \) denotes the image of \( \Gamma \) in \( \text{PSL}_2 \). We observe that, if \( \Gamma_1 \subset \Gamma_2 \) and \( f, g \in S_k(\Gamma_2) \), then

\[
(f, g)_{\Gamma_1} = (f, g)_{\Gamma_2}.
\]

If \( \Gamma \subset \Gamma(1) \) is a congruence subgroup and \( \alpha \in \text{GL}_2^+(\mathbb{Q}) \), put \( \alpha' = \text{det}(\alpha)\alpha^{-1} \). Then: if \( \alpha^{-1} \Gamma \alpha \subset \Gamma(1) \), then for \( f \in S_k(\Gamma), g \in S_k(\alpha^{-1} \Gamma \alpha) \), one has

\[
(f[\alpha]_k, g)_{\alpha^{-1} \Gamma \alpha} = (f, g[\alpha']_k)_{\Gamma}.
\]

Moreover, if \( f, g \in S_k(\Gamma) \), then

\[
(f[\Gamma \alpha \Gamma]_k, g) = (f, g[\Gamma \alpha \Gamma]_k).
\]

Now: recall that the adjoint operator \( T^* \) of a given operator \( T \) satisfies

\[
\langle v, Tw \rangle = \langle T^* v, w \rangle,
\]

and that \( T \) is called normal if it commutes with \( T^* \).

We will use the fact that \( \langle p \rangle^k = \langle p \rangle^{-1} \); this follows from our above calculations applied to \( \alpha = \left( \begin{smallmatrix} 1 & p \\ \phantom{.} & 1 \end{smallmatrix} \right) \), for which \( \alpha' = \alpha \). Similarly, we can show

\[
T_p^* \langle p \rangle^{-1} T_p \text{ for } p \nmid N.
\]
18 Lecture Eighteen

We begin by correcting a statement from the previous lecture (regarding the coefficients $a_m(f)$). Today, we will discuss old forms and new forms.

There are two ways to fit $S_k(\Gamma_1(N))$ into $S_k(\Gamma_1(M))$ when $M|N$: one is via the identity inclusion, as every modular form for $\Gamma_1(M)$ is necessarily a modular form for $\Gamma_1(N)$. There is another way: if $d|\frac{N}{M}$, put

$$\alpha_d = \begin{pmatrix} d \\ 1 \end{pmatrix} \in \text{GL}_2^+(\mathbb{Q}),$$

so that

$$f[\alpha_d]_k(z) = d^{k-1} f(dz)$$

for any function $f : \mathbb{H} \to \mathbb{C}$. An easy calculation shows

$$\alpha_d \Gamma_1(N) \alpha_d^{-1} \subseteq \Gamma_1(M),$$

and so $[\alpha]_d$ takes modular forms for $\Gamma_1(M)$ to modular forms for $\Gamma_1(N)$. Thus, for $d|N$, we have a map

$$\iota_d : \mathcal{S}_k(\Gamma_1(N/d)) \times \mathcal{S}_k(\Gamma_1(N/d)) \to \mathcal{S}_k(\Gamma_1(N))$$

defined by $(f, g) \mapsto f + g[\alpha_d]_k$. We define the space of old forms of level $N$ to be the space

$$\mathcal{S}_k(\Gamma_1(N))^\text{old} = \sum_{p|N} \iota_p(\mathcal{S}_k(\Gamma_1(N/p))).$$

We define the space $\mathcal{S}_k(\Gamma_1(N))^\text{new}$ to be the orthogonal complement of $\mathcal{S}_k(\Gamma_1(N))^\text{old}$ in the space $\mathcal{S}_k(\Gamma_1(N))$.

Fact: The operators $T_n$ and $\langle n \rangle$ preserve $\mathcal{S}_k(\Gamma_1(N))^\text{old}$ and $\mathcal{S}_k(\Gamma_1(N))^\text{new}$, for all $n$.

To prove this fact, one treats separately the old and the new cases. The calculation for the old formms is straightforward, but is not so easy for the new space: for these, we show instead that the space is invariant under the adjoints $T_n^*$ and $\langle n \rangle^*$.

We want to investigate the Fourier expansions of the forms in our spaces. Using our notation from above, we have

$$\iota_d = d^{1-k}[\alpha_d]_k \text{ and } \iota_d(f)(z) = f(dz)$$

65
whenever \( f \in \mathcal{A}_k(\Gamma_1(N)) \). Suppose \( f \) has Fourier expansion

\[
f(z) = \sum_{n=1}^{\infty} a_n q^n;
\]

then \( \iota_d \) has Fourier expansion

\[
(\iota_d f)(z) = \sum_{n=1}^{\infty} a_n q^{nd}.
\]

In particular, if \( f \) is an old form, write

\[
f = \sum_{p\mid N} \iota_p f_p
\]
as before, with each \( f_p \in \mathcal{A}_k(\Gamma_1(N/p)) \). Then \( a_n(f) = 0 \) for all \( n \) such that \( (n, N) = 1 \); in fact, the converse is true.

**Lemma 3.** If \( f \in \mathcal{A}_k(\Gamma_1(N)) \), then \( f \) is an old form if and only if \( a_n(f) = 0 \) for all \( n \) with \( (n, N) = 1 \).

**Proof.** There are three main steps in the proof; we outline them first.

In the first step, we will change \( \iota_p \) so that \( \iota_p \) becomes the identity inclusion. Then, we consider the \( \Gamma(1) \) action on \( \mathcal{A}_k(\Gamma_1) \), for some subgroup \( \Gamma_1 \subseteq \Gamma(1) \); if \( \Gamma_2 \subseteq \Gamma_1 \) has finite index, then the elements of \( \mathcal{A}_k(\Gamma_1) \) are the vectors of \( \mathcal{A}_k(\Gamma_2) \) which are fixed under the action of \( \Gamma_1 \). Finally, we will use representation theory, applied to the finite group \( \Gamma_1/\Gamma_2 \).

First: put

\[
\Gamma^1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : b \equiv 0 \mod N \text{ and } a \equiv d \equiv 1 \mod N \right\};
\]

then

\[
\alpha_M \Gamma_1(M) \alpha_M^{-1} = \Gamma^1(M),
\]

and so \( M^{k-1}[\alpha_M^{-1}]_k : \mathcal{A}_k(\Gamma_1(M)) \to \mathcal{A}_k(\Gamma^1(M)) \) is an isomorphism. We have the
following commutative diagram:

\[
\begin{array}{c}
\mathcal{I}_k(\Gamma_1(M)) \xrightarrow{id} \mathcal{I}_k(\Gamma_1(N)) \\
\downarrow \quad \downarrow \\
\mathcal{I}_k(\Gamma_1(M)) \xrightarrow{\iota_d} \mathcal{I}_k(\Gamma_1(N))
\end{array}
\]

Writing \( q_M = q_1^{M}, q_N = q_1^{N} \), we use the relation \( N = Md \) to obtain \( q_{N}^{d^n} = q_{M}^{n} \) for any \( n \). The image of \( f = \sum_n a_n q^n \) in \( \mathcal{I}_k(\Gamma_1(M)) \) in \( \mathcal{I}_k(\Gamma_1(N)) \) is \( \sum_n a_n q_{N}^{d^n} \).

Next, we reformulate things in terms of representation theory. Define the projection

\[ \pi_d : \mathcal{I}_k(\Gamma(N)) \to \mathcal{I}_k(\Gamma_d), \]

where

\[ \Gamma_d = \Gamma_1(N) \cap \Gamma^0(N/d), \]

and

\[ \Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : b \equiv 0 \mod N \right\}. \]

The inclusions \( \Gamma(N) \subset \Gamma_d \subset \Gamma_1(N) \) allow us to write in co-ordinates

\[ \pi_d \left( \sum_{n=1}^{\infty} a_n q^n \right) = \frac{1}{d} \sum_{b=0}^{d-1} f \left( \begin{pmatrix} 1 & bN/d \\ 1 & \end{pmatrix} \right)_k. \]

If we put

\[ \pi = \prod_{p \mid N} (1 - \pi_p), \]

then the statement that \( f \) is a linear combination of the terms \( \iota_p f_p \) is the statement that \( f \in \ker \pi \). In fact, it can be shown that

\[ \ker \pi = \sum_{p \mid N} \text{Im}(\pi_p). \]
Thus we have obtained a projection $\pi : \mathcal{S}_k(\Gamma(N)) \to \mathcal{S}_k(\Gamma(N))$. Let $G = \Gamma(1)$, and let $H = \Gamma^1(N) = \Gamma(N)$: we will find the $H$-fixed vectors in $\ker \pi$. We have by a previous observation that

$$\ker \pi = \sum_{\rho \mid N} \mathcal{S}_k(\Gamma_\rho);$$

by our representation theory reformulation, we that

$$\mathcal{S}_k(\Gamma(N)) \cap \left( \sum_{\rho \mid N} \mathcal{S}_k(\Gamma(N)) \right)^{\Gamma_p / \Gamma(N)} = \sum_{\rho \mid N} \mathcal{S}_k(\Gamma^1(N/p)), \quad (*)$$

where the superscript $\Gamma_p / \Gamma(N)$ denotes the subset of vectors fixed under the action of that subgroup. Note that we can write

$$\mathcal{S}_k(\Gamma^1(N/p)) = \mathcal{S}_k(\Gamma(N))^{\Gamma^1(N/p)};$$

thus

$$\mathcal{S}_k(\Gamma_\rho) = \mathcal{S}_k(\Gamma(N))^{\Gamma_1(N) \cap \Gamma^0(N/d)}.$$

We know abstractly that if a group $G$ has a (finite) direct sum decomposition $G = \prod_i G_i$, and if $V$ is an irreducible representation of $G$, then for any subgroups $H = \prod_i H_i, K = \prod_i K_i$, one has

$$V^H \cap \sum_i V^{K_i} = \sum_i V^{(H_i, K_i)} \quad (\dagger)$$

where $\langle H_i, K_i \rangle$ is the subgroup of $G$ generated by $H_i$ and $K_i$.

In our situation, we will take $G = \Gamma(1), G_i = \text{SL}_2(\mathbb{Z}/p_i^{\varepsilon_i}), \mathbb{Z}$ (where $N = \prod_i p_i^{\varepsilon_i}$), $H_i = \Gamma^1(p_i^{\varepsilon_i}) / \Gamma(p_i^{\varepsilon_i})$, and

$$K_i = \Gamma^1(p_i^{\varepsilon_i}) \cap \Gamma^0(p_i^{\varepsilon_i-1}) / \Gamma(p_i^{\varepsilon_i}).$$

To complete the proof, it remains to identify equation $\ast$ with the result $\dagger$; this is left as an exercise.

We meet here again in a week and a half.
19 Lecture Nineteen

We closed last time with a discussion of the decomposition of the space of cusp forms into the new and old. These complementary subspaces are preserved under the Petersson inner product. Recall that we saw that \( f \in \mathcal{S}_k(\Gamma_1(N))^\text{old} \) implies that 
\[
a_n(f) = 0 \quad \text{whenever } (n, N) = 1,
\]
where \( a_n(f) \) is the \( n \)th Fourier coefficient of \( f \).

**Definition:** Suppose \( f \in \mathcal{M}_k(\Gamma_1(N)) \); we say that \( f \) is a Hecke eigenform (or simply an eigenform) if it is an eigenvector for all \( T_n \) and all \( \langle n \rangle \).

If we consider only common eigenvectors for those \( T_n \) and \( \langle n \rangle \) such that \( (n, N) = 1 \), then we can show that \( \mathcal{S}_k(\Gamma_1(N))^\text{new} \) has a basis of such eigenvectors. The key point in this proof is the fact that, if \( f \in \mathcal{S}_k(\Gamma_1(N))^\text{new} \) is an eigenvector for all \( T_n \) and \( \langle n \rangle \) with \( (n, N) = 1 \), then it is an eigenform. This follows from the formula

\[
a_n(f) = \lambda_n a_1(f) \quad \text{if } (n, N) = 1,
\]

where \( \lambda_n \) is the eigenvalue of \( T_n \) acting on \( f \). In particular, we must have \( a_1(f) \neq 0 \); otherwise, \( f \) would not be a new form. Normalizing \( f \) so that \( a_1(f) = 1 \), let \( m \in \mathbb{N} \) and let

\[
g_m = T_m f - a_m(f)f.
\]

Then

\[
T_n g_m = T_n(T_m f) - a_m(f)T_n f = \lambda_n(T_m f - a_m(f)f) = \lambda_n g_m,
\]

and so \( g_m \) is an eigenvector for all \( T_n \) with \( (n, N) = 1 \). We have

\[
a_1(g_m) = a_1(T_m f) - a_1(a_m(f)f) = a_m(f) - a_m(f)a_1(f) = 0,
\]

because of our normalization of \( f \); it follows that \( g_m \) is old. But \( g_m = T_m f - a_m(f)f \) is also a new form, and so must equal zero, and we have proven our claim.

**Definition:** A new form is a normalized eigenform in \( \mathcal{S}_k(\Gamma_1(N))^\text{new} \).

**Theorem 19.1.** The eigenspaces of \( T_n \) on \( \mathcal{S}_k(\Gamma_1(N))^\text{new} \) are one-dimensional (this is known as the multiplicity one result). Furthermore, the new forms in \( \mathcal{S}_k(\Gamma_1(N))^\text{new} \) form an orthonormal basis for that space; the \( n \)th Fourier coefficient of each new form is its eigenvalue on \( T_n \); each new form lies in \( \mathcal{S}_k(N, \chi) \) for some \( \chi \); and, if \( f \in \mathcal{S}_k(\Gamma_1(N)) \) is an eigenform, then it is either old or new (it is not the sum of a nonzero new form and a nonzero old form).

The proof is left as an exercise.
We now begin our discussion on $L$-functions, which will probably take us to the end of the course. Suppose I have a modular form $f$ with Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a_n q^n,$$

where $q = \exp(2\pi i z)$. Define the **Dirichlet series** associated to $f$ to be the formal series

$$L(s, f) = \sum_{n=1}^{\infty} a_n n^{-s},$$

where $s \in \mathbb{C}$. Recall that, several weeks ago, we calculated an estimate for the magnitude of the Fourier coefficients of a cusp form; namely, we showed that if $f$ is a cusp form of weight $k$, then $|a_n| \leq C n^{1/2}$ for some absolute constant $C$. An easy exercise is to show that this implies that $L(s, f)$ will converge absolutely for $\text{Re}(s) > 1 + \frac{k}{2}$ when $f$ is a cusp form.

It can be shown (with more work) that, if $f$ is an Eisenstein series, our explicit formula for its Fourier coefficients gives the bound $|a_n| \leq C n^{k-1}$, which will imply that $L(s, f)$ converges absolutely when $\text{Re}(s) > k$.

**Theorem 19.2.** Let $f \in \mathcal{M}_k(N, \chi)$, and suppose $f$ has Fourier expansion

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n.$$

Then $f$ is a normalized eigenform if and only if

$$L(s, f) = \prod_p (1 - a_p p^{-s} + \chi(p)p^{k-1-2s})^{-1},$$

where the product is taken over all primes.

**Proof.** (sketch) We have

$$\sum_{n=0}^{\infty} a_{p^r} p^{-rs} = \frac{1}{1 - a_{p^r} p^{-rs}} = \frac{1}{1 - a_p p^{-s} + \chi(p)p^{k-1-2s}};$$

the normalization $a_1 = 1$ corresponds to the case $r = 0$. Thus

$$\sum_{n=1}^{\infty} a_n n^{-s} = \prod_p \left( \sum_{r=0}^{\infty} a_{p^r} p^{-rs} \right),$$

valid when $\text{Re}(s) \gg 0$. \qed
Now, a brief aside on the Mellin transform; this is the Fourier transform on the locally compact abelian group $\mathbb{R}_{>0}$. First, we discuss the general Fourier transform. Recall that if $G$ is a locally compact abelian group, we denote by $\hat{G}$ its Pontryagin dual, consisting of all multiplicative homomorphisms

$$\chi : G \rightarrow \mathbb{C}^\times.$$  

The **Fourier transform** of a function $f : G \rightarrow \mathbb{C}$ is the function $\hat{f} : \hat{G} \rightarrow \mathbb{C}$ defined by

$$\hat{f}(\chi) = \int_G f(g)\overline{\chi(g)} \, dg.$$ 

For instance, if $G = S^1 = \mathbb{C}^\times$, then $\hat{G}$ consists of maps of the form $z \mapsto z^n$, with $n \in \mathbb{Z}$. Hence $\hat{G} \cong \mathbb{Z}$, and the Fourier coefficient at $n$ is

$$\int_0^1 f(x) \exp(-2\pi inx) \, dx.$$ 

If $G = \mathbb{R}$, then $\hat{G}$ consists of maps of the form $x \mapsto \exp(2\pi ix)$, so $\hat{G} \cong G \cong \mathbb{R}$, and

$$\hat{f}(y) = \int_{\mathbb{R}} f(x) \exp(-2\pi ixy) \, dx.$$ 

Finally, if $G = \mathbb{R}_{>0}$, then characters on $G$ have the form $x \mapsto x^s$ for some $s \in \mathbb{C}$. Hence $\hat{G} \cong \mathbb{C}$, and the Fourier transform is in this case called the **Mellin transform** and takes the form

$$g(s) = \int_0^\infty f(it)t^{s-1} \frac{dt}{t}.$$ 

**Theorem 19.3.** Let $f \in \mathcal{S}_k(\Gamma_1(N))$ and let $g(s)$ be the Mellin transform of $f$; then

$$g(s) = (2\pi)^{-s/2}\Gamma(s)L(s, f),$$

where

$$\Gamma(s) = \int_0^\infty x^{s-1}e^{-x} \, dx$$

is the usual $\Gamma$-function.

**Proof.** Omitted. 

\[ 71 \]
Theorem 19.4. Let $\Lambda_N(s)$ be the “completed $L$-function of $f$”, defined

$$\Lambda_N(s) = N^{s/2}(2\pi)^{-s} \Gamma(s)L(s, f),$$

and let $w_N : \mathcal{S}_k(\Gamma_1(N)) \to \mathcal{S}_k(\Gamma_1(N))$ be the function

$$w_N(f) = i^k N^{1-k/2} f \left[ \begin{array}{cc} 0 & -1 \\ N & 0 \end{array} \right]_k.$$

Then $w_N$ is idempotent (meaning $w_N^2 = \text{id}$) and self-adjoint; there is the decomposition

$$\mathcal{S}_k(\Gamma_1(N)) = \mathcal{S}_k^+ \oplus \mathcal{S}_k^-,$$

where $\mathcal{S}_k^\varepsilon$ denotes the $\varepsilon$-eigenspace of $w_N$ in $\mathcal{S}_k(\Gamma_1(N))$ (for $\varepsilon \in \{\pm 1\}$); and, moreover, if $f \in \mathcal{S}_k^\varepsilon$, then $\Lambda_N(s)$ extends to a function which is entire on $\mathbb{C}$, and which satisfies the functional equation

$$\Lambda_N(s) = \varepsilon \Lambda_N(k - s).$$