Lectures on Modular Forms

Igor Dolgachev

Fall 1997/98

Contents

Lecture 1

Binary Quadratic Forms

1.1 The theory of modular form originates from the work of C.F. Gauss of 1831 in which he gave a geometrical interpretation of some basic notions of number theory.

Let us start with choosing two non-proportional vectors in $\mathbb{R}^2$

$$\mathbf{v} = (a, b), \quad \mathbf{w} = (c, d).$$

The set of vectors

$$\Lambda = \mathbb{Z}\mathbf{v} + \mathbb{Z}\mathbf{w} := \{m_1\mathbf{v} + m_2\mathbf{w} \in \mathbb{R}^2 | \quad m_1, m_2 \in \mathbb{Z}\}$$

forms a *lattice* in $\mathbb{R}^2$, i.e., a free subgroup of rank 2 of the additive group of the vector space $\mathbb{R}^2$. We picture it as follows:

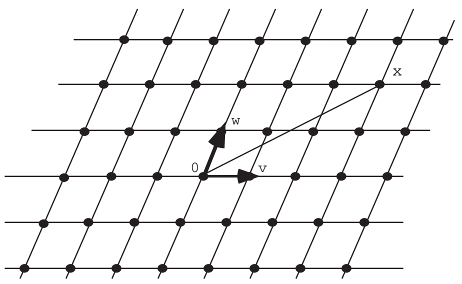

Fig.1

The area $A(\mathbf{v}, \mathbf{w})$ of the parallelogram formed by the vectors $\mathbf{v}$ and $\mathbf{w}$ is given by the formula

$$A(\mathbf{v}, \mathbf{w})^2 = \det \begin{pmatrix} \mathbf{v} \cdot \mathbf{v} & \mathbf{v} \cdot \mathbf{w} \\ \mathbf{v} \cdot \mathbf{w} & \mathbf{w} \cdot \mathbf{w} \end{pmatrix}.$$

Let $\mathbf{x} = m_1\mathbf{v} + m_2\mathbf{w} \in \Lambda$. The length of $\mathbf{x}$ is given by the formula

$$||\mathbf{x}||^2 = ||m_1\mathbf{v} + m_2\mathbf{w}||^2 = (m_1, m_2)\begin{pmatrix} \mathbf{v}\cdot\mathbf{v} & \mathbf{v}\cdot\mathbf{w} \\ \mathbf{v}\cdot\mathbf{w} & \mathbf{w}\cdot\mathbf{w} \end{pmatrix}\begin{pmatrix} m_1 \\ m_2 \end{pmatrix} =$$

$$am_1^2 + 2bm_1m_2 + cm_2^2,$$

where

$$a = \mathbf{v}\cdot\mathbf{v}, \quad b = \mathbf{v}\cdot\mathbf{w}, \quad c = \mathbf{w}\cdot\mathbf{w}. \tag{1.1}$$

Let us consider the (binary) quadratic form (the *distance quadratic form* of Λ)

$$f = ax^2 + 2bxy + cy^2.$$

Notice that its discriminant satisfies

$$D = 4(b^2 - ac) = -4A(\mathbf{v}, \mathbf{w})^2 < 0. \tag{1.2}$$

Thus f is positive definite. Given a positive integer n one may ask about integral solutions of the equation

$$f(x, y) = n.$$

If there is an integral solution (m_1, m_2) of this equation, we say that the binary form f *represents* the number n. Geometrically this means that the circle of radius $\sqrt{n}$ centered at the origin contains one of the points $\mathbf{x} = m_1\mathbf{v} + m_2\mathbf{w}$ of the lattice Λ. Notice that the solution of this problem depends only on the lattice Λ but not on the form f. In other words, if we choose another basis $\mathbf{v}', \mathbf{w}'$ of the lattice Λ, then the corresponding quadratic form

$$f' = a'x^2 + 2b'xy + c'y^2,$$

where $a' = \mathbf{v}'\cdot\mathbf{v}', \quad b' = \mathbf{v}'\cdot\mathbf{w}', \quad c' = \mathbf{w}'\cdot\mathbf{w}'$ has the same set of integral solutions for the equation

$$f'(x, y) = n.$$

Let

$$\mathbf{v}' = \alpha\mathbf{v} + \gamma\mathbf{w}, \quad \mathbf{v}' = \beta\mathbf{v} + \delta\mathbf{w}.$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Since the matrix

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

is invertible in the ring of integral matrices, we must have

$$\det M = \alpha\delta - \beta\gamma = \pm 1.$$

It is easy to see that

$$\begin{pmatrix} \mathbf{v}'\cdot\mathbf{v}' & \mathbf{v}'\cdot\mathbf{w}' \\ \mathbf{v}'\cdot\mathbf{w}' & \mathbf{w}'\cdot\mathbf{w}' \end{pmatrix} = M^t \begin{pmatrix} \mathbf{v}\cdot\mathbf{v} & \mathbf{v}\cdot\mathbf{w} \\ \mathbf{v}\cdot\mathbf{w} & \mathbf{w}\cdot\mathbf{w} \end{pmatrix} M$$

and hence

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

This can be also expressed by saying that the form f' is obtained from the form f by using the change of variables

$$x \to \alpha x + \beta y, \quad y \to \gamma x + \delta y.$$

We write this in the form

$$f' = Mf.$$

According to Lagrange two binary quadratic forms f and g are called *equivalent* if one transforms to another under the change of variables as above defined by an integral matrix with determinant ± 1. An equivalence class is called the *class of forms*. Obviously, for any $n \in \mathbb{Z}$, the set of integral solutions of the equations $f(x, y) = n$ depends only on the class of forms to which f belongs. Also it is clear that two equivalent forms have the same discriminant.

1.2 As we saw before any lattice Λ determines a class of forms expressing the distance from a point in Λ to the origin. Conversely, given a positive definite binary form $f = ax^2 + 2bxy + cy^2$ we can find a lattice Λ corresponding to this form. To do this we choose any vector $\mathbf{v}$ of length $\sqrt{a}$ and let $\mathbf{w}$ be the vector of length $\sqrt{c}$ which forms the positive angle with $\mathbf{v}$ defined by $\cos\phi = b/\sqrt{ac}$. Obviously we use here that f is positive definite. Of course, Λ is defined uniquely only we if identify two lattices obtained from each other by an orthogonal transformation of $\mathbb{R}^2$.

In this way we obtain the following:

Theorem 1.1. *There is a natural bijection between the set of lattices in $\mathbb{R}^2$ modulo an orthogonal transformation and the set of classes of positive definite quadratic forms.*

Let us describe the set of classes of forms in a more explicit way.

Theorem 1.2. *Let f be a positive definite binary form. Then there exists a form $g = Ax^2 + 2Bxy + Cy^2$ equivalent to f which satisfies the conditions:*

$$\{0 \leq 2B \leq A \leq C\}.$$

Proof. Let $f = ax^2 + 2bxy + cy^2$ and Λ be a lattice associated to it. Let us change the basis of Λ in such way that the corresponding form

$$g = \|\mathbf{v}'\|^2 x^2 + 2\mathbf{v}' \cdot \mathbf{w}' xy + \|\mathbf{w}'\|^2 y^2$$

satisfies the assertion of the theorem. We take $\mathbf{v}'$ to be a vector from Λ of smallest length $\sqrt{a}$. Then we take for $\mathbf{w}'$ any vector from Λ of smallest length among all vectors not equal to $\pm\mathbf{v}'$. I claim that $(\mathbf{v}', \mathbf{w}')$ forms a basis of Λ. Assume it is false. Then there exists a vector $\mathbf{x} \in \Lambda$ such that $\mathbf{x} = a\mathbf{v}' + b\mathbf{w}'$ where one of the coefficients a, b is a real number but not an integer. After adding some integral linear combination of $\mathbf{v}', \mathbf{w}'$ we can assume that $|a|, |b| \leq \frac{1}{2}$. If $a, b \neq 0$, this gives

$$\|\mathbf{x}\|^2 = |a|^2\|\mathbf{v}'\|^2 + |b|^2\|\mathbf{w}'\|^2 + 2ab\mathbf{v}' \cdot \mathbf{w}' < (|a|\|\mathbf{v}'\| + |b|\|\mathbf{w}'\|)^2 \leq \frac{1}{2}\|\mathbf{w}'\|^2$$

contradicting the choice of $\mathbf{w}'$. Here we have used the Cauchy inequality together with the fact that the vectors $\mathbf{v}'$ and $\mathbf{w}'$ are not proportional. If a or b is zero, we get $\|x\| = \frac{1}{2}\|\mathbf{v}'\|$ or $\|x\| = \frac{1}{2}\|\mathbf{w}'\|$, again a contradiction.

Now let us look at g. The square of the two diagonals $d_\pm$ of the parallelogram formed by the vectors $\mathbf{v}', \mathbf{w}'$ is equal to

$$d_\pm^2 = \|\mathbf{v}'\|^2 \pm 2\mathbf{v}' \cdot \mathbf{w}' + \|\mathbf{w}'\|^2.$$

Clearly $d_\pm \geq \|\mathbf{w}'\|$. By construction, $\|\mathbf{w}'\| \geq \|\mathbf{v}'\|$. Thus $2|\mathbf{v}' \cdot \mathbf{w}'| \leq \|\mathbf{v}'\|^2 \leq \|\mathbf{w}'\|^2$. It remains to change $\mathbf{v}'$ to $-\mathbf{v}'$, if needed, to assume that $B = \mathbf{v} \cdot \mathbf{w}' \geq 0$. □

Definition. A positive definite binary quadratic form $ax^2 + 2bxy + cy^2$ is called *reduced* if

$$0 \leq 2b \leq a \leq c.$$

The previous theorem says that each positive definite binary quadratic form is equivalent to a reduced form.

Let

$$\Omega = \{(a, b, c) \in \mathbb{R}^3 : 0 \leq 2b \leq a \leq c, a > 0, ac > b^2\}. \tag{1.3}$$

By Theorem 1.2, any positive definite binary quadratic form is equivalent to a form $ax^2 + 2bxy + cy^2$, where $(a, b, c) \in \Omega$.

1.3 Let us find when two reduced forms are equivalent. To do this we should look at the domain Ω from a different angle. Each positive definite quadratic form $f = ax^2 + 2bxy + cy^2$ can be factored over $\mathbb{C}$ into product of linear forms:

$$f = ax^2 + 2bxy + cy^2 = a(x - zy)(x - \bar{z}y),$$

where

$$z = \frac{-b}{a} + i\frac{\sqrt{ac-b^2}}{a}. \tag{1.4}$$

It is clear that f is completely determined by the coefficient a and the root z. Observe that $\mathrm{Im}\ z > 0$. We have a bijective correspondence

$$f = ax^2 + 2bxy + cy^2 \to (a, z)$$

from the set of positive definite binary quadratic forms to the set $\mathbb{R}_+ \times \mathcal{H}$, where

$$\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}\ z > 0\}$$

is the *upper half-plane*. Let us see how the group $\mathrm{GL}(2, \mathbb{Z})$ acts on the both sets. We have

$$Mf = a((\alpha x + \beta y) - z(\gamma x + \delta y))((\alpha x + \beta y) - \bar{z}(\gamma x + \delta y)) =$$

$$a(x(\alpha - \gamma z_1) - y(-\beta + \delta z))(x(\alpha - \gamma\bar{z}) - y(-\beta + \delta\bar{z})) =$$

$$a|\alpha - z\gamma|^2(x - \frac{-\beta + \delta z}{\alpha - \gamma z}y)(x - \frac{-\beta + \delta\bar{z}}{\alpha - \gamma\bar{z}}y).$$

Let us consider the action of $\mathrm{GL}(2, \mathbb{Z})$ on $\mathbb{C} \setminus \mathbb{R}$ by fractional-linear transformations (also called *Moebius transformations*) defined by the formula

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot z = \frac{\alpha z + \beta}{\gamma z + \delta}. \tag{1.5}$$

Notice that

$$\mathrm{Im}\ M \cdot z = \mathrm{Im}\ \frac{\alpha z + \beta}{\gamma z + \delta} = \mathrm{Im}\ \frac{(\alpha z + \beta)(\gamma\bar{z} + \delta)}{|\gamma z + \delta|^2} = \frac{\alpha\delta - \beta\gamma}{|\gamma z + \delta|^2}\mathrm{Im}\ z. \tag{1.6}$$

This explains why the transformation is well-defined on $\mathbb{C} \setminus \mathbb{R}$. Also notice that

$$M^{-1} = \det M \begin{pmatrix} \beta & -\beta \\ -\gamma & \alpha \end{pmatrix}.$$

Thus the root z is transformed to the root $z' = M^{-1} \cdot z$ and we obtain, for any $M \in \mathrm{GL}(2, \mathbb{Z})$,

$$M^{-1} \cdot f = a|\gamma z + \delta|^2(x - M \cdot z)(x - M \cdot \bar{z}).$$

1.4 Until now we considered binary forms up to the equivalence defined by an invertible integral substitution of the variables. We say that two binary forms are *properly equivalent* if they differ by a substitution with determinant equal to 1. In other words, we restrict ourselves with with the subgroup $\mathrm{SL}(2,\mathbb{Z})$ of $\mathrm{GL}(2,\mathbb{Z})$.

Since

$$\mathrm{GL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z}) \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mathrm{SL}(2,\mathbb{Z})$$

and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}(ax^2+2bxy+cy^2) = ax^2-2bxy+cy^2$ we obtain that each f is properly equivalent to a form $ax^2+2bxy+cy^2$, where $(a,b,c) \in \bar{\Omega}$ and

$$\bar{\Omega} = \{(a,b,c) \in \mathbb{R}^3 : |2b| \leq c \leq a, a, ac-b^2 > 0\}.$$

Definition. We shall say that $f = ax^2+2bxy+cy^2$ is *properly reduced* if $(a,b,c) \in \bar{\Omega}$.

Since

$$\mathrm{GL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z}) \cup \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mathrm{SL}(2,\mathbb{Z})$$

and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ corresponds to the switch of the basis vectors $\mathbf{v}, \mathbf{w}$ of the lattice, we obtain

Theorem 1.3. *There is a natural bijective correspondence between proper equivalence classes of positive definite binary forms and lattices in $\mathbb{R}^2$ modulo rotation transformation.*

Let $\mathcal{Q}_2^+$ be the set of positive definite binary quadratic forms on $\mathbb{R}^2$. The group $\mathrm{SL}(2,\mathbb{Z})$ of integral unimodular invertible matrices acts naturally on $\mathcal{Q}_2^+$ by $f \to M^{-1}f$. The map $\mathcal{Q}_2^+ \to \mathbb{R}_+ \times \mathcal{H}$ defined in above is $\mathrm{SL}(2,\mathbb{Z})$-equivariant if we let $\mathrm{SL}(2,\mathbb{Z})$ act on the target by

$$(a,z) \to (a|\gamma z+\delta|^2, M \cdot z).$$

Note that we have restricted ourselves to the subgroup $\mathrm{SL}(2,\mathbb{Z})$ in order to have $\mathrm{Im}\ M \cdot z > 0$.

Using (1.1) we see that the conditions $0 \leq |2b| \leq a \leq c$ correspond to the conditions

$$-\frac{1}{2} \leq \mathrm{Re}\ z \leq \frac{1}{2}, |z| \geq 1, \quad \mathrm{Im}\ z > 0.$$

Let $\mathcal{D}$ be the subset of the upper-half planes described by the above inequalities. It is called the *modular figure* and looks as follows:

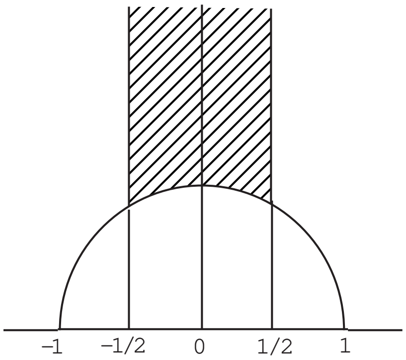

Fig.2

So we have a bijective correspondence between $\bar{\Omega}$ and $\mathbb{R}_+ \times \mathcal{D}$.

Now suppose $f, f' \in \bar{\Omega}$ and $M^{-1} \cdot f = f'$ for some $M \in \mathrm{SL}(2, \mathbb{Z})$. Replacing (f, M) with $(M \cdot f, M^{-1})$, if needed, we may assume that $\mathrm{Im}\ M \cdot z \geq \mathrm{Im}\ z$. The formula (1.3) implies that $|\gamma z + \delta| \leq 1$, where $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. This gives $\gamma \in \{0, 1, -1\}$.

Assume $\gamma = 0$. Then the Moebius transformation defined by M^{-1} is the translation $z \to z + \frac{\beta}{\delta}$ and hence takes z out of the domain $-\frac{1}{2} \leq \mathrm{Re}\ z \leq \frac{1}{2}$ unless $\beta = 0$ or $\beta = \pm 1$ and $\mathrm{Re}\ z = \pm\frac{1}{2}$. In the first case $M = \pm I$ and $f = f'$. In the second case $M = \pm \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$, $f = ax^2 \pm axy + cy^2$ and $f' = ax^2 \mp axy + cy^2$.

Assume $\gamma = \pm 1$. If $\gamma = 1$, then $|z + \delta| \leq 1$ implies

(i) $\delta = 0, |z| = 1$, or

(ii) $z = \rho := \frac{-1+\sqrt{-3}}{2}$ and $\delta = 1$.

In case (i) we have $M = \pm \begin{pmatrix} \alpha & -1 \\ 1 & 0 \end{pmatrix}$ and $M \cdot z = \alpha - \frac{1}{z}$. This easily implies $\alpha = 0$ or $(\alpha, z) = (-1, \rho), (1, -\rho^2)$. So, in the first case, $M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $M \cdot f = cx^2 - 2bxy + ay^2$. Since $(c, b, a) \in \bar{\Omega}$, we get $a = c$. Again f is of the form $ax^2 + 2bxy + ay^2$ and is properly equivalent to $ax^2 - 2bxy + ay^2$.

In the second case $f = a(x^2 + xy + y^2)$ and $Mf = a(x^2 - xy + y^2)$.

Now, in case (ii), we get $M = \begin{pmatrix} \alpha & \alpha - 1 \\ 1 & 1 \end{pmatrix}$ and $M \cdot \rho = (\alpha\rho + (\alpha - 1))/(\rho + 1) = \alpha + \rho$. This implies $\alpha = 0, f = a(x^2 + xy + y^2), Mf = f$.

Finally, the case $\gamma = -1$ is reduced to the case $\gamma = 1$ by replacing M with $-M$.

This analysis proves the following:

Theorem 1.4. *Let $f = ax^2 + 2bxy + cy^2$ and $f' = a'x^2 + 2b'xy + c'y^2$ be two properly reduced positive definite binary forms. Then f is properly equivalent to f' if and only if $f = f'$ or $f = ax^2 \pm axy + cy^2, f' = ax^2 \mp axy + cy^2$, or $f = ax^2 + 2bxy + ay^2, f' = ax^2 - 2bxy + ay^2$. Moreover, $Mf = f$ for some $M \neq \pm I$ if and only if one of the following cases occurs:*

(i) $f = a(x^2 + y^2)$ *and* $M = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$;

(ii) $f = a(x^2 \pm xy + y^2)$ *and* $M = \pm \begin{pmatrix} \mp 1 & -1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

Definition. Let G be a group acting on a set X. A subset S of X is called a *fundamental domain* for the action of G on X if each orbit of G intersects S at exactly one element.

The proof of Theorem 1.4 shows this enlarged set $\bar{\Omega}$ contains a representative of each orbit of $\mathrm{SL}(2, \mathbb{Z})$. Moreover, two points (a, b, c) and (a', b', c') in $\bar{\Omega}$ belong to the same orbit of $\mathrm{SL}(2, \mathbb{Z})$ if and only if either $a = c = a' = c', b = -b'$ or $a' = a, b' = -b = a/2$. Clearly

$$\bar{\Omega} = \mathbb{R}_+ \times \mathcal{D}.$$

To get the fundamental domain for the action of $\mathrm{SL}(2, \mathbb{Z})$ on $\mathcal{Q}_2^+$ we have to consider the subset $\bar{\Omega}'$ of $\bar{\Omega}$ defined by the following inequalities:

$$\bar{\Omega}' = \{(a, b, c) \in \Omega : |2b| < a < c \quad \text{or} \quad a = c \geq 2b > 0 \quad \text{or} \quad a = 2b > 0\}.$$

The corresponding subset of the modular figure is obtained by deleting from it the vertical line Re $z = 1/2$ and the part of the unit circle where the argument is less than $\pi/2$.

Since we do not need we leave it to the reader to state an analog of Theorem 1.3 for reduced (but not properly reduced) forms and find a fundmanetal domain for action of $\mathrm{GL}(2, \mathbb{Z})$ on $\mathcal{Q}_2^+$.

1.5 Theorem 1.4 has a nice application to number theory.

Definition. A binary quadratic form $ax^2 + 2bxy + cy^2$ is called *integral* if $a, 2b, c$ are integers. It is called *primitive* if $(a, 2b, c) = 1$.

Corollary 1.1. . *The set of reduced integral positive definite binary forms with fixed discriminant $D = 4d$ is finite.*

Proof. If we fix the discriminant $D = 4d = 4(b^2 - ac)$, then there are only finitely many points in the domain Ω whose coordinates are integers. $\square$

Definition. We say that two integral positive definite binary forms are in the same *class* if they are properly equivalent.

Corollary 1.2. *The set of classes of primitive integral positive definite binary forms with the same discriminant is finite.*

Exercises

1.1 Let Λ be a lattice in $\mathbb{R}^2$. Show that the number of vertices of shortest distance from the origin can be equal only to $2, 4$ or 6. Find the lattices with 4 and 6 shortest distance points.

1.2 Show that any subgroup of $\mathbb{R}^2$ which is a discrete set (i.e. each ball in $\mathbb{R}^2$ contains only finitely many elements of the set) is a free abelian subgroup of rank at most 2.

1.3 Let Λ be a lattice in $\mathbb{R}^2$. Let us identify $\mathbb{R}^2$ with $\mathbb{C}$ in the usual way. Consider the set $\mathcal{O}_\Lambda$ of complex numbers z such that $z \cdot \Lambda \subset \Lambda$.

(i) Show that $\mathcal{O}_\Lambda$ is a subring of $\mathbb{C}$ and Λ is a module over $\mathcal{O}_\Lambda$;

(ii) Show that $\mathcal{O}_\Lambda = \mathbb{Z}$ unless there exists $c \in \mathbb{C}$ such that $c\Lambda$ is contained in some imaginary quadratic extension $\mathbb{Q}(\sqrt{-d})$ of $\mathbb{Q}$.

1.4 We say that a lattice Λ admits a *complex multiplication* if the ring $\mathcal{O}_\Lambda$ defined in the previous exercise is different from $\mathbb{Z}$. Assume that Λ satisfies this property. Prove the following assertions:

(i) the field of quotients K of $\mathcal{O}_\Lambda$ is a quadratic extension of $\mathbb{Q}$ which contains Λ;

(ii) a distance quadratic form of Λ is proportional to an integral quadratic form;

(iii) the quadratic field K is equal to $\mathbb{Q}(\sqrt{b^2 - ac})$;

(iv) the ring $\mathcal{O}_\Lambda$ is generated over $\mathbb{Z}$ by 1 and $f\omega$, where $\omega = \frac{1+\sqrt{-d}}{2}, f^2 = 4D$ if $d \equiv 1 \bmod (4)$, and $\omega = \sqrt{-d}, f^2 d = D$ otherwise.

1.5 Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field. We shall assume that d is a square free integer. We say that two lattices Λ and Λ' contained in K are similar if $\Lambda' = \alpha\Lambda$ for some $\alpha \in K$.

(i) Find a natural bijective correspondence between the similarity classes of lattices contained in K and the proper equivalence classes of primitive integral positive definite binary forms $ax^2 + 2bxy + cy^2$ which decompose into the product of linear forms over K and whose discriminant $D = 4(ac-b^2)$ is equal to the square of the volume of the fundamental parallelogram of the corresponding lattice.

(ii) Let $ax^2+2bxy+cy^2$ represents a class of primitive integral positive definite binary forms corresponding to the lattice Λ with complex multiplication defined by the ring $\mathcal{O}_\Lambda$. Show that a and $\frac{-b+2\sqrt{b^2-ac}}{2}$ generate a proper ideal in $\mathcal{O}_\Lambda$.

1.6 Let Λ and Λ' be two lattices admitting complex multiplication with $\mathcal{O}_\Lambda = \mathcal{O}_{\Lambda'} = \mathcal{O}$. Define $\Lambda \cdot \Lambda'$ as the subgroup of $\mathbb{C}$ generated by the products $\lambda\lambda', \lambda \in \Lambda, \lambda' \in \Lambda'$.

(i) Show that $\Lambda \cdot \Lambda'$ is a lattice Λ'' with $\mathcal{O}_{\Lambda''} = \mathcal{O}$;

(ii) Show that the operation of product of lattices defined in part (i) is compatible with the similarity relation and defines the structure of a finite abelian group on the set of similarity classes of lattices Λ with the same ring $\mathcal{O}_\Lambda$.

1.7 Using the previous exercises define the structure of an abelian group on the set $C(D)$ of proper equivalence classes of primitive integral positive definite binary forms of given discriminant D.

(i) Compute the product of two forms ax^2+cy^2 and $a'x^2+c'y^2$ with $ac = a'c'$.

(ii) Show that the class of the form x^2+ny^2 (resp. $x^2+xy+ny^2$) is the unit of the group $C(D)$ if $D = 4n$ (resp. if $D = 1+4n$).

(iii) Show that the class of $ax^2-bxy+cy^2$ is the opposite of the class of $ax^2+bxy+cy^2$.

1.8 Using Exercise 1.5 (ii) show that there is a natural isomorphism between the group of similarity classes of lattices with complex multiplication defined by a ring $\mathcal{O}$ and the group $C(\mathcal{O})$ of ideal classes of $\mathcal{O}$.

1.9 Find all reduced primitive integral positive definite quadratic binary forms with discriminant $D = -4, -8, -12, -20, -56$. Compute the number $h(D)$ of classes of primitive integral positive definite quadratic binary forms for these values of D.

1.10 Show that $h(-4n) > 1$ if n is not a prime number.

Lecture 2

Complex Tori

2.1 As we saw in the previous lecture there is a natural bijection between the set $\bar{\Omega}$ of proper equivalence classes of positive definite binary quadratic forms and the product $\mathbb{R}_+ \times \mathcal{D}'$, where $\mathcal{D}'$ is the subset of the modular figure $\mathcal{D}$ whose complement consists of points $\frac{1}{2} + iy$ and $e^{i\phi}, 0 < \phi < \pi/2$. The factor $\mathbb{R}_+$ corresponds to the first coefficient a of the form $f = ax^2 + 2bxy + cy^2$. Now recall that the set of equivalence classes of positive definite binary quadratic formis also bijective to the set of lattices in $\mathbb{R}^2$ modulo orthogonal transformation. The set of proper equivalence classes of positive definite binary quadratic forms corresponds to the set of lattices modulo rotation transformations. Now to get rid of the factor $\mathbb{R}$ let us consider lattices *equivalent* if one is obtained from another by multiplying with a nonzero complex number λ, i.e. $\Lambda \sim \Lambda'$ if $\Lambda' = \{\lambda \mathbf{v} | \mathbf{v} \in \Lambda\}$. Since each complex number can be written in the form $re^{i\phi}$ we see that we allow, additionally to rotations, positive scalar dilations of lattices. If $\mathbf{v}, \mathbf{w}$ is a basis of Λ, then $\lambda\mathbf{v}, \lambda\mathbf{w}$ is a basis of $\lambda\Lambda$. In particular, if $\lambda = r$ is real positive, we get that the corresponding quadratic form $f = ||\mathbf{v}||^2 x^2 + 2\mathbf{v} \cdot \mathbf{w}xy + ||\mathbf{w}||^2 y^2$ is multiplied by r^2. Thus, we may always assume that $||\mathbf{v}||^2 = 1$, hence the equivalence class of Λ is determined by one root $z \in \mathcal{H}$ of the quadratic form f modulo Moebius transformations. Thus we obtain

Theorem 2.1. *There is a natural bijection between the set of equivalence classes of lattices in $\mathbb{R}^2$ and the subset $\mathcal{D}'$ of the modular figure $\mathcal{D}$.*

Now let us find another interpretation of elements from $\mathcal{D}$, this time as isomorphism classes of elliptic curves.

Let Λ be a lattice in $\mathbb{R}^2$. Consider the orbit space

$$E = \mathbb{R}^2/\Lambda.$$

One can choose a representative of each orbit in the *fundamental parallelogram*

$$\Pi = \{x\mathbf{v} + y\mathbf{w} | 0 \leq x, y \leq 1\},$$

where $\mathbf{v}, \mathbf{w}$ is a basis of Λ. In this parallelogram two points belong to the same orbit if and only if they differ by $\mathbf{v}$ or $\mathbf{w}$. So, if we identify the opposite sides of Π, we get a bijective map from Π onto E. Topologically, E is homeomorphic to the torus, or the product of two circles. In fact, as a topological group,

$$\mathbb{R}^2/\Lambda \cong \mathbb{R}^2/\mathbb{Z}^2 \cong (\mathbb{R}/\mathbb{Z}) \times (\mathbb{R}/\mathbb{Z}) \cong S^1 \times S^1.$$

However, we can do more; we put a structure of a complex manifold on E which will depend only on the equivalence class of Λ.

Before we do it let me recall some basics about complex manifolds. Let X be a topological space. A geometric structure on X is defined by assigning to any open subset U of X a certain ring $\mathcal{O}(U)$. Its elements will be interpreted as functions on U. This assignment satisfies the following property:

(i) if $V \subset U$ then there is a unique homomorphism of rings $r_{U/V} : \mathcal{O}(U) \to \mathcal{O}(V)$ such that $r_{W/U} \circ r_{U/V} = r_{W/V}$ whenever $V \subset U \subset W$.

We would like to interpret elements of $\mathcal{O}(U)$ as functions on U and the homomorphism $r_{U/V}$ is as the restriction of functions on U to the subset V. In order to do this, we shall require an additional property. Let x be a point of X. Consider the following equivalence relation on the union of rings $\mathcal{O}(U)$ where U runs through the set of open neighborhoods of x. Let $f \in \mathcal{O}(U), g \in \mathcal{O}(V)$. We say that $f \sim g$ if there exists an open neighborhood W of x contained in $U \cap V$ such that $r_{U/W}(f) = r_{V/W}(g)$. Denote the set of equivalence classes by $\mathcal{O}_x$. There is a natural structure of a ring on $\mathcal{O}_x$ such that for any U containing x the canonical map $\mathcal{O}(U) \to \mathcal{O}_x$ is a homomorphism of rings. We require

(ii) For each $x \in X$ the ring $\mathcal{O}_x$ is a local ring, i.e. contains a unique maximal ideal.

Let $\mathfrak{m}_x$ denotes the unique maximal ideal of $\mathcal{O}_x$ and $\kappa(x) = \mathcal{O}_x/\mathfrak{m}_x$. This is a field. For any open neighborhood U of x there is a canonical homomorphism of rings $\mathcal{O}(U) \to \mathcal{O}_x \to \kappa(x)$ the image of $f \in \mathcal{O}(U)$ in $\kappa(x)$ is called the *value of f at x* and is denoted by $f(x)$. In this way each $f \in \mathcal{O}(U)$ can be considered as a function on U, although at each point x of U the value of f at x may belong to a different field. Of course, we can consider the common set of values by taking the union of all fields $\kappa(x)$. In many special cases, each ring $\mathcal{O}(U)$ is equipped with a structure of an algebra over a field k and the restriction homomorphisms are k-algebra homomorphisms. In this case we may consider k as a subring of $\mathcal{O}(U)$; its elements are called *constant functions*. If are lucky the residue homomorphisms $\mathcal{O}(U) \to \kappa(x)$ induce an isomorphism of fields $k \to \kappa(x)$. In this case we may consider the value of any function on U as an element of the same field k.

A topological space X together with a collection $\mathcal{O}_X$ of the rings $\mathcal{O}_X(U)$ satisfying the previous conditions (i) and (ii) is called a *geometric space*. The collection $\mathcal{O}_X$ is called the *structure sheaf* of the geometric space.

An example of a geometric structure on X is obtained by taking $\mathcal{O}_X(U)$ the ring of continuous real functions on U.

Obviously, a geometric structure $\mathcal{O}_X$ on X equips each open subset $U \subset X$ with the restricted geometric structure. We shall denote it by $\mathcal{O}_U$. A continuous map $f : X \to Y$ of geometric spaces is called a *morphism* of geometric spaces if for any open subset $U \subset Y$ there is a homomorphism of rings $f_U^{\#} : \mathcal{O}_Y(U) \to \mathcal{O}_X(f^{-1}(U))$ satisfying the following properties:

(i) for any $V \subset U$ the following diagram is commutative:

$$\begin{array}{ccc} \mathcal{O}_Y(U) & \xrightarrow{f_U^{\#}} & \mathcal{O}_X(f^{-1}(U)) \\ {\scriptstyle r_{U/V}}\downarrow & & \downarrow{\scriptstyle r_{f^{-1}(U)/f^{-1}(V)}} \\ \mathcal{O}_Y(V) & \xrightarrow{f_V^{\#}} & \mathcal{O}_X(f^{-1}(V)) \end{array}$$

(ii) Let $f(x) = y$ and let $f_{y,x}^{\#} : (\mathcal{O}_Y)_y \to (\mathcal{O}_X)_x$ be defined as follows. Take a representative $\phi \in \mathcal{O}_Y(U)$ of $\bar{\phi} \in (\mathcal{O}_Y)_y$ and define $f_{y,x}^{\#}(\bar{\phi})$ to be the equivalence class of $f_U^{\#}(\phi)$ in $(\mathcal{O}_Y)_x$. It is easy to see that this is wel-defined. We require that $f_{y,x}^{\#}$ maps $\mathfrak{m}_y$ to $\mathfrak{m}_y$.

One interprets the homomorphism $f_U^{\#}$ as the composition of a function on U with the map $f : f^{-1}(U) \to U$. In fact, for each $x \in X$ with $f(x) = y$ the homomorphism $f_{y,x}^{\#}$ induces a homomorphism of fields $\bar{f}_{y,x}^{\#} : \kappa(y) \to \kappa(x)$ such that, for any $\phi \in \mathcal{O}_Y(U), y \in U$,

$$f^{\#}(U)(\phi)(x) = \bar{f}_{y,x}^{\#}(\phi(f(x)))$$

So, a morphism of geometric spaces is a continuous map $f : X \to Y$ which transforms functions on Y to functions on X.

We leave to the reader to define compositions of morphisms of geometric space and to show that the identity map $X \to X$ is a morphism of geometric spaces. This will define a category of geometric spaces. The notion of *isomorphism of geometric spaces* is immediate: it is a morphism of geometric spaces which admits the inverse.

To define a geometric structure on X one need not to define $\mathcal{O}(U)$ for all U; it suffices to do it only for an open set in a base $\{U_i\}_{i \in I}$ of the topology. Then for any open U we set

$$\mathcal{O}(U) = \varprojlim{}_{U_i \subset U} \mathcal{O}(U_i)$$

Here we use the definition of the projective limit: the subset of the product $\prod_{i \in I} \mathcal{O}(U_i)$ which consists of strings $(\ldots, a_i, \ldots, a_j, \ldots)$ such that $r_{U_i/U_k}(a_i) = r_{U_j/U_k}(a_j)$ whenever $U_k \subset U_i \cap U_j$.

We will be mainly concern with an example of a *complex structure*. Let us define it. Let $X = \mathbb{C}^n$ equipped with its standard topology defined by the Euclidean metric $||\mathbf{z}|| = (|z_1|^2 + \ldots + |z_n|^2)^{1/2}$. We define a *complex structure* on X by assigning to each open ball $U_r(\mathbf{a})$ with center at $\mathbf{a}$ and radius r the ring $\mathcal{O}(U_r(\mathbf{a}))$ of complex valued functions on $U_r(\mathbf{a})$ which admit an expansion

$$f(\mathbf{z}) = \sum_{i_1, \ldots, i_n \geq 0} \alpha_{i_1, \ldots, i_n} (z_1 - a_1)^{i_1} \ldots (z_n - a_n)^{i_n}$$

absolutely convergent in $U_r(\mathbf{a})$. A complex valued function on an open set U belongs to $\mathcal{O}(U)$ if and only if for any point $\mathbf{a} \in U$ there exists a ball $U_r(\mathbf{a})$ contained in U such that the restriction of f to it belongs to $\mathcal{O}(U_r(\mathbf{a}))$. Such functions are called *complex analytic* or *holomorphic* functions on U. A non-trivial result from complex analysis says that a function $f = u + iv : U \to \mathbb{C}$ is holomorphic in U if and only if it admits continuous partial derivatives with respect to the real and imaginary coordinates x_i, y_i in $\mathbb{C}^n$ and satisfies the Cauchy-Riemann differential equations in U

$$\frac{\partial}{\partial \bar{z}_i} f(\mathbf{z}) = \frac{1}{2}(\frac{\partial u}{\partial x_i} - \frac{\partial v}{\partial y_i}) + \frac{i}{2}(\frac{\partial u}{\partial y_i} + \frac{\partial v}{\partial x_i}) = 0.$$

We shall denote the ring of holomorphic function on U by $\mathcal{O}^{hol}(U)$. The sheaf defined by the rings $\mathcal{O}^{hol}(U)$ defines a structure of a geometric space on $\mathbb{C}^n$. It is called the *complex affine n-dimensional space.* Clearly the field $\mathbb{C}$ can be identified with constant functions and all residue fields $\kappa(x)$ can be identified with $\mathbb{C}$.

Definition. A geometric space $(X, \mathcal{O})$ with Hausdorff X is called a *complex manifold* of *dimension n* if for each $x \in X$ there exists an open neighborhood U such that the geometric space $(U, \mathcal{O}_U)$ is isomorphic to an open ball in $\mathbb{C}^n$ with the restricted geometric structure of the complex affine n-dimensional space $\mathbb{C}^n$. A complex manifold of dimension 1 is called a *Riemann surface.* A morphism of complex manifolds (not necessary of the same dimension) is called a *holomorphic map.*

A complex manifold is an example of a geometric space $(X, \mathcal{O}_X)$ where the following additional property of $\mathcal{O}_X$ is satisfied:

(ii) Let $U = \cup_{i\in I} U_i$ be an open covering. Suppose that a collection of functions $f_i \in \mathcal{O}(U_i)$ satisfies

$$r_{U_i/U_i\cap U_j}(f_i) = r_{U_j/U_i\cap U_j}(f_j), \quad \forall i, j \in I.$$

Then there exists a unique $f \in \mathcal{O}(U)$ such that, for any $i \in I$, $r_{U/U_i}(f) = f_i$.

Example 2.1. Each non-empty open subset of $\mathbb{C}^n$ with the restricted structure of the geometric space is a complex manifold of dimension n. A map $f : U \to V$ of an open subset of $\mathbb{C}^m$ to an open subset of $\mathbb{C}^n$ is given by n functions $f_i(\mathbf{z})$ (defining the composition $U \to V \hookrightarrow \mathbb{C}^n$). It is holomorphic if and only if each $f_i(\mathbf{z})$ is a holomorphic function on U. More generally, let $f : X \to Y$ be a holomorphic map of complex manifolds. Take an open neighborhood V of a point $y \in f(X)$ isomorphic to an open subset V' of $\mathbb{C}^n$ and let $x \in X$ be mapped to y. Then $f^{-1}(V)$ contains an open neighborhood U of x isomorphic to an open subset U' of $\mathbb{C}^m$. The map $f : U \to V$ defines a map $f' : U' \to V'$ of open subsets of the corresponding complex affine spaces. Then f is holomorphic if and only if f' is holomorphic (for all $x \in X$).

Example 2.2. Let $X = \mathbb{C} \cup \{\infty\}$. Define the topology on X by extending a base of the standard topology on $\mathbb{C}$ by adding open neighborhoods of ∞ of the form

$$U_r(\infty) = \{z \in \mathbb{C} : |z| > r\} \cup \{\infty\}$$

Now extend the structure sheaf $\mathcal{O}^{\mathrm{hol}}$ on $\mathbb{C}$ by adding the rings $\mathcal{O}(U_r(\infty))$, each equal to the ring of complex valued functions $f(z)$ on $U_r(\infty)$ such that $f(1/z) \in \mathcal{O}(U_{1/r}(0))$. We have $X = U_0 \cup U_1$, where $U_0 = U_0(\infty) = X \setminus \{0\}$ and $U_1 = U_\infty(0) = X \setminus \{\infty\} = \mathbb{C}$. The homeomorphism $\tau : U_0 \to U_1$ defined by the formula $z \to 1/z$ is an isomorphism of the geometric spaces. In fact f is holomorphic on an open $U \subset U_1$ if and only if $f(1/z)$ is holomorphic on $\tau^{-1}(U)$. Since U_0 is obviously isomorphic to $\mathbb{C}$, we obtain that X is a geometric space. It is called the *Riemann sphere* or *complex projective line* and is denoted by $\mathbb{CP}^1$. Using the stereographic projection, we see that $\mathbb{CP}^1$ is homeomorphic to a two-dimensional sphere.

Remark 2.1. A more traditional way to define a structure of a complex manifold is by using *local charts.* A collection of $\{(U_\alpha, \phi_\alpha)\}$ of open subsets U_α of X together with homeomorphisms ϕ_α from U_α to an open subset of $\mathbb{C}^n$ is called a local chart if $X = \cup_\alpha U_\alpha$ and, if $U_\alpha \cap U_\beta \neq \emptyset$, the map $\phi_\beta \circ \phi_\alpha^{-1} : \phi_\alpha(U_\alpha \cap U_\beta) \to \phi_\beta(U_\alpha \cap U_\beta)$ is holomorphic. Two local charts are called equivalent if their union is a local chart. A structure of a complex manifold of dimension n on X is an equivalence class of local charts. We leave it as an exercise to check that the two definitions are equivalent.

Let G be a group which *acts holomorphically* on a complex manifold X. This means that for each $g \in G$ the map $\mu(g) : x \to g \cdot x$ is holomorphic. It follows from the definition of an action of a group on a set that $\mu(g^{-1})$ is the holomorphic inverse of $\mu(g)$. Thus each $\mu(g)$ is an automorphism of the complex manifold X. We would like to equip the set of orbits X/G of G with a structure of a complex manifold. We restrict ourselves with the case when G acts *properly discontinuously* on X. This means that for any compact subsets A, B of X the set $\{g \in G : g(A) \cap B \neq \emptyset\}$ is finite. In particular, for any $x \in X$ the stabilizer subgroup $G_x = \{g \in G : g \cdot x = x\}$ is finite.

Theorem 2.2. *Let G be a group which acts holomorphically and properly discontinuously on a Riemann surface X. Then the orbit space X/G admits a structure of a Riemann surface such that the canonical map $p : X \to X/G$ is holomorphic. This structure is unique up to isomorphism.*

Proof. First we define the topology on X/G. This is standard. By definition a subset of X/G is open if its pre-image $p^{-1}(U)$ is an open subset of X. Now we define the structure sheaf. By definition

$$\mathcal{O}_{X/G}(U) = \mathcal{O}_X(p^{-1}(U))^G :=$$

$$\{f \in \mathcal{O}_X(p^{-1}(U)) : f(g \cdot x) = f(x), \forall g \in G, x \in p^{-1}(U)\}$$

It is immediately verified that this defines a structure of a geometric space on $Y = X/G$. Let us show that it is isomorphic to a Riemann surface. Let $y = G \cdot x$ be an orbit, considered as a point of Y. Since X is locally homeomorphic to $\mathbb{R}^2$, it is locally compact. Thus x contains an open neighborhood U whose closure $\bar{U}$ is compact. Let $U = U_1 \supset U_2 \supset \ldots$ be a sequence of strictly decreasing open neighborhoods of x with $\cap_n U_n = \{x\}$. Since each U is relatively compact and G acts properly discontinuously, the set $G(n) = \{g \in G : U_n \cap g(U_n) \neq \emptyset\}$ is finite. Clearly $G(n) \subset G(m)$ for $m < n$. Thus there exists some N such that $G(m) = G(N)$ for all $m \geq N$. I claim that $G(N) \subset G_x$. In fact, if this is false $g \cdot x = x' \neq x$ for some $g \in G(N)$. The map $g : X \to X$ matches the filter of open neighborhoods U_n of x with the filter of open neighborhoods $g(U_n)$ of x'. Since our topology is separated, we can find an open subset U_n with large enough n such that $g(U_n) \cap U_n = \emptyset$. However this contradicts the definition of $G(N)$. So $G(N) \subset G_x$. Obviously, $G_x \subset G(N)$. Thus $G(N) = G_x$, and in particular is finite. Therefore the set $\cap_{g \in G_x} g(U_N)$ is an open neighborhood of x. It is invariant with respect to G_x. Moreover, for any $x', x' \in U_N$ we have $x'' = g \cdot x'$ for some $g \in G$ implies $g \in G_x$. In particular $g(U_N) \cap g'(U_N) \neq \emptyset$ if and only if g, g' belong to the same coset of G modulo the subgroup G_x. Thus

$$p^{-1}(p(U_N)) = \cup_{g \in G} g(U_N) = \coprod_{gG_x \in G/H} g(U_N)$$

is the disjoint union of open subsets homeomorphic to U_N, and hence is open. This implies that $V = p(U_N)$ is an open neighborhood of $y = Gx$ in Y. Since each G-invariant function on $p^{-1}(V)$ is determined uniquely by its values on U_N we obtain

$$\mathcal{O}_Y(V) \cong \mathcal{O}(U_N)^{G_x}$$

If we replace V by a smaller open subset V' and replace U_N with $U'_N = U_N \cap p^{-1}(V')$ we similarly get

$$\mathcal{O}_Y(V') \cong \mathcal{O}(U'_N)^{G_x}$$

This shows that V is isomorphic, as a geometric space, to the orbit space U_N/G_x. In fact the isomorphism is induced by the restriction of the morphism $p: X \to X/G$ of geometric spaces to U_N. Its fibres are G_x-orbits in U_x. Thus we have reduced our assertion to the case when the group G is finite and also fixes a point $x \in X$. Now we have to use the assumption that X is of dimension 1. Without loss of generality we may assume that X is an open ball of finite radius r in $\mathbb{C}$ with center at the origin. For each $g \in G$ the map $\mu(g): X \to X$ is given by a holomorphic function $f(z)$ with $f'(z) \neq 0$ at each point in X and $f(0) = 0$. An elementary theorem from the theory of functions in one complex variable says that $f(z) = ze^{i\theta}$, i.e. g defines a rotation of the ball. Since G_x is of finite order, we obtain that $e^{id\theta} = 1$ for some $d \geq 1$. We also see that G_x is a cyclic group of order d. Now any function $\phi(z)$ invariant with respect to the transformations $z \to z\eta, \eta^d = 1$ must be a holomorphic function in $t = z^d$. This easily follows by considering the Taylor expansion of $\phi(z)$ at 0. Now it is easy to see that the map $z \to z^d$ defines an isomorphism of geometric spaces $U_r(0)/G \to U_{r^d}(0)$. This proves the assertion. □

Remark 2.2. It follows from the proof that the assertion of the theorem remains true in any dimension if we additionally assume that G acts freely on X, i.e., the stabilizer subgroup G_x of any point $x \in X$ is trivial. In general case X/G is not a complex manifold but an *analytic space* with quotient singularities (also called a complex *orbitfold*).

Corollary 2.1. *Let us identify $\mathbb{R}^2$ with $\mathbb{C}$ in the natural way. Then $E = \mathbb{R}^2/\Lambda$ admits a structure of a compact complex manifold of dimension 1 for which the factor map $\mathbb{C} \to E$ is a holomorphic map of complex manifolds.*

Proof. The group Λ acts on the complex manifold $\mathbb{C}$ by translations $z \to z + \lambda, \lambda \in \Lambda$. This action is obviously properly discontinuous. In fact any compact set B in $\mathbb{C}$ is contained in a finite union of λ-translates of the fundamental paralellogram

$$\Pi = \{z \in \mathbb{C} : z = a\omega_1 + b\omega_2, 0 \leq a, b \leq 1\},$$

where ω_1, ω_2 is a basis of Λ. Thus for any compact set A, we have $(m_1\omega_1 + m_2\omega_2 + A) \cap B = \emptyset$ if $|m_1|, |m_2|$ are sufficiently large. This leaves us only with finitely many λ such that $(\lambda + A) \cap B \neq \emptyset$. □

Definition. A Riemann surface X is called a *complex torus* of dimension 1 or an *elliptic curve* if it is isomorphic to $\mathbb{C}/\Lambda$ for some lattice Λ.

Theorem 2.3. *Two elliptic curves $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic if and only if $\Lambda' = a\Lambda$ for some $a \in \mathbb{C} \setminus \{0\}$.*

Proof. We shall use the simple observation that the geometric spaces $\mathbb{C}$ and $E = \mathbb{C}/\Lambda$ are locally isomorphic. This means that for any point $z \in \mathbb{C}$ has a neighborhood isomorphic to an open neighborhood of $z + \Lambda \in E$. This follows immediately from the proof of Theorem 2.2. Assume $\Lambda' = a\Lambda$ for some non-zero complex number a. Consider the map $\mathbb{C} \to \mathbb{C}$ defined by the formula $z \to az$. It is an automorphism of the complex manifold $\mathbb{C}$ which maps Λ onto Λ'. It induces a bijective map of the orbit spaces $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$. It follows from the previous remark that this map is holomorphic.

Conversely, assume that there is a holomorphic isomorphism $f: E = \mathbb{C}/\Lambda \to E' = \mathbb{C}/\Lambda'$. Let $f(0 + \Lambda) = z_0 + \Lambda'$. Consider the map $t_{z_0}: E \to E'$ defined by the formula $z + \Lambda \to (z + z_0) + \Lambda'$. It is easy to see that it is a holomorphic automorphism. Composing f with $t_{-z_0} = t_{z_0}^{-1}$ we may assume that $f(0 + \Lambda) = 0 + \Lambda'$. Now we use that the projection maps $p : \mathbb{C} \to \mathbb{C}/\Lambda$ and $p' : \mathbb{C} \to \mathbb{C}/\Lambda'$ are universal covers of the topological spaces. The composition $\mathbb{C} \to \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is a continuous map of a simply-connected topological space $\mathbb{C}$ to the torus $\mathbb{C}/\Lambda'$. It has a unique lift to a homeomorphism $\tilde{f} : \mathbb{C} \to \mathbb{C}$ of the universal covers. It is also a holomorphic map satisfying $\tilde{f}(0) \in \Lambda'$. In fact, the composition $p' \circ \tilde{f}$ is equal to $f \circ p$ and hence is holomorphic. This easily implies that $\tilde{f}$ is holomorphic. Now for any $\lambda \in \Lambda$ and $z \in \mathbb{C}$ we have $\tilde{f}(z+\lambda) - \tilde{f}(z) \in \Lambda'$. Thus the continuous map $z \to \tilde{f}(z+\lambda) - \tilde{f}(z) \in \Lambda'$ is constant and hence $\tilde{f}(z+\lambda) = \tilde{f}(z) + \tilde{f}(\lambda)$. This shows that the partial derivatives of $\tilde{f}$ are periodic with respect to Λ. By Liouville's theorem, they must be constant. Hence $\tilde{f}$ is a linear map of $\mathbb{C}$ which maps Λ to Λ'. ☐

Corollary 2.2. *There exists a natural bijection between the set of isomorphism classes of elliptic curves and the modular figure $\mathcal{D}$.*

The group law on $\mathbb{C}$ defines a group law of the quotient group $\mathbb{C}/\Lambda$. It follows from the previous theorem that any holomorphic isomorphism of elliptic curves which sends 0 to 0 is a homomorphism of groups. The group of holomorphic group automorphisms of the elliptic curve $\mathbb{C}/\Lambda$ is isomorphic to the group $\{a \in \mathbb{C}^* : a\Lambda = \Lambda\}$. Let ω_1, ω_2 be a basis of Λ. Replacing Λ with $z\Lambda$ for some $z \in \mathbb{C}^*$ we may assume that $\omega_1 = 1, \omega_2 = \omega \in \mathcal{H}$. Then

$$a\omega = \alpha\omega + \beta, \quad a \cdot 1 = \gamma\omega + \delta,$$

for some integral invertible (over $\mathbb{Z}$) matrix $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. This shows that the vector $(\omega, 1) \in \mathbb{C}^2$ is a complex eigenvector of M with eigenvalue a. The eigenvalue $a = x + iy$ satifies the characteristic equation

$$t^2 - (\alpha+\delta)t + \det M = 0.$$

We have $a + \bar{a} = 2x = -(\alpha+\delta) \in \mathbb{Z}$ and $|a| = x^2 + y^2 = \det M = 1$. The only solutions are

$$(x, y) = (0, \pm 1), (\pm 1, 0), (\pm\frac{1}{2}, \pm\sqrt{3/2}).$$

This gives

$$a = \pm i, \pm 1, \pm e^{2\pi/3}, \pm e^{4\pi/3}.$$

Thus there are the following possibilities for the group G of holomorphic group automorphisms of elliptic curve:

$$G \cong \mathbb{Z}/2, \mathbb{Z}/4, \mathbb{Z}/6.$$

The first case is realized for any lattice Λ. The second case is realized by the lattice $\mathbb{Z} + \mathbb{Z}i$. The third case is realized by the lattice $\mathbb{Z} + \mathbb{Z}e^{2\pi/3}$.

Let us show that any elliptic curve with $G \neq \{\pm\}$ is isomorphic to either $E_i = \mathbb{C}/\mathbb{Z} + \mathbb{Z}i$ or $E_\rho = \mathbb{C}/\mathbb{Z} + \mathbb{Z}e^{2\pi i/3}$. By Corollary 2.3, we may assume that ω belongs to the modular figure. Thus $|\text{Re}\ \omega| \le 1/2$ and $|\omega| \ge 1$. We already noticed in Lecture 1 that the derivative of the Moebius transformation $z \to \frac{\alpha z + \beta}{\gamma z + \delta}$ at the point z_0 is equal to $(cz_0 + d)^{-2}$. Since $a^d = 1$ for some $d > 0$, the matrix M is of finite order. This implies that the derivative of the corresponding Moebius transformation is a complex root of 1. In particular, we have $|\gamma\omega + \delta| = 1$. This implies

$$|\omega| = \left|\frac{\alpha\omega + \beta}{\gamma\omega + \delta}\right| = \frac{|(\alpha\omega + \beta)(\gamma\bar{\omega} + \delta)|}{|\gamma\omega + \delta|^2} = |(\alpha\omega + \beta)(\gamma\bar{\omega} + \delta)|.$$

Since $|\omega| \geq 1$,and $\alpha\delta - \beta\gamma = 1$ this gives $|\alpha\omega + \beta|, |\gamma\bar{\omega} + \delta| \geq 1$. Thus

$$|\omega| \geq |\alpha\omega + \beta| \geq |\alpha||\omega|, \quad |\omega| \geq |\gamma\bar{\omega} + \delta| \geq |\gamma||\omega|.$$

Assume $\alpha \neq 0$. Then we must have $|\alpha| = 1, \beta = 0, |\omega| = 1$. Assume $\gamma \neq 0$. Then we must have $|\gamma| = 1, \delta = 0, |\omega| = 1$. Thus we have the following possibilities for the matrix M:

$$M = \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

This gives the following possibilities for ω:

$$\omega = i, M = \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, G \cong \mathbb{Z}/4.$$

$$\omega = e^{2\pi i/3}, M = \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, G \cong \mathbb{Z}/6.$$

This proves the assertion.

Moreover we have shown that the group $\mathrm{PSL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/\pm 1$ acts on the upper half-plane $\mathcal{H}$ freely except at the orbits of the points $\omega = i, e^{2\pi i/3}$. The stabilizer group $\mathrm{P}SL(2,\mathbb{Z})_i \cong \mathbb{Z}/2, \mathrm{PSL}(2,\mathbb{Z})_{e^{2\pi i/3}} = \mathbb{Z}/3$. The elliptic curves corresponding to these two exceptional orbits are called *harmonic* (resp. *anharmonic*).

Exercises

2.1 Let X be the set of prime numbers in $\mathbb{Z}$ together with 0. Define a topology on X by declaring that sets of the form $V(n) = \{p \in X : p|n\}, n \in \mathbb{Z}$ are closed. For each open set $D(n) = X \setminus V(n)$ take $\mathcal{O}(D(n))$ to be the ring of rational numbers whose denominators are products of powers of prime divisors of n. Show that this defines a geometric structure on X. Show that $\kappa(x) = \mathbb{F}_p$, the prime field of p elements, if $x = p$ is prime and the field of rational numbers $\mathbb{Q}$ otherwise. Show that for any $f = a/b \in \mathcal{O}(D(n))$ the value of f at x is equal to itself if $x = 0$ and is equal to $\frac{a \bmod p}{b \bmod p}$ if $x = p$ is prime.

2.2 Using the notion of a geometric structure give a definition of a differentiable manifold of class C^k.

2.3 Show that the projective space $\mathbb{P}^n(\mathbb{C})$ (defined as the set of one-dimensional linear subspaces in $\mathbb{C}^{n+1}$) has a structure of a complex manifold of dimension n. Show that the natural map $\mathbb{C}^{n+1} \setminus \{0\} \to \mathbb{P}^n(\mathbb{C})$ defined by sending $\mathbf{z} = (z_0, \ldots, z_n)$ to the line $\mathbb{C}\mathbf{z}$ is a holomorphic map.

2.4. Let $(X, \mathcal{O}_X)$ be a geometric space. Assume that the value of $f \in \mathcal{O}(U)$ at a point $x \in U$ is not equal to zero. Prove that the restriction of f to some open neighborhood V of x is an invertible element of $\mathcal{O}(V)$.

2.5 Prove that any holomorphic function $f : X \to \mathbb{C}$ defined on a connected compact Riemann surface must be a constant function.

2.6 Let Λ be a lattice with complex multiplication (see Exercise 1.4). Show that the ring $\mathcal{O}_\Lambda$ is isomorphic to the ring of holomorphic group endomorphisms of the elliptic curve $\mathbb{C}/\Lambda$.

2.7 Let A be a cyclic subgroup of the multiplicative group $\mathbb{C}^*$ of the field $\mathbb{C}$ generated by a complex number q with $|q| \neq 1$. Show that the factor group $\mathbb{C}^*/A$ has a structure of a complex manifold of dimension 1 isomorphic to an elliptic curve.

2.8 Generalize the construction of an elliptic curve by showing that a quotient group $\mathbb{C}^n$ modulo the subgroup Λ generated by $2n$ vectors linearly independent over $\mathbb{R}$ has a structure of a compact complex manifold of dimension n. It is called a *complex torus* of dimension n.

2.9 Consider the action of the group $G = \{\pm 1\}$ on $\mathbb{C}^2$ defined by sending (z_1, z_2) to $(-z_1, -z_2)$. Show that $\mathbb{C}^2/G$ does not admit a structure of a complex manifold such that the canonical map $\mathbb{C}^2 \to \mathbb{C}^2/G$ is holomorphic. However $\mathbb{C}^2 \setminus \{0\}/G$ is a complex manifold of dimension 2.

2.10 Let $P(z_1, \ldots, z_n) : \mathbb{C}^n \to \mathbb{C}$ be a complex polynomial in n variables. Assume $\frac{\partial P}{\partial z_1}(a_1, \ldots, a_n) \neq 0$, where $P(a_1, \ldots, a_n) = 0$. Show that there exists an open neighborhood U of the point $(a_1, \ldots, a_n)$ such that $U \cap P^{-1}(0)$ is a complex manifold of dimension $n-1$. Generalize this to the case of a polynomial map $\mathbb{C}^n \to \mathbb{C}^k$.

2.11 Let $P(z_0, \ldots, z_n) : \mathbb{C}^n \to \mathbb{C}$ be a complex homogeneous polynomial in $n+1$ variables. Assume that the equations $\frac{\partial P}{\partial z_i} = 0, \quad i = 0, \ldots, n$ have no common solutions in $\mathbb{C}^{n+1} \setminus \{0\}$. Show that the set of zeroes of P, considered as a subset of projective space $\mathbb{P}^n(\mathbb{C})$ is a complex manifold of dimension $n-1$. Generalize this to the case of the set of zeroes in $\mathbb{P}^n(\mathbb{C})$ of a finite set of homogeneous polynomials.

Lecture 3

Theta Functions

3.1 It is known that a compact smooth manifold of dimension n can be always embedded in $\mathbb{R}^{2n+1}$. This theorem does not have its analog in the complex case. A compact complex manifold cannot be embedded in $\mathbb{C}^N$ for any N. This follows from the fact that any holomorphic function on a connected compact complex manifold must be a constant function. However, it is often possible to embed a complex manifold into projective space $\mathbb{P}^n(\mathbb{C})$. A theorem of Chow says that in this case the complex manifold is isomorphic to a projective algebraic complex manifold. The latter is defined as the set of solutions in $\mathbb{P}^n(\mathbb{C}))$ of a system of homogeneous algebraic equations

$$f_1(x_0, \ldots, x_n) = \ldots = f_N(x_0, \ldots, x_n) = 0. \tag{3.1}$$

This system must satisfy the following smoothness conditions:

(i) the polynomials $f_1, \ldots, f_N$ generate a prime ideal I_X in the ring of polynomials $\mathbb{C}[x_0, \ldots, x_n]$;

(ii) the rank r of the matrix

$$J = \begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \ldots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_N}{\partial x_0} & \ldots & \frac{\partial f_N}{\partial x_n} \end{pmatrix} (a_0, \ldots, a_n) \tag{3.2}$$

does not depend on the point $(a_0, \ldots, a_n)$ satisfying the equations (3.1).

The number $d = n - r$ is equal to the dimension of the complex manifold defined by (3.1) (see Exercise (2.11)). Not every complex manifold X can be given in this way. A necessary (but not sufficient) condition is that the field $\mathcal{M}(X)$ of meromorphic functions on X has the transcendence degree over $\mathbb{C}$ equal to the dimension of X. A *meromorphic function* is defined by choosing a covering of X by open connected subsets U_i and assigning to each U_i an elements f_i of the field $\mathcal{M}(U_i)$ of quotients of $\mathcal{O}(U)^{\mathrm{hol}}$ with the compatibility condition $f_i = f_j$ in $\mathcal{M}(U_i \cap U_j)$. Here we use the fact that $\mathcal{O}(U_i)^{\mathrm{hol}}$ does not have zero divisors. The transcendence degree of the field $\mathcal{M}(X)$ over $\mathbb{C}$ is always less or equal to the dimension of X (see [**Shafarevich**], vol. 2, Chapter 8, §2). If X is a projective algebraic complex manifold, then its field of meromorphic functions coincides with the field of rational functions. A *rational* *function* is an element of the field $\mathcal{R}(X)$ generated by fractions $\frac{P_k(x_0,\dots,x_n)}{Q_k(x_0,\dots,x_n)}$ formed by homogeneous polynomials of the same degree considered modulo the ideal I_X. The transcendence degree of this field is always equal to $n-r$. Dropping the condition (ii), we obtain the definition of an irreducible complex projective *algebraic variety.* Its dimension is equal to the $n-r$, where r is the maximal value of the rank of the Jacobian matrix.

We shall prove later that any compact complex manifold of dimension 1 is isomorphic to a projective algebraic complex manifold (a smooth projective curve). In this lecture we shall find such an isomorphism explicitly for complex tori $X=\mathbb{C}/\Lambda$. Let us try to find a non-constant map $f: X\to\mathbb{P}^n(\mathbb{C})$. Recall that the complex projective space $\mathbb{P}^n(\mathbb{C})$ is defined as the set of lines in $\mathbb{C}^{n+1}$, or equivalently as the set of non-zero vectors $(z_0,\dots,z_n)\in\mathbb{C}^{n+1}$ considered up to multiplicatication by a non-zero scalar. The set $\mathbb{P}^n(\mathbb{C})$ is a complex manifold of dimension n. It is covered by $n+1$ subsets $U_i=\{(z_0,\dots,z_n): z_i\neq 0\}$ each isomorphic to $\mathbb{C}^n$ (see Exercise 2.3). A holomorphic map $f: X\to\mathbb{CP}^n$, after composing with the natural map $\mathbb{C}\to\mathbb{C}/\Lambda$, is defined by $n+1$ holomorphic functions $f_0,\dots,f_n$ on $\mathbb{C}$ which need not be periodic with respect to Λ but must satisfy the weaker property:

$$f_i(z+\lambda)=e_\lambda(z)f_i(z),\quad i=0,\dots,n,\quad \lambda\in\Lambda,$$

where $e_\lambda(z)$ is a holomorphic invertible function on $\mathbb{C}$. Let us try to find such functions.

Definition. A holomorphic function $f(z)$ on $\mathbb{C}$ is called a *theta function* with respct to a lattice Λ if, for any $\lambda\in\Lambda$ there exists an invertible holomorphic function $e_\lambda(z)$ such that

$$f(z+\lambda)=e_\lambda(z)f(z),\quad \forall z\in\mathbb{C}.$$

The set of functions $\{e_\lambda(z)\}$ is called the *theta factor* of f.

Example 3.1. Let $\Lambda=\mathbb{Z}+\mathbb{Z}\tau$, where $\tau\in\mathcal{H}$. We know that each lattice can be reduced to this form by means of a homothety transformation. Set

$$\Theta(z;\tau)=\sum_{n\in\mathbb{Z}}e^{i\pi(n^2\tau+2zn)}.$$

This function is holomorphic on $\mathbb{C}$. In fact, we shall show that the series converges uniformly on any bounded set in $\mathbb{C}$. Then we can differentiate the series and see that the derivative with respect to $\bar z$ is zero. Thus the series represents a holomorphic function on $\mathbb{C}$. Assume that on a bounded set we have $|\mathrm{Im}\ z|<c$. Then

$$\sum_{n\in\mathbb{Z}}|e^{i\pi(n^2\tau+2zn)}|\le\sum_{n\in\mathbb{Z}}e^{-\pi n^2\mathrm{Im}\ (\tau)}e^{2\pi cn}.$$

Choose N such that $e^{-\pi n\mathrm{Im}\ (\tau)}e^{2\pi c}<1$ for $n\ge N$. Then

$$\sum_{n\in\mathbb{Z}}e^{-\pi n^2\mathrm{Im}\ (\tau)}e^{2\pi cn}<\sum_{n\in\mathbb{Z}}e^{-\pi n(n-N)\mathrm{Im}\ (\tau)}.$$

The latter series is obviously converges.

Now let us check that $\Theta(z;\tau)$ is a theta function. Obviously it is periodic with respect to $z\to z+m, m\in\mathbb{Z}$. We also have

$$\Theta(z+\tau;\tau)=\sum_{n\in\mathbb{Z}}e^{i\pi(n^2\tau+2zn+2\tau n)}=\sum_{n\in\mathbb{Z}}e^{i\pi((n+1)^2\tau+2z(n+1)-\tau-2z)}=$$

$$e^{i\pi(-\tau-2z)}\sum_{n\in\mathbb{Z}}e^{i\pi((n+1)^2\tau+2z(n+1)}=e^{-\pi i(\tau+2z)}\Theta(z;\tau).$$

Proceeding by induction we see, for any $\lambda = m + n\tau \in \Lambda$, we have

$$\Theta(z+m+n\tau;\tau)=e^{-\pi i(n^2\tau+2nz)}\Theta(z;\tau),$$

so that $\Theta(z;\tau)$ is a theta function with the theta factor

$$e_{m+n\tau}(z)=e^{-i\pi(n^2\tau+2nz)}.$$

This theta function is called the *Riemann theta function.*

3.2 How to find a general form of a theta function? First notice that the theta factor satisfies the following condition:

$$e_{\lambda+\lambda'}(z)=e_\lambda(z+\lambda')e_{\lambda'}(z). \tag{3.3}$$

This follows from comparing the equalities:

$$f(z+\lambda+\lambda')=e_{\lambda+\lambda'}(z)f(z),$$

$$f(z+\lambda+\lambda')=e_\lambda(z+\lambda')f(z+\lambda')=e_\lambda(z+\lambda')e_{\lambda'}(z)f(z).$$

Let $\phi(z) \in \mathcal{O}(\mathbb{C})^*$ be a holomorphic invertible function on $\mathbb{C}$. For any theta function $f(z)$ with theta factor $e_\lambda(z)$ the function $f(z)\phi(z)$ is also a theta function with the theta factor

$$e_\lambda(z)'=e_\lambda(z)\phi(z+\gamma)\phi(z)^{-1}. \tag{3.4}$$

Definition. A set of holomorphic invertible functions $\{e_\lambda\}_{\lambda\in\Lambda}$ satisfying the functional equation (3.3) is called a *theta factor* with respect to the lattice Λ. Two theta factors $\{e_\lambda\}_{\lambda\in\Lambda}$ and $\{e_\lambda\}'_{\lambda\in\Lambda}$ are called *equivalent* if they either related by (3.4) for some invertible holomorphic function $\phi(z)$ or are obtained from each other by translation of the argument $z \to z + a$.

Let $\mathrm{Th}(\{e_\lambda\};\Lambda)$ denote the set of theta functions with theta factor $\{e_\lambda\}$. Obviously it is a subspace of the space $\mathcal{O}(\mathbb{C})$ of holomorphic functions on $\mathbb{C}$. Notice that for any $f, g \in \mathrm{Th}(\{e_\lambda\};\Lambda)$ the meromorphic function f/g is periodic with respect to Λ. So, it defines a meromorphic function on $\mathbb{C}/\Lambda$. Such functions are called *elliptic functions.*

We have

$$\mathrm{Th}(\{e_\lambda\};\Lambda)\cong\mathrm{Th}(\{e'_\lambda\};\Lambda)$$

if $\{e_\lambda\}$ is equivalent to $\{e'_\lambda\}$. The isomorphism is defined by composition of multiplication with a function ϕ^{-1} defined by (3.4) and the inverse image under the translation map $z \to z + a$.

One can show, we don't really need it, that it is possible to find $\phi(z)$ such that $\log(e_\gamma(z)\phi(z+\gamma)\phi(z)^{-1})$ depends linearly on z. Thus the theta factor $e_\lambda(z)'$ looks like

$$e_\lambda(z)'=e^{-2\pi i(a_\lambda z+b_\lambda)}.$$

Further replacing $f(z)$ by $f(z)e^{2\pi i(\frac{1}{2}a_1z^2+(b_1-\frac{a_1}{2})z)}$ we may assume that $a_1 = b_1 = 0$. In particular

$$f(z+1) = f(z), \quad f(z+\tau) = e^{-2\pi i(az+b)}f(z). \tag{3.5}$$

Now we have

$$f(z+\tau+1) = f((z+\tau)+1) = f(z+\tau) = e^{-2\pi i(az+b)}f(z)$$

$$f(z+\tau+1) = f((z+1)+\tau) = e^{-2\pi i(a(z+1)+b)}f(z) = e^{-2\pi ia}e^{-2\pi i(az+b)}f(z).$$

By comparison, we see that $e^{-2\pi ia} = 1$, hence $a = k$ for some $k \in \mathbb{Z}$. The first equality allows us to expand $f(z)$ in a Fourier series

$$f(z) = \sum_{n\in\mathbb{Z}} c_n e^{2\pi inz}, \quad c_n \in \mathbb{C}.$$

Replacing z with $z+\tau$, we obtain

$$f(z+\tau) = \sum_{n\in\mathbb{Z}} c_n e^{2\pi in\tau} e^{2\pi inz} = e^{-2\pi i(kz+b)}f(z) =$$

$$\sum_{n\in\mathbb{Z}} c_n e^{-2\pi ib} e^{2\pi i(n-k)z} = \sum_{n\in\mathbb{Z}} c_{n+k} e^{-2\pi ib} e^{2\pi inz}.$$

Comparing the coefficients at $e^{2\pi inz}$ we get

$$c_{n+k} = c_n e^{2\pi i(n\tau+b)}. \tag{3.6}$$

If $k = 0$ we must have $c_n = 0$ except maybe for one value N of n satisfying $N\tau + b \in \mathbb{Z}$. This gives

$$f(z) = c_N e^{2\pi iNz}.$$

If $k \neq 0$ we get a recursion for the coefficients. Assume $k < 0$. Let $c_N \neq 0$ for some $N \geq 0$. Then $|c_{N-k}| = |c_N e^{-2\pi i(N\tau+b)}|$. Since Im $\tau > 0$, the absolute value of the coefficients $c_{N-sk}, s \geq 1$, will not go to zero and the Fourier series will diverge. Similarly, if $c_N \neq 0$ for some $N < 0$, we get $|c_{N+sk}|, s \geq 1$, do not go to zero and again the series diverges. It remains to consider the case $k > 0$. In this case all coefficients are determined by k coefficients $c_0, \ldots, c_{k-1}$. In fact, we can solve the recurency explicitly. To simplify the computations, let us replace $f(z)$ with $f(z+\frac{\tau}{2}-\frac{b}{k})$. Then

$$\begin{aligned} f(z+\frac{\tau}{2}-\frac{b}{k}+1) &= f(z+\frac{\tau}{2}-\frac{b}{k}), \\ f(z+\frac{\tau}{2}-\frac{b}{k}+\tau) &= e^{-2\pi i(k(z+\frac{\tau}{2}-\frac{b}{k})+b)}f(z+\frac{\tau}{2}-\frac{b}{k}) = \\ &\quad e^{-2\pi i(kz+k\frac{\tau}{2})}f(z+\frac{\tau}{2}-\frac{b}{k}). \end{aligned} \tag{3.7}$$

So we may assume that

$$b = k\tau/2.$$

Let $s \in \{0, \dots, k-1\}$. Then it is easy to check that

$$c_{s+rk} = e^{\pi i[(s+rk)^2 \tau/k]} c_s \tag{3.8}$$

is the explicit solution of the recurrency 3.6. This shows that each $f(z)$ with the theta factor

$$e_{m+n\tau}(z) = e^{-2\pi i k(nz + \frac{n^2}{2}\tau)} \tag{3.9}$$

can be written in the form

$$f(z) = \sum_{s=0}^{k-1} c_s \Theta_s(z;\tau)_k,$$

where

$$\Theta_s(z;\tau)_k = \sum_{r\in\mathbb{Z}} e^{\pi i[(s+rk)^2\tau/k]} e^{2\pi i z(s+rk)}, \quad s = 0, \dots, k-1.$$

It is convenient to rewrite these functions in the form

$$\Theta_s(z;\tau)_k = \sum_{r\in\mathbb{Z}} e^{\pi i[(\frac{s}{k}+r)^2 k\tau + 2kz(\frac{s}{k}+r)]}.$$

It is easy to see using the uniqueness of Fourier coefficients for a holomorphic function that the functions $\Theta_s(z)_k$ are linearly independent and hence form a basis of the space of theta functions with the theta factor (3.9).

3.3 Summarizing the previous computations, we obtain

Theorem 3.1. *Each theta factor is equivalent to the theta factor of the form*

$$e_{m+n\tau}(z) = e^{-2\pi i(nkz + \frac{n^2}{2}k\tau)}.$$

The space $\mathrm{Th}(k;\Lambda_\tau)$ *of theta functions with theta factor of this form is zero for* $k < 0$*. For* $k = 0$ *it consists of constant functions. For* $k > 0$ *it is of dimension* k *and is spanned by the functions*

$$\Theta_s(z;\tau)_k = \sum_{r\in\mathbb{Z}} e^{\pi i[(\frac{s}{k}+r)^2 k\tau + 2kz(\frac{s}{k}+r)]}, \quad s = 0, \dots, k-1.$$

Observe that

$$e^{-2\pi i(nkz + \frac{n^2}{2}k\tau)} e^{-2\pi i(nk'z + \frac{n^2}{2}k'\tau)} = e^{-2\pi i(n(k+k')z + \frac{n^2}{2}(k+k')\tau)}.$$

Obviously, if $f \in \mathrm{Th}(\{e_\lambda\};\Lambda), g \in \mathrm{Th}(\{e'_\lambda\};\Lambda)$ then $fg \in V(\{e_\lambda e'_\lambda\})$. This implies that the multiplication of functions defines a bilinear map

$$\mathrm{Th}(k;\Lambda_\tau) \times \mathrm{Th}(k';\Lambda_\tau) \to \mathrm{Th}(k+k';\Lambda_\tau).$$

Notice that for $k = 1$ we obtain

$$\Theta_0(z;\tau)_1 = \Theta(z;\tau).$$

Let us modify a little the definition of $\Theta(z;\tau)$ introducing the *theta functions with rational characteristics*

$$\vartheta_{ab}(z;\tau)=\sum_{r\in\mathbb{Z}} e^{\pi i[(a+r)^2\tau+2(z+b)(a+r)]}, \quad a,b\in\mathbb{Q}.$$

In this notation

$$\Theta_s(z;\tau)_k=\vartheta_{\frac{s}{k}0}(kz;k\tau) \tag{3.10}$$

The functions

$$\theta_1(z|\tau)=\vartheta_{\frac12\frac12}(z;\tau)=i\sum_{r\in\frac12+\mathbb{Z}}(-1)^{r-\frac12}v^r q^{\frac{r^2}{2}}, \tag{3.11}$$

$$\theta_2(z|\tau)=\vartheta_{\frac12 0}(z;\tau)=\sum_{r\in\frac12+\mathbb{Z}}v^r q^{\frac{r^2}{2}}, \tag{3.12}$$

$$\theta_3(z|\tau)=\vartheta_{00}(z;\tau)=\sum_{n\in\mathbb{Z}}v^n q^{\frac{n^2}{2}}, \tag{3.13}$$

$$\theta_4(z|\tau)=\vartheta_{0\frac12}(z;\tau)=\sum_{n\in\mathbb{Z}}(-1)^n v^n q^{\frac{n^2}{2}}, \tag{3.14}$$

where $v=e^{2\pi iz}, q=e^{2\pi i\tau}$, are called the *Jacobi theta functions*. It is easy to check the following properties of functions $\vartheta_{ab}(z;\tau)$:

$$\vartheta_{ab}(z;\tau)=e^{2\pi ia(b-b')}\vartheta_{a'b'}(z;\tau) \quad \text{if } a'-a, b'-b\in\mathbb{Z} \tag{3.15}$$

$$\vartheta_{ab}(z+1;\tau)=\sum_{r\in\mathbb{Z}} e^{\pi i[(a+r)^2\tau+2(z+b)(a+r)+2(a+r)]}=e^{2\pi ia}\vartheta_{ab}(z;\tau); \tag{3.16}$$

$$\vartheta_{ab}(z+\tau;\tau)=\sum_{r\in\mathbb{Z}} e^{\pi i[(a+r)^2\tau+2(z+b)(a+r)+2\tau(a+r)]}= \tag{3.17}$$

$$\sum_{r\in\mathbb{Z}} e^{\pi i[(a+r+1)^2\tau-\tau+2(z+b)(a+r+1)-2z-2b]}=e^{-2\pi ib}e^{i\pi(-\tau-2z)}\vartheta_{ab}(z;\tau). \tag{3.18}$$

Also each $\vartheta_{ab}(z;\tau)$ is obtained from $\Theta(z;\tau)$ by translation in the argument z and multiplying by a nowhere vanishing factor.

$$\Theta(z+b+a\tau;\tau)=\sum_{r\in\mathbb{Z}} e^{\pi i[r^2\tau+2(z+b+a\tau)r]}=$$

$$\sum_{r\in\mathbb{Z}} e^{\pi i[(a+r)^2\tau+2(z+b)(r+a)-a^2\tau-2(z+b)a]}=e^{-i\pi(a^2\tau+2(z+b)a)}\vartheta_{ab}(z;\tau).$$

Or, equivalently,

$$\vartheta_{ab}(z;\tau)=e^{i\pi(a^2\tau+2(z+b)a)}\vartheta_{00}(z+b+a\tau;\tau) \tag{3.19}$$

Let us set

$$\mathrm{Th}(k;\Lambda_\tau)_{ab}=\{f\in\mathcal{O}(\mathbb{C}): f(z+m+n\tau)=e^{-2\pi i(-ma+nb)}e^{-2k\pi i(nz+\frac{n^2}{2}\tau)}f(z)\}. \tag{3.20}$$

Its elements are called *theta functions of order k with rational theta characteristics* (a,b). It is easy to see that the multiplication of functions defines a bilinear map

$$\mathrm{Th}(k;\Lambda_\tau)_{ab}\times\mathrm{Th}(k';\Lambda_\tau)_{a'b'}\to\mathrm{Th}(k+k';\Lambda_\tau)_{(a+a')(b+b')}.$$

For any $f\in\mathrm{Th}(k;\Lambda_\tau)$ we have

$$e^{\pi i[a^2\tau+2(z+a)b]}f(z+\frac{b+a\tau}{k})\in\mathrm{Th}(k;\Lambda_\tau)_{ab}.$$

In particular, there is a canonical isomorphism

$$\mathrm{Th}(k;\Lambda_\tau)_{ab}\cong\mathrm{Th}(k;\Lambda_\tau)$$

Also observe that

$$\mathrm{Th}(k;\Lambda_\tau)_{ab}=\mathrm{Th}(k;\Lambda_\tau)_{a'b'}\quad\text{if } a'-a,b'-b\in\mathbb{Z}. \tag{3.21}$$

3.4 Now we are ready to use theta functions to embed $E=\mathbb{C}/\Lambda$ in projective space.

Lemma 3.1. *Let f be a nonzero function from* $\mathrm{Th}(k;\Lambda)$. *Then f has exactly k zeroes in $\mathbb{C}$ modulo Λ counting with multiplicities.*

Proof. We use a well-known formula from the theory of functions in one complex variable: the number of zeroes (counted with multiplicities) of a holomorphic function $f(z)$ on an open subset D of $\mathbb{C}$ inside of a compact set K contained in D together with its oriented boundary Γ is equal to

$$Z=\frac{1}{2\pi}\int_\Gamma d\log f(z)dz.$$

Here we also assume that $f(z)$ has no zeroes on Γ. Let us take for K a small translate $z_0+\Pi$ of the fundamental parallelogram of the lattice Γ such that its boundary Γ does not contain zeroes of $\vartheta_{ab}(z;\tau)$. It is easy to achieve since a holomorphic function has a discrete set of zeroes. Using that

$$f(z+m+n\tau)=e^{-\pi ik(\frac{n^2}{2}\tau+2nz)}f(z),$$

we obtain

$$Z=\frac{1}{2\pi i}\int_\Gamma d\log f(z)=\frac{1}{2\pi i}\int_{z_0}^{z_0+1}d\log f(z)-d\log f((z+\tau;\tau)-$$

$$\frac{1}{2\pi i}\int_{z_0}^{z_0+\tau}d\log f(z)-d\log f(z+1;\tau)=\frac{1}{2\pi i}\int_{z_0}^{z_0+1}d(\pi ik(2z+\tau))=k.$$

Since each zero of $\vartheta_{ab}(z;\tau)$ can be translated to a zero of $\vartheta_{ab}(z;\tau)$ inside K by means of a vector from the lattice, we obtain that the zeroes of $\vartheta_{ab}(z;\tau)$ form k orbits with respect to Λ. This proves the assertion. ∎

Corollary 3.1. *The zeroes of the function $\vartheta_{ab}(z;\tau)$ in $\mathbb{C}$ are the points*

$$z=(a+\frac{1}{2})\tau+(b+\frac{1}{2})+\Lambda.$$

Proof. Using the formula (3.14) it is enough to verify that the function $\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau)$ vanishes at the origin 0. This will follow from the fact that this function is odd. We have

$$\vartheta_{ab}(-z;\tau) = \sum_{r\in\mathbb{Z}} e^{\pi i[(a+r)^2\tau+2(-z+b)(a+r)]} = \sum_{r\in\mathbb{Z}} e^{\pi i[(-a-r)^2\tau+2(z-b)(-a-r)]} = \tag{3.22}$$

$$\sum_{r\in\mathbb{Z}} e^{\pi i[(-a-r)^2\tau+2(z-b)(-a-r)]} = \vartheta_{-a,-b}(z;\tau) \tag{3.23}$$

Taking $(a,b) = (\frac{1}{2},\frac{1}{2})$ and using (3.15) we obtain what we want. □

Corollary 3.2. *The set of zeroes of $\Theta_s(z;\tau)_k$ consists of the points*

$$(\frac{s}{k}+\frac{1}{2})\tau + \frac{1}{2k} + \frac{i}{k} + \Lambda, \quad i = 0,\dots,k-1.$$

Proof. Use (3.9) and the previous lemma. If z is a zero of $\Theta_s(z;\tau)_k$ then kz is the zero of $\vartheta_{\frac{s}{k}0}(z;k\tau)$. Thus

$$kz = (\frac{s}{k}+\frac{1}{2})k\tau + \frac{1}{2} + \mathbb{Z} + \mathbb{Z}k\tau.$$

This gives

$$z = (\frac{s}{k}+\frac{1}{2})\tau + \frac{1}{2k} + \frac{1}{k}\mathbb{Z} + \mathbb{Z}\tau.$$

□

Theorem 3.2. *For each $k \geq 1$ the formula*

$$z \to (\Theta_0(z;\tau)_k,\dots,\Theta_{k-1}(z;\tau)_k)$$

defines a holomorphic map $\phi_k : E_\tau = \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau \to \mathbb{CP}^{k-1}$. If $k \geq 3$, this map is a holomorphic embedding (i.e. injective and the derivative at each point is nonzero).

Proof. First of all the map is well-defined. In fact all theta functions $\Theta_s(z;\tau)_k$ correspond to the same theta factor, hence when we replace z with $z+\lambda, \quad \lambda\in\Lambda$, the right-hand side is multiplied by a non-zero scalar and hence defines the same point in the projective space. Also we see from the previous corollary that the functions $\Theta_s(z;\tau)_k$ do not vanish at the same point, hence not all coordinates of the vector $\phi_k(z)$ are zero. The map is holomorphic since the theta functions are holomorphic functions. Let us show that it is injective when $k \geq 3$. Suppose $\phi_k(z_1) = \phi_k(z_1')$, or $d\phi_k(z_1) = 0$. Using the formulae (3.12) and (3.13), we see that, for any integers m, n,

$$\begin{aligned}\Theta_s(z+\frac{m}{k}+\frac{n\tau}{k};\tau)_k &= \vartheta_{\frac{s}{k}0}(kz+m+n\tau;k\tau) = \\ &e^{\frac{2\pi i m s}{k}} e^{in\pi(\tau+2kz)}\vartheta_{\frac{s}{k}0}(kz;k\tau) = e^{\frac{2\pi i m s}{k}} e^{in\pi(\tau+2kz)}\Theta_s(z;\tau)_k.\end{aligned} \tag{3.24}$$

This shows that $\phi(z_1+\frac{m}{k}+\frac{n\tau}{k}) = \phi(z_1'+\frac{m}{k}+\frac{n\tau}{k})$, or $d\phi_k(z_1) = d\phi_k(z_1+\frac{m}{k}+\frac{n\tau}{k}) = 0$. Note that, if $k\geq 3$ we can always choose m and n such that the four points $z_1, z_1', z_2 = z_1+\frac{m}{k}+\frac{n\tau}{k}, z_2' = z_1'+\frac{m}{k}+\frac{n\tau}{k}$ are distinct. The linear space generated by the functions $\Theta_s(z;\tau)_k$ is of dimension k. So we can find a linear combination f of these functions such that it vanishes at z_1, z_2 and some other $k-3$ points $z_3,\dots,z_{k-1}$ which are distinct modulo Λ. But then f also vanishes at z_1' and z_2', or f has a double zero at z_1 and z_2. Thus we have $k+1$ zeroes of f counting with multiplicities. This contradicts Lemma 3.1 and proves the assertion. □

Remark 3.1. Let us consider the group $\frac{1}{k}\Lambda/\Lambda$. If we consider it as a subgroup of $\mathbb{C}/\Lambda$ we see that

$$\frac{1}{k}\Lambda/\Lambda = \{a \in \mathbb{C}/\Lambda : ka = 0\}$$

is the subgroup ${}_kE$ of k-torsion points on the elliptic curve $E = \mathbb{C}/\Lambda$. The group ${}_kE$ acts by translations on E and on the space of functions V_k generated by $\Theta_s(z;\tau)_k$. In fact, we have

$$\Theta_s(z + \frac{1}{k};\tau)_k = e^{\frac{2\pi i s}{k}}\Theta_s(z;\tau)_k;$$

as we have already noticed in the proof of Theorem 3.2. Also

$$\begin{aligned}\Theta_s(z + \frac{\tau}{k};\tau)_k = \vartheta_{\frac{s}{k}0}(kz+\tau;k\tau) = \sum_{r\in\mathbb{Z}} e^{i\pi(kr+s)^2\frac{\tau}{k}+2(z+\frac{\tau}{k})(kr+s)} = \\ \sum_{r\in\mathbb{Z}} e^{i\pi[(kr+s+1)^2\frac{\tau}{k}+2z(kr+s+1)-2z-\frac{\tau}{k})]} = e^{-\pi i(2z+\frac{\tau}{k})}\Theta_{s+1}(z;\tau)_k,\end{aligned} \tag{3.25}$$

where $\Theta_k(z;\tau)_k = \Theta_0(z;\tau)_k$.

Example 3.2. Let us take $k = 3$ and find the image of the map

$$\phi_3 : E_\tau \to \mathbb{CP}^2.$$

Consider the action of the group $G = \frac{1}{3}\Lambda/\Lambda$ on $\mathbb{CP}^2$ by projective transformations defined on generators by the formula:

$$\begin{aligned}(1/3)\cdot(x_0,x_1,x_2) = (x_0, e^{2\pi i/3}x_1, e^{4\pi i/3}x_2);\\ (\tau/3)\cdot(x_0,x_1,x_2) = (x_1,x_2,x_0).\end{aligned} \tag{3.26}$$

Then it follows from the previous remark that the map ϕ_3 is G-equivariant if we make G act on E by translations. This implies that the image of E_τ must be invariant with respect to the action of G as above. It follows from the remark made after the statement of Theorem 3.1 that for any homogeneous polynomial $F(T_0,T_1,T_2)$ of degree 3 the theta function $F(\Theta_0(z;\tau)_3, \Theta_1(z;\tau)_3, \Theta_2(z;\tau)_3)$ belongs to the space $\mathrm{Th}(9;\Lambda)$ of dimension 9. On the other hand the space of cubic homogeneous polynomials in three variables is of dimension 10. This implies that there exists a cubic polynomial F such that

$$F(\Theta_0(z;\tau)_3, \Theta_1(z;\tau)_3, \Theta_2(z;\tau)_3) \equiv 0,$$

so that the image C of ϕ_3 is contained in the set of zeroes of the homogeneous polynomial $F(x_0,x_1,x_2)$ in $\mathbb{CP}^2$. As we already noticed any compact closed subvariety of $\mathbb{P}^n(\mathbb{C})$ must be the set of zeroes of a system of homogeneous equations. Some elementary algebraic geometry (or better commutative algebra) tells us that C is the set of zeroes of one polynomial. The degree of this polynomial cannot be less than 3. In fact any polynomial of degree 1 defines a a complex manifold isomorphic to $\mathbb{P}^1(\mathbb{C})$ hence homeomorphic to a two-dimensional sphere. But C is homeomorphic to a torus. Similarly a polynomial of degree 2 defining a complex manifold can be reduced by a linear homogeneous transformation to the form $x_0^2 + x_1x_2$. Hence it defines a complex manifold isomorphic to $\mathbb{P}^1(\mathbb{C})$ (use the projection map $(x_0,x_1,x_2) \to (x_0,x_1)$). So we see that C is the set of zeroes of F. The polynomial F must be a common eigenvector for the action of the group $\frac{1}{3}\Lambda/\Lambda \cong (\mathbb{Z}/3)^3$ on the space W of homogeneous cubic polynomials given by the formula (3.26). Also it satisfies the condition that its partial derivatives have no common zeroes. It is easy to see that this is possible only if $F = x_0^3 + x_1^3 + x_2^3 + \gamma x_0 x_1 x_2$ for some scalar γ. This implies that the image of ϕ_3 is a subset of the plane projective curve

$$x_0^3 + x_1^3 + x_2^3 + \gamma x_0 x_1 x_2 = 0. \tag{3.27}$$

Since E_τ is a compact complex manifold of dimension 1, it is easy to see that it must be equal to the whole curve. Also since it is a manifold the partial derivatives of the polynomial in (3.27) do not have a common solutions in $\mathbb{P}^2(\mathbb{C})$ (see Exercise 3.2). This easily implies that

$$\gamma^3 \neq -27.$$

The equation (3.27) is called the *Hesse equation* of an elliptic curve. So we have proved that any elliptic curve is isomorphic to a complex submanifold of the complex projective plane given by the Hesse equation.

Remark 3.2. Consider the affine part of the Hesse cubic where $x_0 \neq 0$. It is isomorphic to the curve C' in $\mathbb{C}^2$ given by the equation

$$1 + x^3 + y^3 + \gamma xy = 0. \tag{3.28}$$

It follows that the functions

$$\Phi_1(z) = \frac{\Theta_1(z;\tau)_3}{\Theta_0(z;\tau)_3}, \quad \Phi_2(z) = \frac{\Theta_2(z;\tau)_3}{\Theta_0(z;\tau)_3}$$

define a surjective holomorphic map $\mathbb{C}^2 \setminus Z \to C'$ whose fibres are equal to the cosets $z + \mathbb{Z} + \tau\mathbb{Z}$. Here Z is the set of zeroes of $\Theta_0(z;\tau)_3$. Observe that the functions $\Phi_1(z)$ and $\Phi_2(z)$ are elliptic functions with respect to Λ, i.e. meromorphic functions with the set of periods Λ. In other words we have succeeded in parametrizing the cubic curve (3.28) by double-periodic functions. For comparison let us consider a homogeneous equation of degree 2. Applying a homogeneous linear transformation we can reduce it to the form $x_0^2 - x_1^2 + x_3^2 = 0$ (if it defines a complex submanifold). Dehomogenizing, we get the equation of a (complex) circle

$$S : x^2 + y^2 = 1.$$

In this case its parametrization $\mathbb{C} \to S$ is defined by one-periodic holomorphic functions $\cos 2\pi z, \sin 2\pi z$. Its fibres are cosets $z + \mathbb{Z}$. One of the best achievements of mathematics of the last century is the Uniformization Theorem of Klein-Poincare which says that any equation $f(x,y) = 0$ defining a Riemann surface in $\mathbb{C}^2$ admits a parametrization by automorphic functions. Its group of periods is not commutative in general.

Exercises

3.1 Using Exercise 2.12 show that the equation $x^3 + y^3 + z^3 + \lambda xyz = 0$ defines a complex manifold of dimension 1 in $\mathbb{P}^2(\mathbb{C})$ if and only if $\lambda^3 + 27 \neq 0$.

3.2 Show that the image of a 3-torsion point of $\mathbb{C}/\Lambda$ under the map ϕ_3 is an inflection point of the Hesse cubic (a unique point at which some line intersects the curve with multiplicity 3). Find the projective coordinates of these points.

3.3 Show that for general value of the parameter γ the group of projective automorphisms of the Hesse cubic is of order 18. Show that it is generated by translations $z+a, a \in \frac{1}{3}\Lambda/\Lambda$ and the inversion automorphism $z \to -z$ of the corresponding complex torus $\mathbb{C}/\Lambda$. Find the corresponding projective automorphisms of the Hesse cubic.

3.4 Show that the image of 2-torsion points on the Hesse cubic are the four points $(0,1,-1), (1,a,a)$, where a is a root of the cubic equation $2t^3 + \lambda t^2 + 1 = 0$.

3.5 Find the values of the parameter γ in the Hesse equation corresponding to the harmonic and anharmonic elliptic curve.

3.6 Show that the parameter λ in the Hesse equation (3.27) is equal to the following function in τ:

$$\lambda = -\frac{\vartheta(0;3\tau)^3 + q^{1/2}\vartheta(t;3\tau)^3 + q^2\vartheta(2\tau;3\tau)}{q^{5/2}\vartheta(0;3\tau)\vartheta(\tau;3\tau)\vartheta(2\tau;3\tau)}.$$

3.7 Analyze the proof of Theorem 3.2 in the case $k = 2$. Show that ϕ_2 defines a holomorphic map $E_\tau \to \mathbb{P}^1(\mathbb{C})$ such that for all points $x \in \mathbb{P}^1(\mathbb{C})$ except four, the pre-image consists of 2 points and over the four points the pre-image consists of one point.

3.8 Show that the map $\mathbb{C} \to \mathbb{P}^4(\mathbb{C})$ given by the formulas

$$z \to (\vartheta_{00}(z), \vartheta_{\frac{1}{2}0}(z), \vartheta_{0\frac{1}{2}}(z), \vartheta_{\frac{1}{2}\frac{1}{2}}(z))$$

defines an isomorphism from $\mathbb{C}/2\Lambda \cong \mathbb{C}/\Lambda$ onto a complex submanifold of $\mathbb{P}^4(\mathbb{C})$ given by two homogeneous polynomials of degree 2.

3.9 Let X be a complex manifold of dimension 1 in $\mathbb{P}^4(\mathbb{C})$ defined by two homogeneous equations of degree 2.

(i) Show that, after linear homogeneous change of variables X can be defined by the equations $z_0^2 + az_1^2 - z_2^2 = 0, z_0^2 + bz_1^2 - z_3^2 = 0$ for some nonzero $a, b \in \mathbb{C}$.

(ii) Show that each X as above is isomorphic to an elliptic curve.

(iii) Find the values of (a,b) in (i) such that the corresponding elliptic curve is harmonic (resp. anharmonic).

3.10 Show that each $\vartheta_{ab}(z;\tau)$ considered as a function of two variables z, τ satisfies the differential equation (the *Heat equation*):

$$\frac{\partial^2 f(z,\tau)}{\partial z^2} - 4\pi i \frac{\partial f(z,\tau)}{\partial \tau} = 0.$$

3.11 Check the following equalities:

$$\vartheta_{00}(0;\tau) = \vartheta_{0\frac{1}{2}}(\frac{1}{2};\tau) = -e^{\pi i\tau/4}\vartheta_{\frac{1}{2}\frac{1}{2}}(\frac{\tau+1}{2};\tau) = e^{\pi i\tau/4}\vartheta_{\frac{1}{2}0}(\frac{\tau}{2};\tau);$$
$$\vartheta_{0\frac{1}{2}}(0;\tau) = \vartheta_{00}(\frac{1}{2};\tau) = ie^{\pi i\tau/4}\vartheta_{\frac{1}{2}0}(\frac{\tau+1}{2};\tau) = ie^{\pi i\tau/4}\vartheta_{\frac{1}{2}\frac{1}{2}}(\frac{\tau}{2};\tau);$$
$$\vartheta_{\frac{1}{2}0}(0;\tau) = -\vartheta_{\frac{1}{2}\frac{1}{2}}(\frac{1}{2};\tau) = e^{\pi i\tau/4}\vartheta_{0\frac{1}{2}}(\frac{\tau+1}{2};\tau) = e^{\pi i\tau/4}\vartheta_{00}(\frac{\tau}{2};\tau).$$

3.12 Prove that, for any $\omega \in \mathbb{C}$,the product $\vartheta_{ab}(z+w;\tau)\vartheta_{a'b'}(z-w;\tau)$ is a theta function of order 2 with theta characteristic $(a+a', b+b')$. Deduce from this the *addition formulae*:

$$\vartheta_{0\frac{1}{2}}(0)^2\vartheta_{0\frac{1}{2}}(z+w)\vartheta_{0\frac{1}{2}}(z-w) = \vartheta_{0\frac{1}{2}}(z)^2\vartheta_{0\frac{1}{2}}(w)^2 - \vartheta_{\frac{1}{2}\frac{1}{2}}(z)^2\vartheta_{\frac{1}{2}\frac{1}{2}}(w)^2,$$
$$\vartheta_{\frac{1}{2}0}(0)^2\vartheta_{\frac{1}{2}0}(z+w)\vartheta_{\frac{1}{2}0}(z-w) = \vartheta_{\frac{1}{2}0}(z)^2\vartheta_{\frac{1}{2}0}(w)^2 - \vartheta_{\frac{1}{2}\frac{1}{2}}(z)^2\vartheta_{\frac{1}{2}\frac{1}{2}}(w)^2,$$
$$\vartheta_{0\frac{1}{2}}(0)^2\vartheta_{\frac{1}{2}\frac{1}{2}}(z+w)\vartheta_{\frac{1}{2}\frac{1}{2}}(z-w) = \vartheta_{\frac{1}{2}\frac{1}{2}}(z)^2\vartheta_{0\frac{1}{2}}(w)^2 - \vartheta_{0\frac{1}{2}}(z)^2\vartheta_{\frac{1}{2}\frac{1}{2}}(w)^2.$$

Lecture 4

Theta Constants

4.1 In this lecture we shall study the functions of τ equal to $\vartheta(0,\tau)$ where $\vartheta(z,\tau)$ is a theta function. To show that they are worth of studying we shall start with the Riemann theta function $\Theta(z;\tau)$. We have

$$\Theta(0,\tau) = \sum_{r\in\mathbb{Z}} e^{\pi i r^2\tau} = \sum_{r\in\mathbb{Z}} q^{r^2}, \quad q = e^{i\pi\tau}. \tag{4.1}$$

We have

$$\Theta(0,\tau)^k = \sum_{r_1\in\mathbb{Z}}\cdots\sum_{r_k\in\mathbb{Z}} q^{r_1^2+\ldots+r_k^2} = \sum_{n=0}^{\infty} c_k(n)q^n,$$

where

$$c_k(n) = \#\{(r_1,\ldots,r_k)\in\mathbb{Z}^k : n = r_1^2+\ldots+r_k^2\}.$$

So $\Theta(0,\tau)^k$ is the generating function for counting the number of representations of an integer as a sum of k squares. For example $c_3(6) = 24$ since all representations of 6 as a sum of 3 squares are obtained from $6 = 2^2+1+1$ by changing the order and signs.

Let us show that $\vartheta(\tau) = \Theta(0,\tau)^k$ satisfies the following functional equation:

$$\vartheta(-1/\tau) = (-i\tau)^{k/2}\vartheta(\tau), \quad \vartheta(\tau+2) = \vartheta(\tau). \tag{4.2}$$

Here in the first equation we take the branch of the square root which is positive on the purely imaginary ray $i\mathbb{R}_{>0}$. The second equation follows immediately from the Fourier expansion. To prove the first one we use the Poisson formula in the theory of Fourier transforms. Recall that for any rapidly decreasing at infinity smooth function f on $\mathbb{R}^n$ one defines its Fourier transform $\hat{f}$ by the formula:

$$\hat{f}(\mathbf{x}) = \int_{\mathbb{R}^n} e^{2\pi i\mathbf{x}\cdot\mathbf{t}} f(\mathbf{t})d\mathbf{t}.$$

Let Λ be a lattice in $\mathbb{R}^n$ and A be the volume of its fundamental parallelopiped. Let $\Lambda' = \{\mathbf{x}\in\mathbb{R}^n : \mathbf{x}\cdot\mathbf{v}\in\mathbb{Z}, \forall\mathbf{v}\in\Lambda\}$. Then the Poisson formula says that

$$\sum_{\mathbf{x}\in\Lambda} f(\mathbf{x}) = A^{-1}\sum_{\mathbf{y}\in\Lambda'} \hat{f}(y). \tag{4.3}$$

We apply this formula to our case. Take $n = 1$ and $\Lambda = \mathbb{Z}$ and $f(x) = e^{-\pi x^2 y}$ considered as a function of $x \in \mathbb{R}$. Then the left-hand side of (4.3) is equal to $\Theta(0, iy)$. Now the Fourier transform of $f(x)$ is easy to compute. We have

$$\hat{f}(x) = \int_{-\infty}^{\infty} e^{2\pi ixt} e^{-\pi t^2 y} dt = \int_{-\infty}^{\infty} e^{-\pi y(t-\frac{x}{y})^2} e^{\pi x^2/y} dt =$$

$$e^{\pi x^2/y}\int_{-\infty}^{\infty} e^{-\pi y t^2} dt = e^{\pi x^2/y}\sqrt{y} = f(-1/y)/\sqrt{y}.$$

This verifies (4.2) when we restrict τ to the imaginary axis $\tau = iy$. Since the set of zeroes of a holomorphic function is discrete this suffices.

Note that if $k = 8n$, (4.2) gives

$$\vartheta(\frac{-1}{\tau}) = \tau^{k/2}\vartheta. \tag{4.4}$$

We shall interpet this later by saying that $\Theta(0;\tau)^k$ is a modular form of weight $k/2$ with respect to the principal congruence subgroup $\Gamma(2)$.

To give you an idea why the functional equation of type (4.2) is useful, let me give one numerical application. Take $\tau = ix$ purely imaginary with $x > 0$. Then (4.2) gives

$$\sum_{r\in\mathbb{Z}} e^{-\pi x r^2} = \frac{1}{\sqrt{x}}\sum_{r\in\mathbb{Z}} e^{-\pi r^2/x} = \frac{1}{\sqrt{x}}(1 + 2\sum_{r=1}^{\infty} e^{-\pi r^2/x})$$

Suppose we want to compute the value of the left-hand side at small x. For $x = .001$ we need fifty terms to reach the accuracy of order 10^{-10}. But now, if we use the right-hand side we have

$$\sum_{r\in\mathbb{Z}} e^{-\pi .001 r^2} = 10(1 + 2e^{-100\pi} + \dots).$$

Since $e^{-100\pi} \sim 10^{-434}$ we need only two terms to reach the accuracy of order 10^{-400}.

4.2 We know that the zeroes z of $\Theta(z,\tau) = \vartheta_{00}(z;\tau)$ satisfy

$$2z = (1 + 2m)\tau + (1 + 2n).$$

Then

$$e^{\pm 2\pi iz} = -e^{\pi i\tau(2m-1)},$$

where we consider only positive m. Let $q = e^{2\pi i\tau}$ be as before, and consider the infinite product

$$P(z;q) = \prod_{m=1}^{\infty}(1 + q^{\frac{2m-1}{2}} e^{2\pi iz})(1 + q^{\frac{2m-1}{2}} e^{-2\pi iz}). \tag{4.5}$$

Recall that an infinite product $\prod_{n=1}^{\infty} f_n$ of holomorphic functions on an open subset U of $\mathbb{C}$ represents a holomorphic function equal to $\lim_{N\to\infty}\prod_{n=1}^{N} f_n$ if for any compact subset K of U the series $\sum_{n=1}^{\infty}(1-f_n)$ is uniformly convergent.

Since $|q|<1$, the infinite series

$$\sum_{m=1}^{\infty} q^{\frac{2m-1}{2}}(e^{2\pi iz}+e^{-2\pi iz})$$

is absolutely convergent for any z and the infinite series (4.5) is a holomorphic function on $\mathbb{C}$. Its zeroes are the same as the zeroes of $\Theta(z,\tau)$. This implies that

$$\Theta(z,\tau)=\vartheta_{00}(z;\tau)=Q(q)\prod_{m=1}^{\infty}(1+q^{\frac{2m-1}{2}}e^{2\pi iz})(1+q^{\frac{2m-1}{2}}e^{-2\pi iz})$$

for some function $Q(q)$. Using formula (3.14) from Lecture 3, we obtain

$$\vartheta_{0\frac{1}{2}}(z;\tau)=Q\prod_{m=1}^{\infty}(1-q^{\frac{2m-1}{2}}e^{2\pi iz})(1-q^{\frac{2m-1}{2}}e^{-2\pi iz}); \tag{4.6}$$

$$\vartheta_{\frac{1}{2}0}(z;\tau)=Qq^{\frac{1}{8}}(e^{\pi iz}+e^{-\pi iz})\prod_{m=1}^{\infty}(1+q^{m}e^{2\pi iz})(1+q^{m}e^{-2\pi iz}); \tag{4.7}$$

$$\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau)=iQq^{\frac{1}{8}}(e^{\pi iz}-e^{-\pi iz})\prod_{m=1}^{\infty}(1-q^{m}e^{2\pi iz})(1-q^{m}e^{-2\pi iz}). \tag{4.8}$$

Plugging in $z=0$ we get

$$\begin{aligned}\vartheta_{00}(0;\tau)&=Q\prod_{m=1}^{\infty}(1+q^{\frac{2m-1}{2}})^2;\\ \vartheta_{0\frac{1}{2}}(0;\tau)&=Q\prod_{m=1}^{\infty}(1-q^{\frac{2m-1}{2}})^2;\\ \vartheta_{\frac{1}{2}0}(0;\tau)&=2Qq^{\frac{1}{8}}\prod_{m=1}^{\infty}(1+q^{m})^2;\\ \vartheta_{\frac{1}{2}\frac{1}{2}}(0;\tau)&=0.\end{aligned} \tag{4.9}$$

Differentiating $\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau)$ in z, we find

$$\vartheta_{\frac{1}{2}\frac{1}{2}}(0;\tau)'=-2\pi Qq^{\frac{1}{8}}\prod_{m=1}^{\infty}(1-q^{m})^2. \tag{4.10}$$

To compute the factor Q we use the following:

Theorem 4.1. *(C. Jacobi).*

$$\vartheta'_{\frac{1}{2}\frac{1}{2}}=-\pi\vartheta_{00}\vartheta_{\frac{1}{2}0}\vartheta_{0\frac{1}{2}}.$$

Here, following the classic notation, we set

$$\vartheta_{ab}(0;\tau)=\vartheta_{ab},$$

$$\frac{d\vartheta_{ab}(z;\tau)}{dz}(0) = \vartheta'_{ab}.$$

Also notice that when $(a,b) = (\epsilon/2, \eta/2)$ where $\epsilon, \eta = 0, 1$ the classic notation is really

$$\vartheta_{\frac{\epsilon}{2}\frac{\eta}{2}}(z;\tau) = \vartheta_{\epsilon\eta}(z;\tau).$$

However we keep our old notation.

Proof. Consider the space $\mathrm{Th}(2;\Lambda)_{ab}$ with $a, b = \epsilon/2, \epsilon = 0, 1$. Its dimension is 2. If $(a,b) = (1/2, 0)$, the functions $\vartheta_{\frac{1}{2}0}(z;\tau)\vartheta_{00}(z;\tau)$ and $\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau)\vartheta_{0\frac{1}{2}}(z;\tau)$ belong to this space. It follows from (3.12) and (3.7) that

$$\vartheta_{\frac{1}{2}0}(z;\tau), \vartheta_{00}(z;\tau), \vartheta_{0\frac{1}{2}}(z;\tau) \quad \text{are even functions in } z,$$

$$\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau) \quad \text{is an odd function in } z.$$

Thus $\vartheta_{\frac{1}{2}0}(z;\tau)\vartheta_{00}(z;\tau)$ is even and $\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau)\vartheta_{0\frac{1}{2}}(z;\tau)$ is odd. Now consider the function

$$F(z) = \vartheta_{ab}(z;\tau)\vartheta_{a'b'}(z;\tau)' - \vartheta_{ab}(z;\tau)'\vartheta_{a'b'}(z;\tau).$$

Observe that $F(z) = \vartheta_{ab}(z;\tau)^2(\vartheta_{a'b'}(z;\tau)/\vartheta_{ab}(z;\tau))'$. The function $\frac{\vartheta_{a'b'}(z;\tau)}{\vartheta_{ab}(z;\tau)}$ is almost periodic with respect to Λ, that is

$$\frac{\vartheta_{a'b'}(z+m+n\tau;\tau)}{\vartheta_{ab}(z+m+n\tau;\tau)} = e^{2\pi i[m(a'-a)-n(b'-b)]}\frac{\vartheta_{a'b'}(z;\tau)}{\vartheta_{ab}(z;\tau)}.$$

This implies that $F(z) \in \mathrm{Th}(2;\Lambda)_{2a+a'-a,2b+b'-b} = \mathrm{Th}(2;\Lambda)_{a+a',b+b'}$. In particular,

$$\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau)'\vartheta_{0\frac{1}{2}}(z;\tau) - \vartheta_{0\frac{1}{2}}(z;\tau)'\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau) \in \mathrm{Th}(2;\Lambda)_{\frac{1}{2}0}.$$

Since this function is even (the derivative of an odd function is even, and the derivative of an even function is odd) we must have

$$\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau)'\vartheta_{0\frac{1}{2}}(z;\tau) - \vartheta_{0\frac{1}{2}}(z;\tau)'\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau) = c\vartheta_{\frac{1}{2}0}(z;\tau)\vartheta_{00}(z;\tau), \tag{4.11}$$

for some constant c. Since $\vartheta_{\frac{1}{2}\frac{1}{2}}(0;\tau) = 0$, we get

$$c = \frac{\vartheta'_{\frac{1}{2}\frac{1}{2}}\vartheta_{0\frac{1}{2}}}{\vartheta_{\frac{1}{2}0}\vartheta_{00}}.$$

Differentiating (4.11) twice in z and plugging in $z = 0$, we obtain

$$\vartheta'''_{\frac{1}{2}\frac{1}{2}}\vartheta_{0\frac{1}{2}} - \vartheta''_{0\frac{1}{2}}\vartheta'_{\frac{1}{2}\frac{1}{2}} = \vartheta'_{\frac{1}{2}\frac{1}{2}}\vartheta_{0\frac{1}{2}}\vartheta_{\frac{1}{2}0}\vartheta_{00}(\vartheta''_{\frac{1}{2}0}\vartheta_{00} + \vartheta_{\frac{1}{2}0}\vartheta''_{00}).$$

This gives

$$\frac{\vartheta'''_{\frac{1}{2}\frac{1}{2}}}{\vartheta'_{\frac{1}{2}\frac{1}{2}}} = \frac{\vartheta''_{0\frac{1}{2}}}{\vartheta_{0\frac{1}{2}}} + \frac{\vartheta''_{\frac{1}{2}0}}{\vartheta_{\frac{1}{2}0}} + \frac{\vartheta''_{00}}{\vartheta_{00}}.$$

Now we use the Heat equation

$$\frac{\partial^2\vartheta_{ab}(z;\tau)(z,\tau)}{\partial z^2} - 4\pi i\frac{\partial\vartheta_{ab}(z;\tau)(z,\tau)}{\partial\tau} = 0 \tag{4.12}$$

(see Exericse 3.10). This allows us to rewrite the previous equality in terms of derivatives in τ. We get

$$\frac{d\log\vartheta'_{\frac{1}{2}\frac{1}{2}}}{d\tau} = \frac{d\log\vartheta_{0\frac{1}{2}}\vartheta_{\frac{1}{2}0}\vartheta_{00}}{d\tau}.$$

Integrating, we get

$$\vartheta'_{\frac{1}{2}\frac{1}{2}} = \alpha\vartheta_{0\frac{1}{2}}\vartheta_{\frac{1}{2}0}\vartheta_{00},$$

for some constant α. To compute α we use (4.14) when $q = 0$ (i.e. taking Im τ go to infinity). This gives $\alpha = -\pi$. The theorem is proven. $\square$

4.3 Now we are in business. Multiplying the equalities in (4.9) and comparing it with the equality (4.10), we obtain using the Jacobi theorem

$$-2\pi Qq^{\frac{1}{8}}\prod_{m=1}^{\infty}(1-q^m)^2 = \vartheta'_{\frac{1}{2}\frac{1}{2}} = -\pi\vartheta_{00}\vartheta_{0\frac{1}{2}}\vartheta_{\frac{1}{2}0} =$$

$$-2\pi Q^3q^{\frac{1}{8}}\prod_{m=1}^{\infty}(1-q^{m-\frac{1}{2}})^2\prod_{m=1}^{\infty}(1+q^{m-\frac{1}{2}})^2\prod_{m=1}^{\infty}(1+q^m)^2.$$

This gives

$$Q = \prod_{m=1}^{\infty}\frac{1-q^m}{(1+q^m)(1+q^{m-\frac{1}{2}})(1-q^{m+\frac{1}{2}})}.$$

Here again we fix the sign in front of Q by looking at the value of both sides at $q = 0$. Replaing q with t^2 and using the obvious equalities

$$\prod_{m=1}^{\infty}(1+t^{2m})(1+t^{2m-1}) = \prod_{m=1}^{\infty}(1+t^m);$$

$$\prod_{m=1}^{\infty}(1-t^{2m}) = \prod_{m=1}^{\infty}(1-t^m)\prod_{m=1}^{\infty}(1+t^{2m-1})(1+t^{2m}),$$

we finally obtain

$$Q = \prod_{m=1}^{\infty}(1-t^{2m}) = \prod_{m=1}^{\infty}(1-q^m). \tag{4.13}$$

Now substituting Q in (4.9) we get

$$\vartheta'_{\frac{1}{2}\frac{1}{2}} = -2\pi q^{1/8}\prod_{m=1}^{\infty}(1-q^m)^3 \tag{4.14}$$

Here comes our first encounter with one of the most notorious functions in mathematics:

Definition. The *Dedekind η-function* is the holomorphic function on the upper-half plane defined by

$$\eta(\eta) = q^{\frac{1}{24}} \prod_{m=1}^{\infty} (1 - q^m), \quad q = e^{2\pi i\tau}. \tag{4.15}$$

Thus $Q = q^{-1/12}\eta(\tau)$ and we can rewrite (4.5) in the form

$$\begin{aligned} \vartheta_{00} &= \eta(\tau)\mathfrak{f}(\tau)^2, \\ \vartheta_{0\frac{1}{2}} &= \eta(\tau)\mathfrak{f}_1(\tau)^2 \\ \vartheta_{\frac{1}{2}0} &= \eta(\tau)\mathfrak{f}_2(\tau)^2 \\ \vartheta'_{\frac{1}{2}\frac{1}{2}} &= -2\pi\eta(\tau)^3, \end{aligned} \tag{4.16}$$

where

$$\mathfrak{f}(\tau) = q^{-1/48} \prod_{m=1}^{\infty} (1 + q^{\frac{2m-1}{2}}); \tag{4.17}$$

$$\mathfrak{f}_1(\tau) = q^{-1/48} \prod_{m=1}^{\infty} (1 - q^{\frac{2m-1}{2}}); \tag{4.18}$$

$$\mathfrak{f}_2(\tau) = \sqrt{2}q^{1/24} \prod_{m=1}^{\infty} (1 + q^m). \tag{4.19}$$

They are called the *Weber functions.*

4.4 Let us give some applications.

We have

$$\vartheta_{00}(z;\tau) = \sum_{r\in\mathbb{Z}} e^{\pi(2rz + ir^2\tau)} = \sum_{r\in\mathbb{Z}} q^{\frac{r^2}{2}} v^r,$$

where $q = e^{2\pi i\tau}, \quad v = e^{2\pi iz}$. It follows from (4.4) and (4.9) that

$$\vartheta_{00}(z;\tau) = \prod_{m=1}^{\infty} (1 - q^m)(1 + q^{\frac{2m-1}{2}} v)(1 + q^{\frac{2m-1}{2}} v^{-1}).$$

Comparing the two expressions we get the identity

$$\sum_{r\in\mathbb{Z}} q^{\frac{r^2}{2}} v^r = \prod_{m=1}^{\infty} (1 - q^m)(1 + q^{\frac{2m+1}{2}} v)(1 + q^{\frac{2m+1}{2}} v^{-1}). \tag{4.20}$$

Here are some special cases corresponding to $v = 1$ and $v = -1$:

$$\sum_{r\in\mathbb{Z}} q^{\frac{r^2}{2}} = \prod_{m=1}^{\infty} (1 - q^m)(1 + q^{\frac{2m+1}{2}})^2, \tag{4.21}$$

$$\sum_{r\in\mathbb{Z}} (-1)^r q^{\frac{r^2}{2}} = \prod_{m=1}^{\infty} (1 - q^m)(1 - q^{\frac{2m-1}{2}})^2. \tag{4.22}$$

To get more of this beautiful stuff, let us consider the function $\vartheta_{\frac{1}{6}\frac{1}{2}}(0,3\tau)$. By (3.14), we have

$$\vartheta_{\frac{1}{6}\frac{1}{2}}(0,3\tau) = e^{\pi i/6}e^{\pi i\tau/12}\vartheta(\frac{1}{2}+\frac{\tau}{2};3\tau)_{00} =$$

$$e^{\pi i/6}e^{\pi i\tau/12}\prod_{m=1}^{\infty}((1-e^{6\pi i m\tau})\prod_{m=1}^{\infty}(1-e^{\pi i(6m+4)\tau})(1-e^{\pi i(6m+2)\tau}) =$$

$$e^{\pi i/6}e^{\pi i\tau/12}\prod_{m=1}^{\infty}(1-q^m).$$

On the other hand, we have

$$\vartheta_{\frac{1}{6}\frac{1}{2}}(0,3\tau) = \sum_{m\in\mathbb{Z}} e^{i\pi[(m+\frac{1}{6})^2 3\tau+2(m+\frac{1}{6})\frac{1}{2}]} =$$

$$e^{\pi i/6}e^{\pi i\tau/12}\sum_{m=0}^{\infty}(-1)^m e^{\pi(3m^2+m)\tau} = e^{\pi i/6}e^{\pi i\tau/12}\sum_{m\in\mathbb{Z}}(-1)^m q^{m(3m+1)/2}.$$

This gives the *Euler identity*

$$\sum_{r\in\mathbb{Z}}(-1)^r q^{r(3r+1)/2} = \prod_{m=1}^{\infty}(1-q^m). \tag{4.23}$$

In particular, we get the following Fourier expansion for the Dedekind's function $\eta(\tau)$:

$$\eta(\tau) = q^{\frac{1}{24}}\sum_{r\in\mathbb{Z}}(-1)^r q^{r(3r+1)/2}.$$

The positive integers of the form $n+(k-2)\frac{n(n-1)}{2}, n = 1,2,\ldots$ are called *k-gonal numbers.* The number of beads arranged in the form of a regular k-polygon is expressed by k-gonal numbers. In the Euler identity we are dealing with pentagonal numbers. They correspond to the powers of q when r is negative.

The Euler identity (4.23) is one of the series of *MacDonald's identities* associated to a simple Lie algebra:

$$\sum_{r\in\mathbb{Z}} a_{r,k}q^r = \prod_{m=0}^{\infty}(1-q^m)^k.$$

The Euler identity is the special case corresponding to the algebra $\mathfrak{sl}(2)$.

Exercises

4.1 Let $p(n)$ denote the number of partitions of a positive integer n as a sum of positive integers. Using the Euler identity prove that

$$p(n)-p(n-1)-p(n-2)+p(n-5)+\ldots+(-1)^k p(n-\frac{1}{2}k(3k-1))+$$
$$(-1)^k p(n-\frac{1}{2}k(3k+1))+\ldots = 0.$$

Using this identity compute the values of $p(n)$ for $n \leq 20$.

4.2 Prove the *Gauss identity*:

$$2\prod_{n=0}^{\infty}(1-x^{2n+2})\Big(\prod_{n=0}^{\infty}(1-x^{2n+1})\Big)^{-1} = \sum_{r=0}^{\infty} x^{r(r+1)/2}.$$

4.3 Prove the *Jacobi identity*:

$$\prod_{n=1}^{\infty}(1-x^n)^3 = \sum_{r=0}^{\infty}(-1)^r(2r+1)x^{r(r+1)/2}.$$

4.4 Using (4.2) prove the following identity about *Gaussian sums*:

$$\frac{1}{\sqrt{q}}\sum_{r=0}^{q-1} e^{-\pi r^2 p/q} = \frac{1}{\sqrt{p}}\sum_{r=0}^{p-1} e^{-\pi r^2 q/p}.$$

Here p, q are two coprime natural numbers.[Hint: Consider the assymptotic of the function $f(x) = \Theta(0; ix + \frac{p}{q})$ when x goes to zero.]

4.5 Prove the *Jacobi triple product identity*:

$$\prod_{n=1}^{\infty}(1-q^n)(1+q^{n-\frac{1}{2}}t)(1+q^{n-\frac{1}{2}}t^{-1}) = \sum_{r\in\mathbb{Z}} q^{\frac{r^2}{2}}t^n.$$

4.6 Prove a *doubling identity* for theta constants:

$$\vartheta_{0\frac{1}{2}}(2\tau)^2 = \vartheta_{00}(\tau)\vartheta_{0\frac{1}{2}}(\tau).$$

(see other doubling identities in Exercise 10.10).

4.7 Prove the following formulas expressing the Weber functions in terms of the η-function:

$$\mathfrak{f}(\tau) = e^{-2\pi i/48}\eta(\frac{\tau+1}{2})\eta(\tau), \quad \mathfrak{f}_1(\tau) = \eta(\frac{\tau}{2})\eta(\tau), \quad \mathfrak{f}_2(\tau) = \sqrt{2}\eta(2\tau)\eta(\tau).$$

4.8 Prove the following identities connecting the Weber functions:

$$\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \sqrt{2}.$$

Lecture 5

Transformations of Theta Functions

5.1 Let us see now that the theta constants ϑ_{ab} and their derivatives ϑ'_{ab} satisfy the functional equation similar to (4.2). This will imply that certain powers of theta constants are modular forms. For brevity we denote the lattice $\mathbb{Z}+\tau\mathbb{Z}$ by Λ_τ.

Theorem 5.1. *Let $\vartheta(z;\tau)\in \mathrm{Th}(k;\Lambda_\tau)_{ab}$ and $M=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in \mathrm{SL}(2,\mathbb{Z})$. Then*

$$e^{-i\pi(\frac{k\gamma z^2}{\gamma\tau+\delta})}\vartheta(\frac{z}{\gamma\tau+\delta};\frac{\alpha\tau+\beta}{\gamma\tau+\delta})\in \mathrm{Th}(k;\Lambda_\tau)_{a'b'},$$

where

$$(a',b')=(\alpha a+\gamma b-\frac{k\gamma\alpha}{2},\beta a+\delta b+\frac{k\beta\delta}{2}).$$

Proof. First observe that for any $f(z)\in \mathrm{Th}(\{e_\lambda\};\Lambda)$ and $t\in\mathbb{C}^*$,

$$\phi(z)=f(\frac{z}{t})\in \mathrm{Th}(\{e'_{\lambda'}\};t\Lambda),$$

where

$$e'_{\lambda'}(z)=e_{\frac{\lambda'}{t}}(\frac{z}{t}).$$

In fact, for any $\lambda'=t\lambda\in t\Lambda$,

$$\phi(z+t\lambda')=f(\frac{z+t\lambda}{t})=f(\frac{z}{t}+\lambda)=e_\lambda(\frac{z}{t})f(\frac{z}{t})=e_{\frac{\lambda'}{t}}(\frac{z}{t})\phi(z).$$

We have

$$\mathrm{Th}(k;\Lambda_\tau)_{ab}=\mathrm{Th}(\{e_\lambda\};\mathbb{Z}+\tau\mathbb{Z}),$$

where

$$e_{m+n\tau}(z)=e^{2\pi i(ma-nb)}e^{-\pi ik(2nz+n^2\tau)}. \tag{5.1}$$

For any $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ we have

$$(\gamma\tau+\delta)\mathbb{Z} + (\alpha\tau+\beta)\mathbb{Z} = \mathbb{Z} + \tau\mathbb{Z}.$$

Thus for any $\vartheta \in \mathrm{Th}(k;\Lambda_\tau)_{ab}$, we have

$$\vartheta(z(\gamma\tau+\delta)) \in \mathrm{Th}(e'_{\lambda'};\mathbb{Z}+\tau'\mathbb{Z}),$$

where

$$\tau' = \frac{\alpha\tau+\beta}{\gamma\tau+\delta},$$

$$e'_{m+n\tau'}(z) = e_{(m+n\tau')(\gamma\tau+\delta)}(z(\gamma\tau+\delta)).$$

We have, using (5.1),

$$e'_1(z) = e_{\gamma\tau+\delta}(z(\gamma\tau+\delta)) = e^{2\pi i(a\delta-b\gamma)}e^{-\pi ik(2\gamma z(\gamma\tau+\delta)+\gamma^2\tau)} =$$

$$e^{-\pi ik\gamma((\gamma\tau+\delta)(z+1)^2-(\gamma\tau+\delta)z^2)}e^{\pi ik\gamma\delta}e^{2\pi i(a\delta-b\gamma)}.$$

This shows that

$$e^{\pi ik\gamma(\gamma\tau+\delta)z^2}\mathrm{Th}(\{e'_{\lambda'}(z)\};\mathbb{Z}+\tau'\mathbb{Z}) = \mathrm{Th}(\{e''_{\lambda'}(z)\};\mathbb{Z}+\tau'\mathbb{Z}),$$

where

$$e''_1(z) = e^{\pi i[k\gamma\delta+2(a\delta-b\gamma)]}. \tag{5.2}$$

Now comes a miracle! Let us compute $e''_{\tau'}(z)$. We have

$$e''_{\tau'}(z) = e^{\pi ik\gamma(\gamma\tau+\delta)((z+\tau')^2-z^2)}e_{\tau'(\gamma\tau+\delta)}(z(\gamma\tau+\delta)) =$$

$$e^{\pi ik\gamma(\gamma\tau+\delta)(2z\tau'+\tau'^2)}e_{\beta+\alpha\tau}(z(\gamma\tau+\delta)) = \tag{5.3}$$

$$e^{\pi ik[\gamma(\gamma\tau+\delta)(2z\tau'+\tau'^2)-(2\alpha z(\gamma\tau+\delta)+\alpha^2\tau)}e^{2\pi i(-b\alpha+\beta a)]} = e^{i\pi ikG}e^{2\pi i(-b\alpha+\beta a)},$$

where

$$G = \gamma(\gamma\tau+\delta)(2z\tau'+\tau'^2) - 2\alpha z(\gamma\tau+\delta) - \alpha^2\tau =$$

$$\gamma(\gamma\tau+\delta)(2z(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) + (\frac{\alpha\tau+\beta}{\gamma\tau+\delta})^2) - 2\alpha z(\gamma\tau+\delta) - \alpha^2\tau =$$

$$2z\gamma(\alpha\tau+\beta) + \frac{\gamma(\alpha\tau+\beta)^2}{\gamma\tau+\delta} - 2\alpha z(\gamma\tau+\delta) - \alpha^2\tau =$$

$$-2z + \frac{\gamma(\alpha\tau+\beta)^2 - \alpha^2\tau(\gamma\tau+\delta)}{\gamma\tau+\delta}.$$

Here we used that $\alpha\delta - \beta\gamma = 1$. Now

$$\gamma(\alpha\tau+\beta)^2 - \alpha^2\tau(\gamma\tau+\delta) = 2\gamma\alpha\beta\tau + \gamma\beta^2 - \delta\alpha^2\tau =$$

$$-\alpha(\alpha\delta-\beta\gamma)\tau+\alpha\beta(\gamma\tau+\delta)-\beta(\alpha\delta-\beta\gamma)=-(\alpha\tau+\beta)+\alpha\beta(\gamma\tau+\delta).$$

This allows us to rewrite G in the form

$$G=-2z-\frac{\alpha\tau+\beta}{\gamma\tau+\delta}+\alpha\beta=-2z-\tau'+\alpha\beta.$$

Putting G back in the expression (5.3) we get

$$e''_{\tau'}(z)=e^{-\pi ik(2z+\tau')}e^{\pi i[k\alpha\beta-2(\beta a-\alpha b)]}.$$

Together with (5.2) this shows that

$$\mathrm{Th}(\{e''_{\tau'}(z)\},\Lambda_{\tau'})=\mathrm{Th}(k,\Lambda_{\tau'})_{a'b'},$$

where

$$(a',b')=(\delta a-\gamma b+\frac{k\gamma\delta}{2},-\beta a+\alpha b-\frac{k\alpha\beta}{2}). \tag{5.4}$$

Summarizing we obtain that, for any $\vartheta(z,\tau)\in\mathrm{Th}(k;\Lambda_\tau)_{ab}$,

$$e^{i\pi k\gamma(\gamma\tau+\delta)z^2}\vartheta((\gamma\tau+\delta)z;\tau)\in\mathrm{Th}(k,\Lambda_{\tau'})_{a'b'}. \tag{5.5}$$

Now let us replace $\left(\begin{smallmatrix}\alpha&\beta\\ \gamma&\delta\end{smallmatrix}\right)$ with its inverse $\left(\begin{smallmatrix}-\delta&-\beta\\ -\gamma&\alpha\end{smallmatrix}\right)$. We rewrite (5.13) and (5.14) as

$$e^{-i\pi k\gamma(-\gamma\tau+\alpha)z^2}\vartheta((-\gamma\tau+\alpha)z;\tau)\in\mathrm{Th}(k,\Lambda_{\tau'})_{a'b'}, \tag{5.6}$$

where

$$(a',b')=(\alpha a+\gamma b-\frac{k\gamma\alpha}{2},\beta a+\delta b+\frac{k\delta\beta}{2}).$$

It remains to replace τ with $\frac{\alpha\tau+\beta}{\gamma\tau+\delta}$ in (5.15) to obtain the assertion of the theorem. □

Substituting $z=0$ we get

Corollary 5.1. *Let $\vartheta_1(z,\tau),\ldots,\vartheta_k(z;\tau)$ be a basis of the space $\mathrm{Th}(k;\Lambda_\tau)_{ab}$ and $\vartheta'_1(z,\tau),\ldots,\vartheta'_k(z;\tau)$ be a basis of $\mathrm{Th}(k;\Lambda_\tau)_{a'b'}$, where (a',b') are defined in the Theorem. Then, for any $M=\left(\begin{smallmatrix}\alpha&\beta\\ \gamma&\delta\end{smallmatrix}\right)\in\mathrm{SL}(2,\mathbb{Z})$ there exists a matrix $A=(c_{ij})\in\mathrm{GL}(k,\mathbb{C})$ depending on M and τ only such that*

$$\vartheta_i(0,\frac{\alpha\tau+\beta}{\gamma\tau+\delta})=\sum_{j=1}^{k}c_{ij}\vartheta'_j(0,\tau).$$

5.2 Let us take $k=1$ and $(a,b)=(\epsilon/2,\eta/2),\epsilon,\eta=0,1$. Applying the previous Theorem, we get

$$\vartheta_{ab}(z;\tau+1)=C\vartheta_{a,b+a+\frac{1}{2}}(z;\tau)$$

for some C depending only on τ and (a,b). In particular,

$$\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau+1)=C\vartheta_{\frac{1}{2}\frac{3}{2}}(z;\tau)=-C\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau).$$

Taking derivative in z at $z=0$ we obtain

$$\vartheta(0;\tau+1)'_{\frac{1}{2}\frac{1}{2}} = -C\vartheta_{\frac{1}{2}\frac{1}{2}}(0;\tau)'.$$

Recall now from (4.14) that

$$\vartheta_{\frac{1}{2}\frac{1}{2}}(0;\tau)' = -2\pi q^{\frac{1}{8}}\prod_{m=1}^{\infty}(1-q^m)^3.$$

Since the substitution $\tau\to\tau+1$ changes q^a into $e^{2\pi a(\tau+1)} = q^a e^{2\pi a}$ we obtain

$$C = e^{\pi i/4}.$$

Similarly, using the formulas (4.16) and (4.17) which give the infinite product expansions for other theta constants, we find

$$\vartheta_{00}(z;\tau+1) = \vartheta_{0\frac{1}{2}}(z;\tau), \tag{5.7}$$

$$\vartheta_{0\frac{1}{2}}(z;\tau+1) = \vartheta_{00}(z;\tau), \tag{5.8}$$

$$\vartheta_{\frac{1}{2}0}(z;\tau+1) = -e^{\pi i/4}\vartheta_{\frac{1}{2}0}(z;\tau). \tag{5.9}$$

Now take $M = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. We have

$$e^{-i\pi z^2/\tau}\vartheta_{00}(z/\tau;-1/\tau) = B\vartheta_{00}(z;\tau)$$

for some B depending only on τ. Plugging in $z=0$ and applying (4.2), we get

$$B = \sqrt{-i\tau}, \tag{5.10}$$

where the square root takes positive values on $\tau\in i\mathbb{R}$.

In particular,

$$\vartheta_{00}(0;-1/\tau) = \sqrt{-i\tau}\,\vartheta_{00}(0;\tau). \tag{5.11}$$

Applying the formula (3.14) we have

$$\begin{aligned} e^{-i\pi z^2/\tau}\vartheta_{0\frac{1}{2}}(\frac{z}{\tau};-\frac{1}{\tau}) &= e^{-i\pi z^2/\tau}\vartheta_{00}(\frac{z}{\tau}+\frac{1}{2};-\frac{1}{\tau}) = \\ e^{-i\pi z^2/\tau}\vartheta_{00}(\frac{z+\frac{\tau}{2}}{\tau};-\frac{1}{\tau}) &= Be^{-i\pi z^2/\tau}e^{i\pi(z+\frac{\tau}{2})^2/\tau}\vartheta_{00}(z+\frac{\tau}{2};\tau) = \\ &Be^{i\pi(\tau/4+z)}\vartheta_{00}(z+\frac{\tau}{2};\tau) = B\vartheta_{\frac{1}{2}0}(z;\tau). \end{aligned} \tag{5.12}$$

In particular,

$$\vartheta(0;-1/\tau)_{0\frac{1}{2}} = \sqrt{-i\tau}\,\vartheta(0;\tau)_{\frac{1}{2}0}. \tag{5.13}$$

Replacing here τ with $-1/\tau$, we obtain

$$\vartheta(0;-1/\tau)_{\frac{1}{2}0} = \sqrt{i\tau}\,\vartheta(0;\tau)_{0\frac{1}{2}}. \tag{5.14}$$

This shows that

$$e^{-i\pi z^2/\tau}\vartheta(z/\tau;-1/\tau)_{\frac{1}{2}0} = \sqrt{i\tau}\,\vartheta(z;\tau)_{0\frac{1}{2}}. \tag{5.15}$$

Finally, using (5.13), (5.14) and (5.15) and applying the Jacobi theorem, we obtain

$$\vartheta(0;-1/\tau)'_{\frac{1}{2}\frac{1}{2}} = -\tau\sqrt{-i\tau}\vartheta_{\frac{1}{2}\frac{1}{2}}(0;\tau)'. \tag{5.16}$$

We know from Theorem 5.1 that

$$e^{-i\pi z^2/\tau}\vartheta(z/\tau;-1/\tau)_{\frac{1}{2}\frac{1}{2}} = B'\vartheta(z;\tau)_{\frac{1}{2}-\frac{1}{2}} = -B'\vartheta(z;\tau)_{\frac{1}{2}\frac{1}{2}}.$$

for some constant B' depending only on τ. Differentiating in z and setting $z=0$ we obtain

$$\frac{1}{\tau}\vartheta(0;-1/\tau)'_{\frac{1}{2}\frac{1}{2}} = B'\vartheta_{\frac{1}{2}\frac{1}{2}}(0;\tau)'.$$

Comparing with (5.16), we get $B' = B$ and hence

$$\vartheta(0;-1/\tau)'_{\frac{1}{2}\frac{1}{2}} = \tau\sqrt{-i\tau}\vartheta(0;-1/\tau)'_{\frac{1}{2}\frac{1}{2}}. \tag{5.17}$$

5.3 We shall interpret the previous computations later by saying that powers of theta constants are modular forms with respect to certain sungroups of the modular group. Right now we only observe the following

Corollary 5.2. *Let $f(\tau) = \vartheta'_{\frac{1}{2}\frac{1}{2}}$. Then, for any $M = \left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$, we have*

$$f(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = \zeta(M)(\gamma\tau+\delta)^{\frac{3}{2}}f(\tau),$$

where $\zeta(M)^8 = 1$.

Proof. We shall prove in the next lecture that it is enough to check this for generators of the group $\mathrm{SL}(2,\mathbb{Z})$. Also we shall show that the group $\mathrm{SL}(2,\mathbb{Z})$ is generated by the matrices $M_1 = \left(\begin{smallmatrix}1 & 1 \\ 0 & 1\end{smallmatrix}\right), M_2 = \left(\begin{smallmatrix}0 & -1 \\ 1 & 0\end{smallmatrix}\right), -I$. We have from (4.14) and (4.15)

$$f(\tau+1)^8 = f(\tau)^8, \quad f(-1/\tau)^8 = \tau^{12}f(\tau)^8.$$

This proves the assertion. □

Corollary 5.3. *Let $\eta(\tau)$ be the Dedekind η-function. Then*

$$\eta(\tau)^{24} = q\prod_{m=1}^{\infty}(1-q^m), \quad q = e^{2\pi i\tau}$$

satisfies

$$\eta(frac\alpha\tau+\beta\gamma\tau+\delta)^{24} = (\gamma\tau+\delta)^{12}\eta(\tau)^{24}.$$

Proof. Use (4.10)

$$\vartheta'_{\frac{1}{2}\frac{1}{2}} = -2\pi\eta(\tau)^3.$$

□

Corollary 5.4. *Let* $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. *Assume that the products* $\alpha\beta, \gamma\delta$ *are even. Then*

$$\Theta(\frac{z}{\gamma\tau + \delta}; \frac{\alpha\tau + \beta}{\gamma\tau + \delta}) = \zeta(\gamma\tau + \delta)^{\frac{1}{2}} e^{\pi i\gamma z^2/(\gamma\tau+\delta)}\Theta(z; \tau), \tag{5.18}$$

where $\zeta^8 = 1$ *and the branch of the square root is chosen to have non-negative real part.*

Proof. Recall that $\Theta(z; \tau) = \vartheta_{00}(z; \tau)$, so Theorem 5.1 gives immediately that

$$\Theta(\frac{z}{\gamma\tau + \delta}; \frac{\alpha\tau + \beta}{\gamma\tau + \delta}) = c(M, \tau)e^{\pi i\gamma z^2/(\gamma\tau+\delta)}\Theta(z; \tau)$$

for some constant $c(M, \tau)$ depending only on M and τ. Take $M = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Then formula (5.13) checks the assertion in this case. Take $M = \left(\begin{smallmatrix} 1 & \pm 2 \\ 0 & 1 \end{smallmatrix}\right)$. Then the assertion follows from (5.10). Now we argue by induction on $|\gamma| + |\delta|$. If $|\delta| > |\gamma|$, using that $\Theta(z, \tau + 2) = \theta(z; \tau)$, we substitute $\tau \pm 2$ in (5.16) to obtain that the assertion is true for $M' = \left(\begin{smallmatrix} \alpha & \beta\pm2\alpha \\ \gamma & \delta\pm2\gamma \end{smallmatrix}\right)$. Since we can decrease $|\delta \pm 2\gamma|$ in this way, the assertion will follow by induction. Note that we used that $|\delta \pm 2\gamma|$ is not equal to $|\delta|$ or $|\gamma|$ because $(\gamma, \delta) = 1$ and $\gamma\delta$ is even. Now, if $|\delta| < |\gamma|$, we use the substitution $\tau \to -1/\tau$. Using (5.13) we see that the asssertion for M follows from the assertion fo $M' = \left(\begin{smallmatrix} \beta & -\alpha \\ \delta & -\gamma \end{smallmatrix}\right)$. This reduces again to the case $|\delta| > |\gamma|$. □

Exercises

5.1 Show that the constant $\zeta(M)$ in (5.16) is equal to $i^{\frac{\delta-1}{2}}(\frac{\gamma}{|\delta|})$ when γ is even and δ is odd. If γ is odd and δ is even, it is equal to $e^{-\pi i\gamma/4}(\frac{\delta}{\gamma})$. Here $(\frac{x}{y})$ is the Jacobi-Legendre symbol, where we also set $(\frac{0}{1}) = 1$.

5.2 Extend the transformation law for theta functons by considering transformations defined by matrices $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ with determinant n not necessary equal to 1:

$$e^{-\pi i\frac{nk\gamma z^2}{\gamma\tau+\delta}}\vartheta(\frac{nz}{\gamma\tau + \delta}; \frac{\alpha\tau + \beta}{\gamma\tau + \delta}) \in \mathrm{Th}(nk, \Lambda_\tau)_{a'b'},$$

where $\vartheta(z; \tau) \in \mathrm{Th}(k, \Lambda_\tau)_{ab}$ and

$$(a', b') = (\alpha a + \gamma b - \frac{k\gamma\alpha}{2}, \beta a + \delta b + \frac{k\delta\beta}{2}).$$

5.3 Using the previous exercise show that

(i) $A\vartheta_{\frac{1}{2}\frac{1}{2}}(z; \tau/2) = \vartheta_{0\frac{1}{2}}(z; \tau)\vartheta_{\frac{1}{2}\frac{1}{2}}(z; \tau)$ for some constant A;

(ii) $A'\vartheta_{\frac{1}{2}0}(z; \tau/2) = \vartheta_{00}(z; \tau)\vartheta_{\frac{1}{2}0}(z; \tau)$ for some constant A';

(iii) (*Gauss' transformation formulas*

$$\vartheta_{\frac{1}{2}0}(0;\tau/2)\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau/2) = 2\vartheta_{\frac{1}{2}0}(z;\tau)\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau),$$

$$\vartheta_{0\frac{1}{2}}(0;\tau/2)\vartheta_{\frac{1}{2}0}(z;\tau/2) = 2\vartheta_{00}(z;\tau)\vartheta_{\frac{1}{2}0}(z;\tau),$$

[Hint: Apply (3.14) to get $A = A'$, then differentiate (i) and use the Jacobi theorem].

5.4 (*Landen's transformation formulas*) Using Exercise 5.2 show

$$\vartheta_{0\frac{1}{2}}(0;2\tau)\vartheta_{\frac{1}{2}\frac{1}{2}}(2z;2\tau) = \vartheta_{\frac{1}{2}0}(z;\tau)\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau),$$

$$\vartheta_{0\frac{1}{2}}(0;2\tau)\vartheta_{0\frac{1}{2}}(2z;2\tau) = \vartheta_{00}(z;\tau)\vartheta_{0\frac{1}{2}}(z;\tau),$$

5.5 Let n be an odd integer.

(i) Show that, for any integer ν, $\vartheta_{0\frac{1}{2}}(\frac{\nu}{n};\tau)$ depends only on the residue of ν modulo n.

(ii) Show that

$$\prod_{\nu=1}^{n-1}\vartheta_{0\frac{1}{2}}(\frac{\nu}{n};\tau) = \prod_{\nu=1}^{n-1}\vartheta_{0\frac{1}{2}}(\frac{2\nu}{n};\tau).$$

(iii) Using Exercises 5.3 and 5.4 show that

$$\frac{\vartheta_{00}(z;2\tau)\vartheta_{\frac{1}{2}0}(z;2\tau)\vartheta_{0\frac{1}{2}}(2z;2\tau)}{\vartheta_{00}(0;2\tau)\vartheta_{\frac{1}{2}0}(0;2\tau)\vartheta_{0\frac{1}{2}}(0;2\tau)} = \frac{\vartheta_{00}(z;\tau)\vartheta_{\frac{1}{2}0}(z;\tau)\vartheta_{0\frac{1}{2}}(z;\tau)}{\vartheta_{00}(0;\tau)\vartheta_{\frac{1}{2}0}(0;\tau)\vartheta_{0\frac{1}{2}}(0;\tau)}.$$

(iv) Show that the expression

$$\frac{\prod_{\nu=1}^{n-1}\vartheta_{00}(\frac{\nu}{n};\tau)\vartheta_{\frac{1}{2}0}(\frac{\nu}{n};\tau)\vartheta_{0\frac{1}{2}}(\frac{\nu}{n};\tau)}{\vartheta_{00}(0;\tau)^{n-1}\vartheta_{\frac{1}{2}0}(0;\tau)^{n-1}\vartheta_{0\frac{1}{2}}(0;\tau)^{n-1}}.$$

does not change when τ is replaced with 2τ.

(v) Show that

$$\frac{\prod_{\nu=1}^{n-1}\vartheta_{00}(\frac{\nu}{n};\tau)\vartheta_{\frac{1}{2}0}(\frac{\nu}{n};\tau)\vartheta_{0\frac{1}{2}}(\frac{\nu}{n};\tau)}{\vartheta_{00}(0;\tau)^{n-1}\vartheta_{\frac{1}{2}0}(0;\tau)^{n-1}\vartheta_{0\frac{1}{2}}(0;\tau)^{n-1}} =$$

$$(-1)^{\frac{n-1}{2}}\left(\frac{\prod_{\nu=1}^{\frac{n-1}{2}}\vartheta_{00}(\frac{\nu}{n};\tau)\vartheta_{\frac{1}{2}0}(\frac{\nu}{n};\tau)\vartheta_{0\frac{1}{2}}(\frac{\nu}{n};\tau)}{\vartheta_{00}(0;\tau)^{n-1}\vartheta_{\frac{1}{2}0}(0;\tau)^{n-1}\vartheta_{0\frac{1}{2}}(0;\tau)^{n-1}}\right)^2$$

(vi) Prove the formula

$$\frac{\prod_{\nu=1}^{\frac{n-1}{2}}\vartheta_{00}(\frac{\nu}{n};\tau)\vartheta_{\frac{1}{2}0}(\frac{\nu}{n};\tau)\vartheta_{0\frac{1}{2}}(\frac{\nu}{n};\tau)}{\vartheta_{00}(0;\tau)^{n-1}\vartheta_{\frac{1}{2}0}(0;\tau)^{n-1}\vartheta_{0\frac{1}{2}}(0;\tau)^{n-1}} = 2^{\frac{1-n}{2}}.$$

5.6 Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Set $t(z;\omega_1,\omega_2) = \vartheta_{\frac{1}{2}\frac{1}{2}}(\frac{z}{\omega_1};\frac{\omega_2}{\omega_1})$.

(i) Show that

$$t(z+\omega_1;\omega_1,\omega_2) = -t(z;\omega_1,\omega_2),$$

$$t(z+\omega_2;\omega_1,\omega_2) = -e^{-\pi i\frac{2z+\omega_2}{\omega_1}}t(z;\omega_1,\omega_2).$$

(ii) Let ω_1',ω_2' be another basis of Λ. Show that

$$t(z;\omega_1',\omega_2') = Ce^{az^2+bz}t(z;\omega_1,\omega_2)$$

for some constants C, a, b.

(iii) By taking the logarithmic derivative of both sides in (ii) show that

$$a = -\frac{t'''(0;\omega_1,\omega_2)}{6t'(0;\omega_1,\omega_2)} + \frac{t'''(0;\omega_1',\omega_2')}{6t'(0;\omega_1',\omega_2')}, \quad b = \frac{t''(0;\omega_1,\omega_2)}{2t'(0;\omega_1,\omega_2)},$$

and

$$C = \frac{t'(0;\omega_1',\omega_2')}{t'(0;\omega_1,\omega_2)};$$

(iv) using (iii) show that

$$a = -\frac{\vartheta'''_{\frac{1}{2}\frac{1}{2}}(0)}{6\vartheta'_{\frac{1}{2}\frac{1}{2}}(0)\omega_1^2} + \frac{\vartheta'''_{\frac{1}{2}\frac{1}{2}}(0)}{6\vartheta'_{\frac{1}{2}\frac{1}{2}}(0){\omega_1'}^2}$$

and $b = 0$;

(v) using the Heat equation (see Exercise 3.8) show that

$$\frac{\vartheta'''_{\frac{1}{2}\frac{1}{2}}(0)}{\vartheta'_{\frac{1}{2}\frac{1}{2}}(0)} = 12\pi i\frac{d\log\eta(\tau)}{d\tau},$$

where $\tau = \frac{\omega_2}{\omega_1}$.

5.7 Define the *Weierstrass σ-function* by

$$\sigma(z;\omega_1,\omega_2) = \omega_1 e^{-z^2(\vartheta'''_{\frac{1}{2}\frac{1}{2}}/6\omega_1^2\vartheta'_{\frac{1}{2}\frac{1}{2}})}\frac{\vartheta_{\frac{1}{2}\frac{1}{2}}(\frac{z}{\omega_1};\frac{\omega_2}{\omega_1})}{\vartheta'_{\frac{1}{2}\frac{1}{2}}(0)}.$$

Show that

(i) $\sigma(z;\omega_1,\omega_2)$ does not depend on the basis ω_1,ω_2 of the lattice Λ;

(ii) $\sigma(-z) = -\sigma(z)$;

(iii)

$$\sigma(z+\omega_1) = -e^{\eta_1(z+\omega_1 2)}\sigma(z), \quad \sigma(z+\omega_2) = -e^{\eta_2(z+\omega_2 2)}\sigma(z),$$

where $\eta_1 = \sigma'(\omega_1 2)/\sigma(\omega_1 2)$; $\eta_2 = \sigma'(\omega_2 2)/\sigma(\omega_2 2)$.

(iv) (*Legendre-Weierstrass relation*)

$$\eta_1\omega_2 - \eta_2\omega_1 = 2\pi i.$$

[Hint: integrate the function σ along the fundamental parallelogram using (iii)];

(v)

$$\eta_1 = -\frac{\pi i}{\omega_1^2}\frac{d\log\eta(\tau)}{d\tau}, \quad \eta_2 = -\frac{\pi i\omega_2}{\omega_1^2}\frac{d\log\eta(\tau)}{d\tau} - \frac{\pi}{2\omega_1},$$

where $\tau = \omega_2/\omega_1$.

5.8 Using formulas from Lecture 4 prove the following infinite product expansion of $\sigma(z;\omega_1,\omega_2)$:

$$\sigma(z;\omega_1,\omega_2) = \frac{\omega_1}{2\pi i}e^{\frac{\eta_1 z^2}{2\omega_1}}(v - v^{-1})\prod_{m=1}^{\infty}\frac{(1-q^m v^{-2})(1-q^m v^2)}{(1-q^m)^2},$$

where $q = e^{2\pi i\frac{\omega_2}{\omega_1}}$, $v = e^{\pi iz/\omega_1}$.

Lecture 6

Modular Forms

6.1 We have seen already in Lecture 5 (5.2) and Corollary 5.3 that the functions $\theta(\tau)^{4k} = \vartheta_{00}(0;\tau)^{4k}$ (resp. $\eta(\tau)^{24}$) satisfy the functional equation

$$f(\tau+2) = f(\tau), \quad f(-1/\tau) = \tau^2 f(\tau),$$

(resp.

$$f(\tau+1) = f(\tau), \quad f(-1/\tau) = \tau^{12} f(\tau)).$$

In fact, they satisfy a more general equation

$$f(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^{2k} f(\tau), \quad \forall \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma, \tag{6.1}$$

where Γ is the subgroup of $\mathrm{SL}(2,\mathbb{Z})$ generated by the matrices $\pm\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \pm\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ (resp. $\pm\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \pm\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$).

To see this we first rewrite (6.1) in the form

$$f(g\cdot\tau) j_g(\tau)^k = f(\tau), \tag{6.2}$$

where

$$j_g(\tau) = \frac{d}{d\tau}\frac{\alpha\tau+\beta}{\gamma\tau+\delta} = (\gamma\tau+\delta)^{-2}. \tag{6.3}$$

By the chain rule

$$j_{gg'}(\tau) = j_g(g'\cdot\tau) j_{g'}(\tau). \tag{6.4}$$

Thus replacing τ with $g'\cdot\tau$ in (6.2), we get

$$(f(g\cdot(g'\cdot\tau)) j_g^k(g'\cdot\tau)) j_{g'}^k(\tau) = f(gg'\cdot\tau) j_{gg'}^k(\tau) = f(\tau).$$

This shows that

$$f(\tau)|_k g := f(g\cdot\tau) j_g(\tau)^k \tag{6.5}$$

satisfies

$$f(\tau)|_k(gg') = (f(\tau)|_k g)|_k g', \quad \forall g, g' \in \Gamma.$$

In other words (6.5) defines a linear representation

$$\rho : \Gamma \to GL(\mathcal{O}(H)^{\mathrm{hol}})$$

of Γ in the space of holomorphic functions on $\mathcal{H}$ defined by

$$\rho(g)(\phi(z)) = \phi|_k g^{-1}. \tag{6.6}$$

Note that we switched here to g^{-1} in order to get

$$\rho(gg') = \rho(g) \circ \rho(g').$$

It follows from the above that to check (6.1) for some subgroup Γ it is enough to verify it only for generators of Γ. Now we use the following:

Lemma 6.1. *The group $G = P\mathrm{SL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/\{\pm\}$ is generated by the matrices*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

These matrices satisfy the relations

$$S^2 = 1, \quad (ST)^3 = 1.$$

Proof. We know that the modular figure $\mathcal{D}$ (more exactly its subset $\mathcal{D}'$) is a fundamental domain for the action of G in the upper half-plane $\mathcal{H}$ by Moebius transformations. Take some interior point $z_0 \in \mathcal{D}$ and any $g \in G$. Let G' be the subgroup of G generated by S and T. If we find an element $g' \in G$ such that $g'g \cdot z_0$ belongs to $\mathcal{D}$, then $g'g = 1$ and hence $g \in G'$. Let us do it. First find $g' \in G'$ such that $\mathrm{Im}\ (g' \cdot (g \cdot z_0))$ is maximal possible. We have, for any $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$,

$$\mathrm{Im}\ g \cdot z = \frac{\mathrm{Im}\ z}{|\gamma\tau + \delta|} \leq \frac{\mathrm{Im}\ z}{|\gamma||z| + |\delta|} < C\mathrm{Im}\ z,$$

where C is a positive constant independent of g. So the set $\{\mathrm{Im}\ g' \cdot z : g' \in G'\}$ is bounded and discrete and hence we can find a maximal element. Take $z = g \cdot z_0$. Let g' realize this maximum. Applying transformations T^n we may assume that $|\mathrm{Re}\ T^n g'g \cdot z_0| \leq \frac{1}{2}$. If $|T^n g'g \cdot z_0| \geq 1$ we are done since $z' = T^n g'g \cdot z_0 \in \mathcal{D}$. If not, we apply S. Then

$$\mathrm{Im}\ S \cdot z' = \mathrm{Im}\ \frac{-1}{z'} = \mathrm{Im}\ \frac{z'}{|z'|^2} < \mathrm{Im}\ z',$$

contradicting the choice of g'. This proves the first assertion. The second one is checked by direct matrix multiplication. □

This explains why (6.1) is satisfied for the functions θ_{00}^k and $\eta(\tau)^{24}$.

Definition. Let Γ be a subgroup of finite index of $\mathrm{SL}(2,\mathbb{Z})$. A holomorphic (resp. meromorphic) function $f:\mathcal{H}\to\mathbb{C}$ satisfying

$$f(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^{2k}f(\tau) = j_g^{-k}(\tau)f(\tau), \quad \forall g = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in\Gamma,$$

is called a *weak modular form* (resp. a *weak meromorphic modular form*) of *weight* k with respect to Γ.

We shall later add one more condition to get rid of the adjective "weak".

Remark 6.1. . Some authors prefer to call $2k$ the weight of a weak modular form admitting k to be equal $1/2$. Since j_g has a meaning for any group Γ acting discretely on a complex manifold M, our definition can be easily extended to a more general situation leading to the notion of an *automorphic form* of weight k.

6.2 Suppose we have $n+1$ linearly independent functions $f_0,\dots,f_n$ satisfying (6.1) (with the same number k). Then we can consider the map

$$f:\mathcal{H}\to\mathbb{CP}^n, \quad \tau\to(f_0(\tau),\dots,f_n(\tau)). \tag{6.7}$$

When we replace τ with $\frac{\alpha\tau+\beta}{\gamma\tau+\delta}$, the coordinates of the image will all multiply by the same number, and hence define the same point in the projective space. This shows that the map f factors through the map

$$\bar{f}:\mathcal{H}/\mathrm{SL}(2,\mathbb{Z})\to\mathbb{CP}^n.$$

Now recall that the points of $\mathcal{H}/\mathrm{SL}(2,\mathbb{Z})$ are in a natural bijective correspondence with the isomorphism classes of elliptic curves. This allows us (under certain conditions) to view the set of elliptic curves as a subset of a projective space and study it by means of algebraic geometry. Other problems on elliptic curves lead us to consider the sets of elliptic curves with additional structure. These sets are parametrized by the quotient $\mathcal{H}/\Gamma$ where Γ is a subgroup of $\mathrm{SL}(2,\mathbb{Z})$ of finite index. To embed these quotients we need to consider functions satisfying property (6.1) but only restriced to matrices from Γ.

Many examples of such functions are obtained from powers of theta constants.

We will need one more property to define a modular form. It is related to the behaviour of $f(z)$ when Im z goes to infinity. Because of this property the image of the map (6.7) is an algebraic variety.

Let Γ be a subgroup of $\mathrm{SL}(2,\mathbb{Z})$ of finite index. We can extend the Moebius action of Γ on $\mathcal{H}$ to the set

$$\mathcal{H}^* = \mathcal{H}\cup\mathbb{Q}\cup\{\infty\} = \mathcal{H}\cup\mathbb{P}^1(\mathbb{Q})$$

by requiring that the subset $\mathbb{P}^1(\mathbb{Q})$ is preserved under this action and the group Γ acts naturally on it with respect to its natural linear action on $\mathbb{Q}^2$:

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\cdot(p,q) = (\alpha p+\beta q, \gamma p+\delta q).$$

In particular, if we identify rational numbers x with points $(x:1)\in\mathbb{P}^1(\mathbb{Q})$ and the infinity ∞ with the point $(1,0)$ we have

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\cdot x=\begin{cases}\frac{\alpha x+\beta}{\gamma x+\delta} & \text{if } \gamma x+\delta\neq 0:\\ \infty & \text{if } \gamma x+\delta=0.\end{cases} \tag{6.8}$$

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\cdot -\frac{\delta}{\gamma}=\infty,$$

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\cdot \infty=\begin{cases}\frac{\alpha}{\gamma} & \text{if } \gamma\neq 0\\ \infty & \text{if } \gamma=0.\end{cases} \tag{6.9}$$

Note that $\mathrm{SL}(2,\mathbb{Z})$ acts transitively on the set $\mathbb{Q}\cup\{\infty\}$. In fact for any rational number $x=\frac{p}{q}$ with $(p,q)=1$ we can find a pair of integers u,v such that $up-vq=1$ so that

$$\begin{pmatrix}u & -v\\ -q & p\end{pmatrix}\cdot\frac{p}{q}=\infty.$$

Thus any subgroup of finite index Γ of $\mathrm{SL}(2,\mathbb{Z})$ has only finitely many orbits on $\mathbb{Q}\cup\{\infty\}$. Each such orbit is called a *cusp* of Γ. For each cusp $c=\Gamma\cdot x$ of Γ represented by a rational number x or ∞ the stabilizer group Γ_x is conjugate to a subgroup of $\mathrm{SL}(2,\mathbb{Z})_\infty$. In fact, if $g\cdot x=\infty$ for some $g\in\mathrm{SL}(2,\mathbb{Z})$, then

$$g\cdot\Gamma_x\cdot g^{-1}\cdot\infty=\infty.$$

Since

$$\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\cdot\infty=\infty\Leftrightarrow\gamma=0,$$

we have

$$g\cdot\Gamma_x\cdot g^{-1}\subset\{\pm\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix},\beta\in\mathbb{Z}\}$$

Let h be the smallest positive β occured in this way. Then it is immediately seen that $g\cdot\Gamma_x\cdot g^{-1}$ is generated by the matrices

$$T^h=\pm\begin{pmatrix}1 & h\\ 0 & 1\end{pmatrix},\quad -I=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}.$$

The number h is also equal to the index of the subgroup $g\cdot\Gamma_x\cdot g^{-1}$ in $\mathrm{SL}(2,\mathbb{Z})_\infty=(T,-I)$. In particular, all x from the same cusp of Γ define the same number h. We shall call it the *index* of the cusp. Let $f(\tau)$ be a holomorphic function satisfying (6.1). For each $x\in\mathbb{Q}\cup\{\infty\}$ consider the function $\phi(\tau)=f(\tau)|_k g^{-1}$, where $g\cdot x=\infty$ for some $g\in\mathrm{SL}(2,\mathbb{Z})$. We have

$$\phi(\tau)|_k g\Gamma_x g^{-1}=f(\tau)|_k g^{-1}g\Gamma_x g^{-1}=f(\tau)|_k\Gamma_x g^{-1}=f(\tau)|_k g^{-1}=\phi(\tau).$$

This implies that $\phi(\tau)$ satisfies (6.1) with respect to the group $g\Gamma_x g^{-1}$. Since the latter contains the transformation T^h we have

$$\phi(T^h\cdot\tau)=\phi(\tau+h)=\phi(\tau).$$

Thus we can consider the Laurent expansion of $\phi(\tau)$

$$\phi(\tau) = \sum_{r\in\mathbb{Z}} c_r q^r, \quad q = e^{2\pi i\tau/h}. \tag{6.10}$$

This converges for all $q \neq 0$. We say that $f(\tau)$ is *holomorphic at a cusp* (resp. *meromorphic*) if $a_r = 0$ for $r < 0$ (resp. $a_r = 0$ for $r < -N$ for some positive N). It is easy to see that this definition is independent of the choice of a representative x of the cusp. Now we are ready to give our main definition:

Definition. A holomorphic (resp. meromorphic) function $f(\tau)$ on the the upper half-plane $\mathcal{H}$ is called a *modular form* (resp. *meromorphic modular form*) of *weight* k with respect to a subgroup Γ of $\mathrm{SL}(2,\mathbb{Z})$ of finite index if it is holomorphic (resp. meromorphic) at each cusp and satisfies

$$f(g\cdot\tau) = j_g(\tau)^k f(\tau), \quad \forall g\in\Gamma.$$

A modular form is called a *cusp form* or a *parabolic form* if its Fourier expansion at each cusp has no constant term. A meromorphic modular form of weight 0 is called a *modular function* with respect to Γ.

6.3 Let us give some examples.

Example 6.1. Let

$$\Delta(\tau) = \eta(\tau)^{24}.$$

It is called the *discriminant* function. We know that $\Delta(\tau)$ satisfies (6.1) with $k = 6$ with respect to the group $\Gamma = \mathrm{SL}(2,\mathbb{Z})$. By (4.9)

$$\Delta(\tau) = \frac{1}{(2\pi)^8}{\vartheta'_{\frac12\frac12}}^8.$$

Since

$$\Delta(\tau) = q\prod_{m=1}^{\infty}(1-q^m)^{24}$$

we see that the Fourier expansion of $\Delta(\tau)$ contains only positive powers of q. This shows that $\Delta(\tau)$ is a cusp form of weight 6.

Example 6.2. The function $\vartheta_{00}(\tau)$ has the Fourier expansion $\sum q^{m^2/2}$. It is convergent at $q = 0$. So ϑ_{00}^{4k} is a modular form of weight k. It is not a cusp form.

Let us give more examples of modular forms. This time we use the groups other than $\mathrm{SL}(2,\mathbb{Z})$. For each N let us introduce the *principal congruence subgroup* of $\mathrm{SL}(2,\mathbb{Z})$ of *level* N

$$\Gamma(N) = \{M = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in\mathrm{SL}(2,\mathbb{Z}) : M\equiv I \mod N\}.$$

Notice that the map

$$\mathrm{SL}(2,\mathbb{Z})\to\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z}), \quad \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\to\begin{pmatrix}\bar\alpha & \bar\beta\\ \bar\gamma & \bar\delta\end{pmatrix}$$

is a homomorphism of groups. Being the kernel of this homomorphism, $\Gamma(N)$ is a normal subgroup of $\Gamma(1) = \mathrm{SL}(2,\mathbb{Z})$. I think it is time to name the group $\Gamma(1)$. It is called the *full modular group*.

We have

Lemma 6.2. *The group $\Gamma(2)$ is generated by the matrices*

$$-I, \quad T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad ST^2S = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}.$$

Proof. Let H be the subgroup of $\Gamma(1)$ generated by $T^2, -I$ and ST^2S^{-1}. We know that $\Gamma(1)$ is generated by T and S, it is easy to verify that H is a normal subgroup of $\Gamma(1)$ contained in $\Gamma(2)$. Since $\Gamma(1)/\Gamma(2) \cong \mathrm{SL}(2, \mathbb{Z}/2)$ it suffices to show that the natural homomorphism $\phi : \Gamma(1)/H \to \mathrm{SL}(2, \mathbb{Z}/2)$ is injective. Let $g \in \Gamma(1) \setminus H$ be an element of the kernel of ϕ. It can be written as a word in S and T. Since

$$\phi(T) = \phi(T^{-1}), \quad \phi(T^2) = 1, \quad S^2 = 1, \quad S^{-1} = S,$$

we can replace g with another element from the same coset modulo H to assume that g is a word in S and T where no S^2 or T^2 appears. Since we know that $(ST)^3 = STSTST = 1$, we have the following possible expressions for g:

$$S,\ ST,\ STS,\ STST,\ STSTS,\ T.$$

Here we used that $\phi(TS) = \phi(ST)^{-1}$ since $\phi(T^2S^2) = 1$ and similarly

$$\phi(TST) = \phi(STS)^{-1}, \phi(TSTS) = \phi(STST)^{-1},$$

$$\phi(TSTST) = \phi(STSTS)^{-1}.$$

Also $\phi(ST) = \phi(STST)^{-1}$. Thus it is enough to verify that the elements $S,\ ST,\ STS,$ T are not in the kernel, i.e. do not belong to $\Gamma(2)$. This is verified directly. □

Example 6.3. Consider the theta constants $\vartheta_{\frac{\epsilon}{2}\frac{\epsilon}{2}}$. Applying the transformation $\tau' = \tau + 1$ twice and using formulas (5.1) , we obtain

$$\vartheta_{00}(\tau + 2) = \vartheta_{0\frac{1}{2}}(\tau + 1) = \vartheta_{00}(\tau),$$

$$\vartheta_{0\frac{1}{2}}(\tau + 2) = \vartheta_{00}(\tau + 1) = \vartheta_{0\frac{1}{2}}(\tau),$$

$$\vartheta_{\frac{1}{2}0}(\tau + 2) = e^{\pi i/4}\vartheta_{\frac{1}{2}0}(\tau + 1) = e^{\pi i/2}\vartheta_{\frac{1}{2}0}(\tau).$$

Next, using formulas (5.11)-(5.14), we have

$$\vartheta_{00}(ST^2S\tau) = \vartheta_{00}(\left(\begin{smallmatrix} -1 & 0 \\ 2 & -1 \end{smallmatrix}\right) \cdot \tau) = \vartheta_{00}(\frac{-1}{(-1/\tau) + 2}) = e^{3\pi i/4}(\frac{-1}{\tau} + 2)^{1/2}\vartheta_{00}(\frac{-1}{\tau} + 2) =$$

$$e^{3\pi i/4}(-\frac{1}{\tau} + 2)^{1/2}\vartheta_{00}(-\frac{1}{\tau}) =$$

$$e^{3\pi i/2}(-\frac{1}{\tau} + 2)^{1/2}(\tau)^{1/2}\vartheta_{00}(\tau) = -i(2\tau - 1)^{1/2}\vartheta_{00}(\tau).$$

Similarly we obtain

$$\vartheta_{0\frac{1}{2}}(ST^2S\tau) = e^{3\pi i/4}(-\frac{1}{\tau} + 2)^{1/2}\vartheta_{\frac{1}{2}0}(-\frac{1}{\tau} + 2) =$$

$$ie^{3\pi i/4}(-\frac{1}{\tau}+2)^{1/2}\vartheta_{\frac{1}{2}0}(-\frac{1}{\tau}) = (2\tau-1)^{1/2}\vartheta_{0\frac{1}{2}}(\tau),$$

$$\vartheta_{\frac{1}{2}0}(ST^2S\tau) = -i(2\tau-1)^{1/2}\vartheta_{0\frac{1}{2}}(\tau).$$

Applying Lemma 6.2, this shows that

$$\vartheta_{00}(\tau)^4, \quad \vartheta_{\frac{1}{2}0}(\tau)^4, \quad \vartheta_{0\frac{1}{2}}(\tau)^4 \tag{6.11}$$

are weak modular forms with respect to the group $\Gamma(2)$. This group has three cusps represented by $0, 1$, and ∞. Since Γ_∞ is generated by the matrices $\pm T^2$, we see that ∞ is the cusp of $\Gamma(2)$ of index 2. Since the subgroup $\Gamma(2)$ is normal in $\Gamma(1)$ all cusps have the same index. Also it is enough to check the condition of holomorphicity only at one cusp, say the ∞. By formula (4.6) $\vartheta_{ab}(\tau)^4$ has infinite product in $q^{\frac{1}{2}} = e^{\pi i\tau}$ with only non-negative powers of q. Thus the functions (6.11)) are modular forms of weight 1 with respect to $\Gamma(2)$. Since

$$\vartheta_{\frac{1}{2}0}(\tau)^4 = 2^4 q^{\frac{1}{2}} \prod_{m=1}^{\infty}(1-q^m)^4(1+q^m)^8,$$

we see that $\vartheta_{\frac{1}{2}0}^4$ is a cusp form.

6.4 We know that any elliptic curve is isomorphic to a Hesse cubic curve. Let us give another cubic equation for an elliptic curve, called a Weierstrass equation. Its coefficients will give us new examples of modular forms. Recall that $\dim \mathrm{Th}(k,\Lambda_\tau)_{ab} = k$. Let use $<,>$ to denote the linear span. We have

$$\mathrm{Th}(1,\Lambda_\tau)_{\frac{1}{2}\frac{1}{2}} =< \vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau) >=< T >;$$

$$\mathrm{Th}(2,\Lambda_\tau) =< T^2, X' >,$$

$$\mathrm{Th}(3,\Lambda_\tau)_{\frac{1}{2}\frac{1}{2}} =< T^3, TX', Y' >,$$

for some functions $X' \in \mathrm{Th}(2,\Lambda_\tau), Y' \in \mathrm{Th}(3,\Lambda_\tau)_{\frac{1}{2}\frac{1}{2}}$. Now the following seven functions

$$T^6,\ T^4X',\ T^2X'^2,\ X'^3,\ T^3Y',\ TX'Y',\ Y'^2$$

all belong to the space $\mathrm{Th}(6,\Lambda_\tau)$. They must be linearly dependent and we have

$$aT^6 + bT^4X'^2 + cT^2X'^2 + dX'^3 + eT^3Y' + fTX'Y' + gY'^2 = 0. \tag{6.12}$$

Assume $g \neq 0, d \neq 0$. It is easy to find

$$X = \alpha X + \beta T^2, \quad Y = \gamma Y' + \delta XT + \omega T^3$$

which reduces this expression to the form

$$Y^2T - X^3 - AXT^4 - BT^6 = 0, \tag{6.13}$$

for some scalars A, B. Let

$$\wp(z) = X/T^2, \quad \wp_1(z) = Y/T^3.$$

Dividing (6.13) by T^6 we obtain a relation

$$\wp_1(z)^2 = \wp(z)^3 + A\wp(z) + B. \tag{6.14}$$

Since both X and T^2 belong to the same space $\mathrm{Th}(2,\tau)$ the functions $\wp(z), \wp_1(z)$ have periods $\lambda \in \mathbb{Z} + \tau\mathbb{Z}$ and meromorphic on $\mathbb{C}$. As we shall see a little later, $\wp_1(z) = \frac{d\wp}{dz}$. Consider the map

$$E_\tau = \mathbb{C}/\Lambda \to \mathbb{P}^2, \quad z \to (T(z)^3, T(z)X(z), Y(z)).$$

Since $T(z)^3, T(z)X(z), Y(z)$ all belong to the same space $\mathrm{Th}(3,\Lambda_\tau)_{\frac{1}{2},\frac{1}{2}}$ this map is well-defined and holomorphic. It differs from the map from Example 3.2 only by a composition with a translation on E_τ and a linear change of the projective coordinates coordinates. This is because, for any $f \in \mathrm{Th}(k;\Lambda)$ we have

$$e^{\pi i[a^2\tau+2(z+a)b]} f(z + \frac{b+a\tau}{k}) \in \mathrm{Th}(k;\Lambda)_{ab}$$

(see Lecture 3). So it is an isomorphism onto its image. The relation (6.13) tells us that the image is the plane projective curve of degree 3 given by the equation

$$y^2t - x^3 - Axt^2 - Bt^3 = 0, \tag{6.15}$$

Now it is clear why we assumed that the coefficients d, g in (6.12) are not equal to zero. If $g = 0$, we obtain an equation $f(x,y,t) = 0$ for the image of E_τ in which y enters only in the first degree. Thus we can express y in terms of x, t and obtain that E_τ is isomorphic to $\mathbb{P}^1(\mathbb{C})$. If $d = 0$ we obtain that f could be chosen of degree 2. Again this is impossible. Note that we also have in (6.13)

$$4A^3 + 27B^2. \neq 0 \tag{6.16}$$

This is the condition that the polynomial $x^3 + Ax^2 + B$ does not have a multiple root. If it has, (6.13) does not define a Riemann surface. A cubic equation of the form (6.15) with the condition (6.16) is called a *Weierstrass cubic equation*.

We know from Lecture 3 that $T = \vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau)$ has simple zeroes at the points $z = \lambda \in \Lambda_\tau$. Since X does not vanish at these points (it is a linear combinations of T^2 and $\vartheta_{00}(z;\tau)^2$), $\wp(z)$ has poles of order 2 at $z \in \Lambda$. Differentiating (6.14), we obtain

$$2\wp_1(z)\wp_1(z)' = (3\wp(z)^2 + A)\wp(z)'.$$

Let $\wp_1(z_1) = 0$. If $3\wp(z_1)^2 + A = 0$, the polynomial $x^3 + Ax + B$ is reducible since $\wp(z_1)$ must be its double root. So, $\wp_1(z)$ has common roots with $\wp(z)'$. Now both functions have a pole of order 3 at points from Λ. This shows that the function $\wp_1/\wp'$ has no poles and zeroes, hence it is constant. Let $c\wp_1 = \wp$. Replacing $\wp_1$ by $c^3\wp_1$, $\wp$ by $c^2\wp$, A by c^4A, B by c^6B we may assume that

$$\wp_1(z) = \wp(z)'. \tag{6.17}$$

Let

$$\wp(z) = a_{-2}z^{-2} + a_2z^2 + \dots$$

be the Laurent expansion of $\wp(z)$ at 0. Note that $\wp(z)$ must be an even function since all functions in $\mathrm{Th}(2,\Lambda_\tau)$ are even. We have

$$\wp_1(z)=\wp(z)'=-2a_{-2}z^{-3}+2a_2z+\dots.$$

Plugging in the equation (6.11) we obtain $4a_{-2}^2=a_{-2}^3$ hence $a_{-2}=4$. Finally, if we replace $\wp(z)$ with $\wp(z)/4$ we can assume that

$$\wp(z)=z^{-2}+c_2z^2+c_4z^4+\dots, \tag{6.18}$$

and

$$\wp(z)'^2=4\wp(z)^3-g_2\wp(z)-g_3. \tag{6.19}$$

Here we use the classical notation for the coefficients of the *Weierstrass equation.* Differentiating (6.18) we find

$$\wp(z)'=-2z^{-3}+2c_2z+4c_4z^3+\dots, \tag{6.20}$$

Plugging this in the Weierstrass equation (6.19), we easily get

$$\wp(z)'^2-4\wp(z)^3=-20c_2z^{-2}-28c_4+z^2(\dots).$$

Thus the function $\wp(z)'^2-4\wp(z)^3+20c_2\wp(z)+28c_4$ is holomorphic and periodic. It must be a constant. Since it vanishes at 0, it is identical zero. Comparing this with the Weierstrass equation, we find that

$$g_2=20c_2,\quad g_3=28c_4. \tag{6.21}$$

After all of these normalizations, the elliptic function $\wp(z)$ with respect to Λ_τ is uniquely determined by the conditions (6.18) and (6.19). It is called called the *Weierstrass function* with respect to the lattice Λ_τ.

One can find explicitly the function $\wp(z)$ as follows. I claim that

$$\wp(z)=\phi(z):=\frac{1}{z^2}+\sum_{\lambda\in\Lambda\setminus\{0\}}\left(\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right). \tag{6.22}$$

First of all the series (6.22) is absolutely convergent on any compact subset of $\mathbb{C}$ not containing 0. We shall skip the proof of this fact (see for example [**Cartan**])[?]. This implies that $\phi(z)$ is a meromorphic function with pole of order 2 at 0. Its derivative is a meromorphic function given by the series

$$\phi(z)'=-2\sum_{\lambda\in\Lambda}\frac{1}{(z-\lambda)^3}.$$

It is obviously periodic. This implies that $\phi(z)$ is periodic too.

Since $\phi(z)$ is an even function, $\phi(z)'$ is odd. But then it must vanish at all $\lambda\in\frac{1}{2}\Lambda$. In fact

$$\phi'(-\lambda/2)=-\phi'(\lambda/2)=-\phi'(-\lambda/2+\lambda)=-\phi'(\lambda/2).$$

The same argument shows that $\wp(z)'$ vanishes at the same points. It follows from the Cauchy residue formula that the number of zeroes minus the number of poles of a meromorphic double periodic function inside of its fundamental parallelogram is equal to zero (see computations from Lecture 3). This shows that ϕ' and $\wp'$ has the same set of zeroes and poles counting with multiplicities. This implies that $\phi'(z) = c\wp(z)'$ for some constant c. Now comparing the coefficients at z^{-3} we see that $c = 1$. So $\wp(z)' = \phi(z)'$. After integrating we get $\wp(z) = \phi(z)$+constant. Again comparing the terms at z^{-2} we get $\phi(z) = \wp(z)$. This proves (6.22).

After differentiating $\wp(z)$ at 0 we obtain

$$c_2 = 3 \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^4}, \quad c_4 = 5 \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^6}.$$

Remark 6.2. Now it is time to explain the reason for the names "elliptic functions" and "elliptic curves". We know that the Weierstrass function $\wp(z;\tau)$ is a solution of the differential equation $(\frac{dx}{dz})^2 = 4x^3 - g_2x - g_3$. Thus the function $z = \wp^{-1}(x)$ is given, up to adding a constant, by the indefinite integral

$$z = \int \frac{dx}{\sqrt{4x^3 - g_2x - g_3}}. \tag{6.23}$$

This is called an *elliptic integral*. Of course, the function $x = \wp(z)$ does not have single-valued inverse, so one has to justify the previous equality. To do this we consider a non-empty simply connected region U in the complex plane $\mathbb{C}$ which does not contain the roots e_1, e_2, e_3 of the polynomial $4x^3 - g_2x - g_3$. Then we define $f : U \to \mathbb{C}$ by

$$f(u) = \int_u^\infty \frac{dx}{\sqrt{4x^3 - g_2x - g_3}}$$

This is independent of the path from u to ∞ since U is simply connected. Using analytic continuation we obtain a multivalued holomorphic function defined on $\mathbb{C} \setminus \{e_1, e_2, e_3\}$. Using the chain rule one verifies that $\wp(f(u)) = \pm u$. So, f is well-defined as a holomorphic map from $\mathbb{C} \setminus \{e_1, e_2, e_3\}$ to $(\mathbb{C}/\Lambda_\tau)/(z \to -z)$. It can be shown that it extends to a holomorphic isomorphism from the Weierstrass cubic $y^2 = 4x^3 - g_2x - g_3$ onto $(\mathbb{C}/\Lambda_\tau) \setminus \{0\}$. This is the inverse of the map given by $z \to (\wp(z), \wp(z)')$. As was first shown by Euler, the elliptic integral (6.23) with special values of g_2 and g_3 over a special path in the real part of the complex plane x gives the value of the length of an arc of an ellipse. This explains the names "elliptic".

6.5 Next we shall show that, considered as functions of the lattice $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, and hence as functions of τ, the coefficients g_2 and g_3 are modular forms of level 4 and 6, respectively. Set for any positive even integer k:

$$E_k(\tau) = \sum_{\lambda \in \Lambda_\tau \setminus \{0\}} \frac{1}{\lambda^k}.$$

Assume $|\tau| > R > 0$ and $k > 2$. Since

$$\sum_{\lambda \in \mathbb{Z} + \tau\mathbb{Z} \setminus \{0\}} \frac{1}{|\lambda|^k} < \int\int_{|x+iy|>R} |x+iy|^{-k} dxdy =$$

$$\int_R^\infty \int_0^{2\pi} r^{-k+1} dr d\theta = 2\pi \int_R^\infty r^{1-k} dr,$$

we see that $E_k(\tau)$ is absolutely convergent on any compact subset of $\mathcal{H}$. Thus $E_k(\tau)$ are holomorphic functions on $\mathcal{H}$ for $k > 2$. From (6.21) we infer

$$g_2 = 60E_4, \quad g_3 = 140E_6. \tag{6.24}$$

We have

$$E_k(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = \sum_{(m,n)\neq 0} [m(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) + n]^{-k} =$$

$$(\gamma\tau+\delta)^k \sum_{(m,n)\neq 0} [(m\alpha+n\gamma)\tau + (m\beta+n\delta)]^{-k} = (\gamma\tau+\delta)^k E_k(\tau).$$

This shows that $E_k(\tau)$ is a weak modular form with respect to the full modular group $\Gamma(1)$. We can also compute the Fourier expansion at the cusp ∞. We have

$$E_k(\tau) = \sum_{m\in\mathbb{Z}\setminus\{0\}} \frac{1}{m^k} + \sum_{n\in\mathbb{Z}\setminus\{0\}} \Big(\sum_{m\in\mathbb{Z}} \frac{1}{(m+n\tau)^k}\Big).$$

Since k is even, this can be rewritten in the form

$$E_k(\tau) = 2\sum_{m\in\mathbb{N}} \frac{1}{m^k} + 2\sum_{n\in\mathbb{N}}(\sum_{m\in\mathbb{Z}} \frac{1}{(m+n\tau)^k}) = 2(\zeta(k) + \sum_{n\in\mathbb{N}}(\sum_{m\in\mathbb{Z}} \frac{1}{(m+n\tau)^k}),$$

where

$$\zeta(s) = \sum_{m\in\mathbb{N}} \frac{1}{m^s}, \quad \text{Re } s > 1$$

is the *Riemann zeta function*. Now we use the well-known formula (see for example **[Cartan]**, Chapter V, §2, (3.2)):

$$\pi\cot(\pi z) = \sum_{m\in\mathbb{Z}}^{\infty} (z+m)^{-1}.$$

Setting $t = e^{2\pi i z}$, we rewrite the left-hand side as follows:

$$\pi\cot(\pi z) = \pi\frac{\cos\pi z}{\sin\pi z} = i\pi\frac{e^{\pi i z}+e^{-\pi i z}}{e^{\pi i z}-e^{-\pi i z}}) = i\pi\frac{t+1}{t-1} = i\pi(1 - 2\sum_{m=0}^{\infty} t^m).$$

Differentiating $k-1 \geq 2$ times in z, we get

$$(k-1)!\sum_{m\in\mathbb{Z}}^{\infty} (z+m)^{-k} = (2\pi i)^k \sum_{m=1}^{\infty} m^{k-1}t^m.$$

This gives us the needed Fourier expansion of $E_k(\tau)$. Replace in above z with $n\tau$, set $q = e^{2\pi i\tau}$ to obtain

$$E_k(\tau) = 2\zeta(k) + \sum_{n\in\mathbb{N}} \frac{2(2\pi i)^k}{(k-1)!}(\sum_{m=1}^{\infty} m^{k-1}q^{nm}). \tag{6.25}$$

It is obviously convergent at $q = 0$. So, we obtain that $E_k(\tau)$ is a modular form of weight $k/2$ with respect to the full modular group $\Gamma(1)$. It is called the *Eisenstein form* of weight $k/2$. Recall that k must be even and also $k \geq 4$. One can rewrite (6.21) in the form

$$E_k(\tau) = 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}\sigma_{k-1}(m)q^m, \tag{6.26}$$

where

$$\sigma_n(m) = \sum_{d|m} d^n = \quad \text{sum of } n^{\text{th}} \text{ powers of all positive divisors of } m.$$

Now we observe that we have 3 modular forms of weight 6 with respect to $\Gamma(1)$. They are $g_2^3 = 60^3E_4^3, g_3 = (140)^2E_6^2, \Delta$. There is a linear relation between these 3 forms:

Theorem 6.1.

$$(2\pi)^{12}\Delta = g_2^3 - 27g_3^2.$$

Proof. First notice that $g_2^3 - 27g_3^2$ is equal to the discriminant of the cubic polynomial $4x^3 - g_2x - g_3$ (this is the reason for naming Δ the discriminant). Thus the function $g_2^3 - 27g_3^2$ does not vanish for any $\tau \in \mathcal{H}$. Since Δ is proportional to a power of $\vartheta'_{\frac{1}{2}\frac{1}{2}}$ and the latter does not vanish on $\mathcal{H}$ (because $\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau)$ has zero of the first order at 0), we see that Δ also does not vanish on $\mathcal{H}$. Now consider the ratio $g_2^3 - 27g_3^2/\Delta$. It has neither zeroes nor poles in $\mathcal{H}$. Let us look at its behaviour at infinity. Let

$$X = \sum_{n=1}^{\infty}\sigma_3(n)q^n, \quad Y = \sum_{n=1}^{\infty}\sigma_5(n)q^n.$$

We use the well-known formula (see, for example,[**Serre**][**?**]),)

$$\zeta(2r) = \frac{2^{2r-1}}{(2r)!}B_{2r}\pi^{2r},$$

where B_i are the Bernoulli numbers defined by the identity

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{i=1}^{\infty}(-1)^{i+1}B_i\frac{x^{2i}}{(2i)!}.$$

In particular, $120\zeta(4) = (2\pi)^4/12, \quad 280\zeta(6) = (2\pi)^6/216$ and we can write

$$g_2 = (2\pi)^4[\frac{1}{12} + 20X], \quad g_3 = (2\pi)^6[\frac{1}{216} - \frac{7Y}{3}].$$

This gives

$$g_2^3 - 27g_3^2 = (2\pi)^{12}[(5X + 7Y)/12 + 100X^2 + 20X^3 - 42Y^2] =$$

$$(2\pi)^{12}q + q^2(\dots).$$

Now from Example 6.1 we have $\Delta(\tau) = q + q^2(\dots)$. This shows that the ratio $R = g_2^3 - 27g_3^2/\Delta$ is holomorphic at ∞ too. This implies that R is bounded on the fundamental domain $\mathcal{D}$ of $\Gamma(1)$. Since R is invariant with respect to $\Gamma(1)$ we see that R is bounded on the whole upper half-plane. By Liouville's theorem it is constant. Comparing the coefficients at q, we get the assertion. $\square$

6.6 Recall that we constructed the modular forms g_2 and g_3 as the coefficients of the elliptic function $\wp(z;\tau)$ in its Taylor expansion at $z=0$. The next theorem gives a generalization of this construction providing a convenient way to construct modular forms with respect to a subgroup of finite index Γ of $\mathrm{SL}(2,\mathbb{Z})$.

Theorem 6.2. *Let $\Phi(z;\tau)$ be a meromorphic periodic function in z with respect to the lattice $\Lambda_\tau = \mathbb{Z}+\mathbb{Z}\tau$. Assume that, as a function of τ, it satisfies*

$$\Phi(\frac{z}{\gamma\tau+\delta};\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^m\Phi(z;\tau), \quad \forall \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \Gamma \subset \Gamma(1)$$

Let $g_n(\tau)$ be the n-th coefficient of the Taylor expansion of $\Phi(z;\tau)$ at $z_0 = x\tau+y$ for some $x,y\in\mathbb{R}$. Then

$$g_n(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^{m+n}g_n(\tau),$$

for any $M\in\mathrm{SL}(2,\mathbb{Z})$ such that $(x',y') = (x,y)\cdot M \equiv (x,y) \mod \mathbb{Z}^2$.

Proof. Use the Cauchy formula

$$g_n(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = \frac{1}{2\pi i}\oint \frac{\Phi(z+x\frac{\alpha\tau+\beta}{\gamma\tau+\delta}+y;\frac{\alpha\tau+\beta}{\gamma\tau+\delta})}{z^{n+1}}dz =$$

$$\frac{1}{2\pi i}\oint \frac{\Phi(\frac{z(\gamma\tau+\delta)+x(\alpha\tau+\beta)+y(\gamma\tau+\delta)}{\gamma\tau+\delta};\frac{\alpha\tau+\beta}{\gamma\tau+\delta})}{z^{n+1}}dz =$$

$$\frac{1}{2\pi i}\oint \Phi(z(\gamma\tau+\delta)+x(\alpha\tau+\beta)+y(\gamma\tau+\delta);\tau)(\gamma\tau+\delta)^m z^{n+1}dz =$$

$$\frac{1}{2\pi i}\oint \frac{\Phi(z(\gamma\tau+\delta)+x'\tau+y';\tau)(\gamma\tau+\delta)^m}{z^{n+1}}dz =$$

$$\frac{1}{2\pi i}\oint \frac{\Phi(z(\gamma\tau+\delta)+x\tau+y;\tau)(\gamma\tau+\delta)^m}{z^{n+1}}dz.$$

here we integrate along a circle of a small radius with center at 0 in a counterclockwise direction.

After substitution $z(\gamma\tau+\delta) = z'$, we obtain

$$g_n(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^{m+n}g_n(\tau).$$

□

Example 6.4. We apply the previous theorem to $\Phi(z;\tau) = \wp(z)$ and $z=\frac{1}{2}$. In this case

$$\Gamma = \Gamma_0(2) = \{\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \Gamma(1) : 2|\gamma\}.$$

Now, replacing z with $z/(\gamma\tau+\delta)$ in (6.22), we get

$$\wp(\frac{z}{\gamma\tau+\delta};\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^2[z^{-2}+\sum_{(m,n)\neq(0,0)}\frac{1}{z-m(\gamma\tau+\delta)+n(\alpha\tau+\beta)}].$$

Since $\mathbb{Z}+\mathbb{Z}\tau = \mathbb{Z}(\gamma\tau+\delta)+\mathbb{Z}(\alpha\tau+\beta)$, we get finally that

$$\wp(\frac{z}{\gamma\tau+\delta};\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^2\wp(z;\tau).$$

Thus $\wp(z;\tau)$ satisfies the assumption of the Lemma with $m=2$. Let $M\in\Gamma(1)$. Since $(0,\frac{1}{2})\cdot M-(\frac{1}{2},0)\in\mathbb{Z}^2$ if and only if $M\in\Gamma_0(2)$ we obtain that the 0-th coefficient $g_0(\tau)=\wp(\frac{1}{2})$ of the Taylor expansion of $\wp(z)$ at $\frac{1}{2}$ satisfies

$$\wp(\frac{1}{2};\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^2\wp(\frac{1}{2};\tau).$$

Similarly, if we replace $\frac{1}{2}$ with $\frac{\tau}{2}$ and $\frac{\tau}{2}+\frac{1}{2}$ we get that

$$\wp(\frac{\tau}{2};\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^2\wp(\frac{\tau}{2};\tau), \quad \forall\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in\Gamma^0(2),$$

where

$$\Gamma^0(2) = \{\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in\Gamma(1):2|\beta\} = \begin{pmatrix}1 & 1\\ -1 & 0\end{pmatrix}\Gamma_0(2)\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}.$$

$$\wp(\frac{\tau}{2}+\frac{1}{2};\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^2\wp(\frac{\tau}{2}+\frac{1}{2};\tau).$$

We skip the verification that $\wp(\frac{\tau}{2})$ and $\wp(\frac{1}{2})$ satisfy the regularity condition at the cusps. Since both $\Gamma_0(2)$ and $\Gamma^0(2)$ contain $\Gamma(2)$ as its subgroup, we see that

$$\wp(\frac{\tau}{2}+\frac{1}{2}), \quad \wp(\frac{\tau}{2}), \quad \wp(\frac{1}{2})$$

are modular forms of weight 1 with respect to $\Gamma(2)$.

Exercises

6.1 Show that $\wp(z)$ is a time independent solution of the *Kortweg-de Vries partial differential equation*

$$u_t = u_{xxx}-12uu_x, u=u(x,t).$$

6.2 Compute the first two coefficients c_6, c_8 in the Laurent expansion of $\wp(z)$.

6.3 Show that $\wp(z) = -\frac{d^2}{dz^2}\log\vartheta_{\frac{1}{2}\frac{1}{2}}(z;\tau)$+constant.

6.4 Let $E_\tau\setminus\{0\}\to\mathbb{C}^2$ be the map given by $z\to(\wp(z),\wp(z)')$. Show that the images of the non-trivial 2-torsion points of E_τ are the points $(\alpha_i,0)$, where α_i are the zeroes of the polynomial $4x^3-g_2x-g_3$.

6.5 Show that

$$\det\begin{pmatrix}\wp(z_1) & \wp'(z_1) & 1\\ \wp(z_2) & \wp'(z_2) & 1\\ r\wp(z_3) & \wp'(z_3) & 1\end{pmatrix} = 0$$

whenever $z_1+z_2+z_3=0$. Deduce from this an explicit formula for the group law on the projective cubic curve $y^2t = 4x^3 - g_2xt^2 - g_3t^3$.

6.6 (*Weierstrass ζ-function*) It is defined by

$$Z(z;\Lambda) = \frac{1}{z} + \sum_{\omega\in\Lambda\setminus\{0\}}\Big(\frac{1}{-\omega}+\frac{1}{\omega}+\frac{z}{\omega^2}\Big).$$

Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Show that

(i) $Z'(z) = -\wp(z)$;

(ii) $Z(z+\omega_i) = Z(z)+\eta_i, i = 1,2$ where $\eta_i = Z(\omega_i/2)$;

(iii) $\eta_1\omega_2 - \eta_2\omega_1 = 2\pi i$;

(iv) $Z(\lambda z;\lambda\cdot\Lambda) = \lambda^{-1}Z(z;\cdot\Lambda)$, where λ is any nonzero complex number.

6.7 Let $\phi(z)$ be a holomorphic function satisfying

$$\phi(z)'/\phi(z) = Z(z),$$

(i) Show that $\phi(-z) = -\phi(z)$;

(ii) $\phi(z+\omega_i) = -e^{\eta_i(z+\frac{\omega_i}{2}}\phi(z)$;

(iii) $\phi(z) = \sigma(z)$, where $\sigma(z)$ is the Weierstrass σ-function.

6.8 Using the previous exercise show that the Weierstrass σ-function $\sigma(z)$ admits an in finite product expansion of the form

$$\sigma(z) = z\prod_{\omega\in\Lambda\setminus\{0\}}(1-\frac{z}{\omega})e^{\frac{z}{\omega}+\frac{1}{2}(\frac{z}{\omega})^2}$$

which converges absolutely, and uniformly in each disc $|z|\le R$.

6.9 Let E_τ be an elliptic curve and $y^2 = 4x^3 - g_2x - g_3$ be its Weierstrass equation. Show that any automorphism of E_τ is obtained by a linear transformation of the variables (x,y) which transforms the Weierstrass equation to the form $y^2 = 4x^3 - c^4g_2x - c^6g_3$ for some $c\neq 0$. Show that E_τ is harmonic (resp. anharmonic) if and only if $g_3 = 0$ (resp. $g_2 = 0$).

6.10 Let k be an even integer and let $L\subset\mathbb{R}^k$ be a lattice with a basis $(e_1,\ldots,e_k)$. Assume that $||v||^2$ is even for any $v\in L$. Let D be the determinant of the matrix $(e_i\cdot e_j)$ and N be the smallest positive integer such that $N||v^*||^2\in 2\mathbb{Z}$ for all $v^*\in\mathbb{R}^k$ satisfying $v^*\cdot w\in\mathbb{Z}$ for all $w\in L$. Define the *theta series of the lattice* L by

$$\theta_L(\tau) = \sum_{n=0}^{\infty}\#\{v\in L: ||v||^2 = 2n\}e^{2\pi in\tau}.$$

(i) Show that $\theta_L(\tau) = \sum_{v\in L}e^{\pi i\tau||v||^2}$;

(ii) Show that the functions $\Theta(0,\tau)^k$ discussed in the beginning of Lecture 6 are special cases of the function θ_L.

(iii) Show that $\theta_L(\tau)$ is "almost" modular form for the group

$$\Gamma_0(N) = \{\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : N|c\},$$

i.e.

$$\theta_L(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^{k/2}\chi(d)\theta_L(\tau), \quad \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \Gamma_0(N),$$

where $\chi(d) = (\frac{(-1)^{\frac{k}{2}}D}{d})$ is the quadratic residue symbol.

(iv) Prove that $\theta_L(\tau)$ is a modular form for $\Gamma_0(2)$ whenever $D = 1$ and $k \equiv 0 \bmod 4$.

6.11 Let $\Phi(z;\tau)$ be a function in z and τ satisfying the assumptions of Theorem 6.2 (such a function is called a *Jacobi form* of weight m and index 0 with respect to the group Γ). Show that

(i) $\wp(z;\tau)$ is a Jacobi form of weight 2 and index 0 with respect to $\Gamma(1)$;

(ii) $\sigma(z;1,\tau)$ is a Jacobi form of weight 1 with respect to $\Gamma(1)$.

6.12 Let n be a positive integer greater than 2. Consider the map of a complex torus $E_\tau \setminus \{0\} \to \mathbb{C}^n$ given by the formula

$$z \to (1, \wp(z), \ldots, \wp(z)^{\frac{n-1}{2}}, \wp(z)', \wp(z)\wp(z)', \ldots, \wp(z)^{\frac{n-3}{2}}\wp(z)')$$

if n is odd and

$$z \to (1, \wp(z), \ldots, \wp(z)^{\frac{n}{2}}, \wp(z)', \wp(z)\wp(z)', \ldots, \wp(z)^{\frac{n-4}{2}}\wp(z)')$$

if n is even. Show this map extends uniquely to a holomorphic map $f_n : E_\tau \to \mathbb{P}^n$. Show that f_n is an isomorphism onto its image (a *normal elliptic curve* of degree n). Find the image for $n = 4$.

6.13 Let $q = e^{2\pi i\tau}, v = e^{2\pi iz}$.

(i) Show that the function

$$X = \sum_{r\in\mathbb{Z}} \frac{1}{(q^{r/2}v^{\frac{1}{2}} - q^{-r/2}v^{-\frac{1}{2}})^2} - \frac{1}{12} + \sum_{r\in\mathbb{Z}, r\neq 0} \frac{1}{(q^{r/2} - q^{-r/2})^2}$$

coincides with $\wp(z)$.

(ii) Using (i) show that $\wp(z;\tau)$ considered as a function of τ has the following Fourier expansion

$$\frac{1}{(2\pi i)^2}\wp(z;\tau) = \frac{1}{(v^{\frac{1}{2}} - v^{-\frac{1}{2}})^2} + \sum_{n=1}^{\infty}(\sum_{d|n} d(v^d + v^{-d}))q^n +$$

$$\frac{1}{12}(1 - 24\sum \sigma_1(n)q^n).$$

Lecture 7

The Algebra of Modular Forms

7.1 Let Γ be a subgroup of finite index of $\Gamma(1)$. We set

$$\mathcal{M}_k(\Gamma) = \{\text{modular forms of weight } k \text{ with respect to } \Gamma\},$$

We also denote by $\mathcal{M}_k(\Gamma)^0$ the subspace of cuspidal modular forms. It is clear that $\mathcal{M}_k(\Gamma)$ is a vector space over $\mathbb{C}$. Also multiplication of functions defines a bilinear map

$$\mathcal{M}_k(\Gamma) \times \mathcal{M}_l(\Gamma) \to \mathcal{M}_{k+l}(\Gamma).$$

This allows us to consider the direct space

$$\mathcal{M}(\Gamma) = \bigoplus_{k=-\infty}^{\infty} \mathcal{M}_k(\Gamma) \tag{7.1}$$

as a graded commutative algebra over $\mathbb{C}$. Since $\mathcal{M}_k(\Gamma) \cap \mathcal{M}_l(\Gamma) = \{0\}$ if $k \neq l$, we may view $\mathcal{M}(\Gamma)$ as a graded subalgebra of $\mathcal{O}(\mathcal{H})$.

Notice that

$$\mathcal{M}(\Gamma)^0 = \bigoplus_{k=-\infty}^{\infty} \mathcal{M}_k(\Gamma)^0 \tag{7.2}$$

is an ideal in $\mathcal{M}(\Gamma)$.

We shall see later that there are no modular forms of negative weight.

7.2 Our next goal is to prove that the algebra $\mathcal{M}(\Gamma)$ is finitely generated. In particular each space $\mathcal{M}_k(\Gamma)$ is finite-dimensional.

Let $f(z)$ be a meromorphic function in a neighborhood of a point $a \in \mathbb{C}$ and let

$$f(z) = \sum_{n=m}^{\infty} c_n (z-a)^n$$

be its Laurent expansion in a neighborhood of the point a. We assume that $c_m \neq 0$ and set $\nu_a(f) = m$. We shall call the number $\nu_a(f)$ the *order* (of zero if $m \geq 0$ or of pole if $m < 0$) of f at a. If f is meromorphic at ∞ we set

$$\nu_\infty(f) = \nu_0(f(1/z)).$$

Note that when f is a modular form with respect to a group Γ we have

$$\nu_{g\cdot\tau}(f) = \nu_\tau(f), \quad \forall g \in \Gamma.$$

For each $\tau \in \mathcal{H}$ let

$$m_\tau = \begin{cases} 2 & \text{if } \tau \in \Gamma(1)\cdot i, \\ 3 & \text{if } \tau \in \Gamma(1)\cdot e^{2\pi i/3}, \\ 1 & \text{otherwise.} \end{cases} \tag{7.3}$$

Lemma 7.1. *Let $f(\tau)$ be a modular form of weight k with respect to the full modular group $\Gamma(1)$. Then*

$$\sum_{\tau\in\mathcal{H}/\Gamma(1)} \frac{\nu_\tau(f)}{m_\tau} = \frac{k}{6}.$$

Proof. Consider the subset P of the modular figure $\mathcal{D}$ obtained as follows. First delete the part of $\mathcal{D}$ defined by the condition Im $\tau > h$ for sufficiently large h such that f has no zeroes or poles for Im $\tau \geq h$. Let $C_r(\rho), C_r(\rho^2), C_r(i)$ be a small circle of radius r centered at $\rho = e^{\pi i/3}$ at ρ^2 and at i, respectively. Delete from $\mathcal{D}$ the intersection with each of these circles. Finally if $f(z)$ has a zero or pole a at the boundary of $\mathcal{D}$ we delete from $\mathcal{D}$ its intersection with a small circle of radius r with center at a.

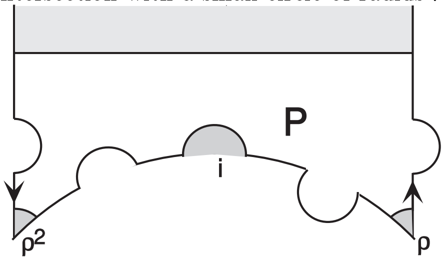

Fig.1

Applying the Cauchy Residue Theorem we obtain

$$\frac{1}{2\pi i}\int_{\partial P} \frac{f'd\tau}{f} = \sum_{\tau\in P} \nu_\tau(f) = \sum_{\tau\in P} \frac{\nu_\tau(f)}{m_\tau}.$$

When we integrate over the part ∂P_1 of the boundary defined by Im $\tau = h$ we obtain

$$\frac{1}{2\pi i}\int_{\partial P_1} \frac{f'dz}{f} = -\nu_\infty(f).$$

In fact, considering the Fourier expansions of f at ∞, we get

$$f(\tau) = \sum_{n=\nu_\infty(f)}^{\infty} a_n e^{2\pi i n\tau},$$

$$f(\tau)' = \sum_{n=\nu_\infty(f)}^{\infty} (2\pi i n) a_n e^{2\pi n i \tau}.$$

Use the function $q = e^{2\pi i \tau}$ to map the segment $\{\tau : |\text{Re } \tau| \leq \frac{1}{2}, \text{Im } \tau = h\}$ onto the circle $C : |q| = e^{-2\pi h}$. When we move along the segment from the point $\frac{1}{2} + ih$ to the point $-\frac{1}{2} + ih$ the image point moves along the circle in the clockwise way. We have

$$\frac{1}{2\pi i} \int_{\partial P_1} \frac{f' d\tau}{f} = -\frac{1}{2\pi i} \int_C \frac{(2\pi i \nu_\infty(f) q^{\nu_\infty(f)} + \dots) dq}{2\pi i q (a_{\nu_\infty(f)} q^{\nu_\infty(f)} + \dots)} = -\nu_\infty(f).$$

If we integrate along the part ∂P_2 of the boundary of P which lies on the circle $C_r(\rho^2)$ we get

$$\lim_{r\to 0} \frac{1}{2\pi i} \int_{\partial P_2} \frac{f' d\tau}{f} = -\frac{1}{6} \nu_{\rho^2}(f).$$

This is because the arc ∂P_2 approaches to the one-sixth of the full circle when its radius goes to zero. Also we take into account that the direction of the path is clockwise. Similarly, if we let $\partial P_3 = \partial P \cap C_r(i), \partial P_4 = \partial P \cap C_r(\rho)$, we find

$$\lim_{r\to 0} \frac{1}{2\pi i} \int_{\partial P_3} \frac{f' d\tau}{f} = -\frac{1}{2} \nu_i(f).$$

$$\lim_{r\to 0} \frac{1}{2\pi i} \int_{\partial P_4} \frac{f' d\tau}{f} = -\frac{1}{6} \nu_\rho(f).$$

Now the transformation $T : \tau \to \tau + 1$ transforms the path along ∂P from $-\frac{1}{2} + ih$ to ρ^2 to the path along the boundary from the point ρ to the point $\frac{1}{2} + ih$. Since our function satisfies $f(\tau + 1) = f(\tau)$ and we are moving in the opposite direction along these paths, the two contributions to the total integral cancel out. Finally, if we consider the remaining part of the boundary, and use the transformation $S : \tau \to -\frac{1}{\tau}$ we obtain

$$\frac{df(\frac{-1}{\tau})}{f(\frac{-1}{\tau})} = \frac{d(\tau^{2k} f(\tau)}{f(\tau))} = 2k\frac{d\tau}{\tau} + \frac{df}{f},$$

When we move from ρ^2 to i the point $S \cdot \tau$ moves from ρ to i. This easily gives us that the portion of the integral over the remaining part of the boundary is equal to (when r goes to zero)

$$\frac{1}{2\pi i} \int_\gamma \frac{-2k d\tau}{\tau} = -2k(-\frac{1}{12}) = \frac{k}{6},$$

where γ is the part of the circle $\tau = 1$ starting at ρ^2 and ending at i. Collecting everything together we obtain the assertion of the lemma. $\square$

Theorem 7.1. *$\mathcal{M}_k(\Gamma(1)) = \{0\}$ if $k < 0$. If $k \geq 0$, we have*

$$\dim \mathcal{M}_k(\Gamma(1)) = \begin{cases} [k/6] & \text{if } k \equiv 1 \ mod \ (6) \\ [k/6] + 1 & \text{otherwise.} \end{cases}$$

Proof. Let $f(\tau) \in \mathcal{M}_k(\Gamma(1))$. Then $\nu_\tau \geq 0$ for all $\tau \in \mathcal{H}$, and Lemma 7.1 implies that $\frac{k}{6} = A + \frac{B}{2} + \frac{C}{3}$ for some non-negative integers A, B, C. Clearly this implies that $\dim \mathcal{M}_k(\Gamma(1)) = \{0\}$ when $k < 0$ or $k = 1$. If $k = 2$ we must have $A = B = 0, C = 1$. Since $f \in \mathcal{M}_2(\Gamma(1))$ we have

$$\nu_\rho(f) = \nu_{\rho^2}(f) = 1.$$

In particular, this is true for g_2. For any other $f \in \mathcal{M}_2(\Gamma(1))$ we have f/g_2 is $\Gamma(1)$ invariant and also holomorphic at ∞ (since g_2 is not a cusp form). This shows that f/g_2 is constant and

$$\mathcal{M}_2(\Gamma(1)) = \mathbb{C}g_2.$$

Similar arguments show that

$$\mathcal{M}_3(\Gamma(1)) = \mathbb{C}g_3,$$

$$\mathcal{M}_4(\Gamma(1)) = \mathbb{C}g_2^2,$$

$$\mathcal{M}_5(\Gamma(1)) = \mathbb{C}g_2g_3.$$

This checks the assertion for $k < 6$. Now for any cuspidal form $f \in \mathcal{M}_k(\Gamma(1))$ with $k > 6$ we have f/Δ is a modular form of weight $k - 6$ (because Δ does not vanish on $\mathcal{H}$ and has a simple zero at infinity). This shows that for $k > 6$

$$\mathcal{M}_k(\Gamma(1))^0 = \Delta\mathcal{M}_{k-6}(\Gamma(1)). \tag{7.4}$$

Since $\mathcal{M}_k(\Gamma(1))/\mathcal{M}_k(\Gamma(1))^0 \cong \mathbb{C}$ (we have only one cusp) we obtain for $k > 6$

$$\dim \mathcal{M}_k(\Gamma(1)) = \dim \mathcal{M}_{k-6}(\Gamma(1)) + 1.$$

Now the assertion follows by induction on k. $\square$

Corollary 7.1. *The algebra $\mathcal{M}(\Gamma(1))$ is generated by the modular forms g_2 and g_3. The homomorphism of algebras $\phi : \mathbb{C}[T_1, T_2] \to \mathcal{M}(\Gamma(1))$ defined by sending T_1 to g_2 and T_2 to g_3 defines an isomorphism between $\mathcal{M}(\Gamma(1))$ and the algebra of complex polynomials in two variables.*

Proof. The first assertion is equivalent to the surjectivity of the homomorphism ϕ. Let us prove it. We have to show that any $f \in \mathcal{M}(\Gamma(1))$ can be written as a polynomial in g_2 and g_3. Without loss of generality we may assume that $f \in \mathcal{M}(\Gamma(1))_k$ for some $k \geq 0$. Write k in form $k = 2a + 3b$ for some nonnegative integers a and b. Since $g_2^a g_3^b$ does not vanish at infinity, we can find a constant c such that $f - cg_2^a g_3^b$ is a cuspidal form. By (7.4), it is equal to $g\Delta$ for some $g \in \mathcal{M}(\Gamma(1))_{k-6}$. Since Δ is a polynomial in g_2 and g_3, proceeding by induction on k we prove the first assertion. To prove the second assertion we use that any element $F(T_1, T_2)$ from the kernel of ϕ can be written uniquely as a sum of polynomials G_d satisfying

$$G_d(\tau^2 T_1, \tau^3 t_3) = \tau^d G_d(T_1, T_2)$$

for some $d > 0$ and any $\tau \in \mathcal{H}$. In fact, writing F as a sum of monomials in T_1, T_2 we define G_d as the sum of monomials $T_1^i T_2^j$ entering into F such that $2i + 3j = d$. Since

$$F(g_2(-1/\tau), g_3(-1/\tau)) = F(\tau^2 g_2, \tau^3 g_3) \equiv 0,$$

each G_d must belong to the kernel of ϕ. This allows us to assume that $F = G_d$ for some d. Dividing by T_2^d we obtain $G_d(g_2, g_3)/g_3^d = G(g_2^3/g_3^2) \equiv 0$ for some polynomial G in one variable $T = T_1/T_2$. Since $\mathbb{C}$ is algebraically closed, g_2^3/g_3^2 must be a constant. But this is impossible since g_3 vanishes only at $\Gamma \cdot i$ and g_2 vanishes only at $\Gamma(1) \cdot \rho$. □

Corollary 7.2. *The ideal of cuspidal modular forms $\mathcal{M}^0(\Gamma(1))$ is generated by Δ.*

Proof. We have seen already in (7.4) that $\mathcal{M}_k(\Gamma(1))^0 = \Delta\mathcal{M}_{k-6}(\Gamma(1))$. Also we have $\mathcal{M}_k(\Gamma(1))^0 = \{0\}$ for $k < 6$. This checks the assertion. □

7.3 Let us give some examples.

Example 7.1. We know that the Eisenstein series E_{2k} is a modular form of weight k with respect to $\Gamma(1)$. Since $\mathcal{M}_4(\Gamma(1)) = \mathbb{C}g_2^2 = \mathbb{C}E_4^2$, comparing the constant coefficients in the Fourier expansions we obtain

$$E_8 = \frac{\zeta(8)}{2\zeta(4)^2} E_4^2.$$

Comparing the other coefficients we get a lot of identities between the numbers $\sigma_k(n)$. For example, we have

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{0<m<n} \sigma_3(m)\sigma_3(n-m). \tag{7.5}$$

Similarly we have

$$E_{10} = \frac{\zeta(10)}{2\zeta(4)\zeta(6)} E_4 E_6.$$

This gives us more identities. By the way our old relation

$$(2\pi)^{12}\Delta = g_2^3 - 27g_3^2$$

gives the expression of the *Ramanujan function* $\tau(n)$ defined by

$$\Delta = q \prod_{m=1}^{\infty} (1 - q^m)^{24} = \sum_{n=0} \tau(n) q^n$$

in terms of the functions $\sigma_k(n)$:

$$\tau(n) = \frac{65}{756}\sigma_{11}(n) + \frac{691}{756}\sigma_5(n) - \frac{691}{3} \sum_{0<m<n} \sigma_5(m)\sigma_5(n-m). \tag{7.6}$$

We shall prove in Lecture 11 that $\tau(n)$ satisfies

$$\tau(nm) = \tau(n)\tau(m) \quad \text{if } (n, m) = 1,$$

$$\tau(p^{k+1}) = \tau(p)\tau(p^k) - p^{11}\tau(p^{k-1}) \quad \text{if } p \text{ is prime, } k \geq 0.$$

Example 7.2. Let L be a lattice in $\mathbb{R}^n$ of rank n such that for any $v \in L$ the Euclidean norm $||v||^2$ takes integer values. We say that L is an *integral lattice* in $\mathbb{R}^n$. If $(v_1, \dots, v_n)$ is a basis of Λ, then the dot products $a_{ij} = v_i \cdot v_j$ define an integral symmetric non-degenerate matrix, hence an integral quadratic form

$$Q = \sum_{i,j=1}^{n} a_{ij} x_i x_j .$$

Obviously for any $v = (a_1, \dots, a_n) \neq 0$ we have

$$Q(v) = ||v||^2 > 0.$$

In other words, Q is positive definite. Conversely given any positive definite integral quadratic form Q as above, we can find a basis $(e_1', \dots, e_n')$ such that Q diagonalizes, i.e. its matrix with respect to this basis is the identity matrix. Let $\phi : \mathbb{R}^n \to \mathbb{R}^n$ be the linear automorphism which sends the standard basis $(e_1, \dots, e_n)$ to the basis $(e_1', \dots, e_n')$. Then the pre-image of the standard lattice $\mathbb{Z}^n = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n$ is an integral lattice L with the distance function Q.

Let us define the *theta function of the lattice* L by setting

$$\theta_L(\tau) = \sum_{m=0}^{\infty} r_L(m) q^m = \sum_{v \in L} q^{Q(v)/2}, \tag{7.7}$$

where

$$r_L(m) = \#\{v \in L : Q(v) = 2m\}.$$

(see Exercise 6.10). Since $r_L(m) \leq (2m)^{n/2}$ (inscribe the cube around the sphere of radius $\sqrt{2m}$), and hence grows only polynomially, we easily see that $\theta_L(\tau)$ absolutely converges on any bounded subset of $\mathcal{H}$, and therefore defines a holomorphic form on $\mathcal{H}$.

We shall assume that L is *unimodular*, i.e. the determinant of the matrix (a_{ij}) is equal to 1. This definition does not depend on the choice of a basis in L and is equivalent to the property that L is equal to the set of vectors w in $\mathbb{R}^n$ such that $w \cdot v \in \mathbb{Z}$ for all $v \in L$. For example, if L is the standard lattice $\mathbb{Z}^n$ we see from Lecture 4 that

$$\theta_{\mathbb{Z}^n}(\tau) = \Theta(0, \tau)^n.$$

Repeating the argument from the beginning of Lecture 4 we obtain that, for any unimodular lattice L,

$$\theta_L(-1/\tau) = (-i\tau)^{n/2} \theta_L(\tau). \tag{7.8}$$

Also, if we additionally assume that L is even, i.e. $Q(v) \in 2\mathbb{Z}$ for any $v \in L$, we obviously get

$$\theta_L(\tau + 1) = \theta_L(\tau).$$

In particular, if $8|n$ we see that $\theta_L(\tau)$ is a modular form with respect to $\Gamma(1)$. It is amazing that one does not need to assume that n is divisible by 8. It is a fact! Let us prove it. Assume n is not divisible by 8. Replacing n by $2n$ (if n is even)(resp. $4n$ if n

is odd), and L by $L \oplus L$ (resp. by $L \oplus L \oplus L \oplus L$), we may assume that n is divisible by 4 but not by 8. By (7.8) we get

$$\theta_L(-1/\tau) = -\tau^{n/2}\theta_L(\tau).$$

Since θ_L is always periodic with respect to 1, this implies

$$\theta_L|_{\frac{n}{2}}ST = -\theta_L|_{\frac{n}{2}}T = -\theta_L.$$

Obviously this contradicts the fact that $(ST)^3 = 1$. Now we know that for any even unimodular lattice

$$\theta_L \in \mathcal{M}_{n/4}(\Gamma(1)). \tag{7.9}$$

Now let $n = 8$. Since $\mathcal{M}_2(\Gamma(1)) = \mathbb{C}E_4$ we see that θ_L is proportional to the Eisenstein series E_4. Comparing the constant coefficients we see that

$$\theta_L = E_4/2\zeta(4).$$

In particular, for any $m \geq 1$,

$$r_L(m) = 240\sigma_3(m). \tag{7.10}$$

In fact there exists only one even unimodular lattice in $\mathbb{R}^8$ (up to equivalence of lattices). The lattice is the famous E_8 lattice, the root lattice of simple Lie algebra of type E_8.

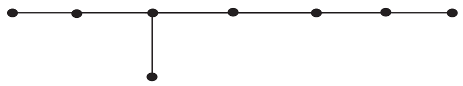

Fig.2

Here the diagram describes a symmetric matrix as follows. All the diagonal elements are equal to 2. If we order the vertices, then the entry a_{ij} is equal to -1 or 0 dependent on whether the i-th vertex is connected to the j-th vertex or not, respectively.

Take $n = 16$. Since $\mathcal{M}_4(\Gamma(1)) = \mathbb{C}E_8$, we obtain, by comparing the constant coefficients,

$$\theta_L = E_8/2\zeta(8).$$

In particular, we have

$$r_L(m) = 16\sigma_7(m)/B_4, \tag{7.11}$$

where B_4 is the fourth Bernoulli number (see Lecture 6). There exist two even unimodular lattices in $\mathbb{R}^{16}$. One is $E_8 \oplus E_8$. Another is Γ_{16} defined by the following graph:

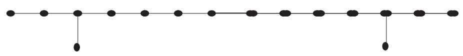

Fig.3

Now let $n = 24$. The space $\mathcal{M}_6(\Gamma(1))$ is spanned by Δ and E_{12}. We can write

$$\theta_L = \frac{1}{2\zeta(12)}E_{12} + c_L\Delta.$$

This gives

$$r_L(m) = \frac{65520}{691}\sigma_{11}(m) + c_L\tau(m), \tag{7.12}$$

where $\tau(m)$ is the Ramanujan function (the coefficient at q^m in Δ). Setting $m = 1$, we get

$$c_L = r_L(1) - \frac{65520}{691}. \tag{7.13}$$

Clearly, $c_L \neq 0$.

Except obvious examples $E_8 \oplus E_8 \oplus E_8$ or $E_8 \oplus \Gamma_{16}$ there are 22 more even unimodular lattices of rank 24. One of them is the *Leech lattice* Λ. It differs from any other lattice by the property that $r_\Lambda(1) = 0$. So,

$$r_L(m) = \frac{65520}{691}(\sigma_{11}(m) - \tau(m)), \tag{7.14}$$

In particular, we see that

$$\tau(m) \equiv \sigma_{11}(m) \mod 691.$$

This is one of the numerous congruences satisfied by the Ramanujan function $\tau(m)$.

7.4 Our goal is to prove an analog of Theorem 7.1 for any subgroup of finite index Γ of $\Gamma(1)$. Let $\Gamma' \subset \Gamma$ be two such subgroups. Assume also that Γ' is normal in Γ and let $G = \Gamma/\Gamma'$ be the quotient group. The group G acts on $\mathcal{M}_k(\Gamma')$ as follows. Take a representative g of $\bar{g} \in G$. Then set, for any $f \in \mathcal{M}_k(\Gamma')$,

$$\bar{g} \cdot f = f|_k g.$$

Since $f|_k g' = f$ for any $g' \in \Gamma'$ this definition does not depend on the choice of a representative.

The following lemma follows from the definition of elements of $\mathcal{M}_k(\Gamma)$.

Lemma 7.2. *Let Γ' be a normal subgroup of Γ and $G = \Gamma/\Gamma'$. Then*

$$\mathcal{M}_k(\Gamma) = \mathcal{M}_k(\Gamma')^G = \{f \in \mathcal{M}_k(\Gamma') : g \cdot f = f, \forall g \in G\}.$$

It follows from this lemma that the algebra $\mathcal{M}(\Gamma)$ is equal to the subalgebra of $\mathcal{M}(\Gamma')$ which consists of elements invariant with respect to the action of the group Γ/Γ'. Let n be the order of the group $G = \Gamma/\Gamma'$ (recall that we consider only subgroups of finite index of $\Gamma(1)$). For any $f \in \mathcal{M}(\Gamma')$ we have

$$\prod_{g \in G}(f - (g \cdot f)) = 0$$

since the factor of this product corresponding to 1 is equal to zero. We have

$$f^n + h_1 f^{n-1} + \ldots + h_n = 0, \tag{7.15}$$

where h_i are symmetric polynomials in $g \cdot f, g \in G$. Clearly they are invariant with respect to G and hence, by Lemma 7.2, represent elements of $\mathcal{M}(\Gamma)$. In particular we see that for any normal subgroup Γ of $\Gamma(1)$

$$\mathcal{M}_k(\Gamma) = \{0\}, \quad k < 0.$$

In fact, any modular form of negative weight k will satisfy an equation (7.6) where we may assume that each coefficient h_i is a modular form of weight ik with respect to $\Gamma(1)$. However no such modular forms exist except zero. If Γ is not normal we choose a normal subgroup of finite index Γ' of Γ and apply Lemma 7.2.

Lemma 7.3. *Let B be any commutative algebra over a field F without zero divisors and A be a Noetherian subalgebra of B. Assume that each element $b \in B$ satisfies a monic equation with coefficients in A:*

$$b^n + a_1 b^{n-1} + \ldots + a_n = 0$$

(we say in this case that that B is integral *over A). Also assume that the field of fractions of B is a finite extension of the field of fractions of A. Then B is finitely generated F-algebra if and only if A is finitely generated F-algebra.*

Proof. This fact can be found in any text-book in commutative algebra and its proof will be omitted. □

Theorem 7.2. *For any subgroup Γ of finite index of $\Gamma(1)$ the algebra $\mathcal{M}(\Gamma)$ is a finitely generated algebra over $\mathbb{C}$.*

Proof. Let Γ' be a normal subgroup of finite index in $\Gamma(1)$ which is contained in Γ. It always can be found by taking the intersection of conjugate subgroups $g^{-1} \cdot \Gamma \cdot g, g \in \Gamma(1)$. We first apply Lemma 7.3 to the case when $B = \mathcal{M}(\Gamma'), A = \mathcal{M}(\Gamma(1))$. Since $A \cong \mathbb{C}[T_1, T_2]$ is finitely generated, B is finitely generated. It follows easily from (7.15) that the field of fractions of B is a finite extension of the field of fractions of A of degree equal to the order of the group Γ/Γ'. Next we apply the same lemma to the case when $B = \mathcal{M}(\Gamma'), A = \mathcal{M}(\Gamma)$. Then B is finitely generated, hence A is finitely generated. □

Corollary 7.3. *The linear spaces $\mathcal{M}_k(\Gamma)$ are finite-dimensional.*

Proof. Let $f_1, \ldots, f_k$ be a set of generators of the algebra $\mathcal{M}_k(\Gamma)$. Writing each f_i as a linear combination of modular forms of different weights, and then adding to the set of generators all the summands, we may assume that $\mathcal{M}_k(\Gamma)$ is generated by finitely many modular forms $f_i \in \mathcal{M}_{k_i}(\Gamma), i = 1, \ldots, n$. Now $\mathcal{M}_k(\Gamma)$ is spanned as a vector space over $\mathbb{C}$ by the monomials $f_1^{i_1} \ldots f_n^{i_n}$ where $k_1 i_1 + \ldots + i_n k_n = k$. The number of such monomials is finite. It is equal to the coefficient at t^k of the Taylor expansion of the rational function

$$\prod_{i=1}^{n} \frac{1}{(1 - t^{k_i})}.$$

□

In the next lecture we shall give an explicit formula for the dimension of the spaces $\mathcal{M}_k(\Gamma)$.

Exercises

7.1 Find a fundamental domain for the principal congruence subgroup $\Gamma(2)$ of level 2.

7.2 Using Exercise 7.1 find and prove an analog of Lemma 7.1 for the case $\Gamma = \Gamma(2)$.

7.3 Let $n = 8k$. Consider the subgroup Γ_n of $\mathbb{R}^n$ generated by vectors $v = (a_1, \dots, a_n)$ with $a_i \in \mathbb{Z}$ and $a_1 + \dots + a_n \in 2\mathbb{Z}$ and the vector $(\frac{1}{2}, \dots, \frac{1}{2})$.

(i) Show that Γ_n is an even unimodular lattice in $\mathbb{R}^n$.

(ii) Show that Γ_8 is isomorphic to the lattice E_8 defined in the lecture.

(iii) Show that Γ_{16} can be defined by the graph from Fig.3

(iv) Show that Γ_{16} is not isomorphic to $\Gamma_8 \oplus \Gamma_8$.

(v) Compute the number of points $(x_1, \dots, x_8) \in \mathbb{R}^8$ such that $2x_i \in 2\mathbb{Z}, x_i - x_j \in \mathbb{Z}, x_1 + \dots + x_8 \in \mathbb{Z}, x_1^2 + \dots + x_8^2 = 2N$, where $N = 1, 2$.

7.4 Let $L \subset \mathbb{R}^n$ be an integral lattice not necessary unimodular. Using the Poisson formula from Lecture 4 show that

$$\theta_L(-\frac{1}{\tau}) = (\frac{\tau}{i})^{n/2}\frac{1}{D_L^{1/2}}\theta_{L^*}(\tau),$$

where L^* is the *dual lattice* defined by $L^* = \{v \in \mathbb{R}^n : v \cdot x \in \mathbb{Z} \text{ for all } x \in L\}$ and D_L is the *discriminant* of L defined by $D_L = \#L^*/L$.

7.5 Let C be a linear subspace of $\mathbb{F}_2^n$ (a *linear binary code*). Let $L_C = \frac{1}{\sqrt{2}}r^{-1}(C)$, where r is the natural homomorphism $\mathbb{Z}^n \to \mathbb{F}_2^n$.

(i) Show that L_C is an integral lattice if and only if for any $x = (\epsilon_1, \dots, \epsilon_n) \in C$ the number $\mathrm{wt}(x) = \#\{i : \epsilon_i \neq 0\}$ (called the *weight* of x) is divisible by 4. In this case we say that C is a *doubly even* linear code.

(ii) Show that the discriminant of the lattice L_C is equal to 2^{n-2k}, where $k = \dim C$.

(iii) Let $C^\perp = \{y \in \mathbb{F}_2^n : x \cdot y = 0, \forall x \in C\}$. Show that L_C is integral if and only if $C \subset C^\perp$.

(iv) Assume C is doubly even. Show that $L_{C^\perp} = L_C^*$. In particular, L_C is a unimodular even lattice if and only if $C = C^\perp$ (in this case C is called a *self-dual code*).

(v) Let $C \subset \mathbb{F}_2^n$ be a self-dual doubly even code. Show that n must be divisible by 8.

7.6 Let $A(\tau) = \vartheta(0;\tau), B(\tau) = \vartheta_{\frac{1}{2}0}(0;\tau)$.

(i) Show that

$$(A(-1/\tau), B(-1/\tau)) = (\frac{\tau}{i})^{1/2}(A(\tau), B(\tau)) \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}.$$

(ii) Show that the expression $A^4B^4(A^4 - B^4)^4$ is a modular form of weight 6 with respect to $\Gamma(1)$.

(iii) Show that $A^4B^4(A^4 - B^4)^4 = 16\Delta(\tau)$.

(iv) Show that $A^8 + 14A^4B^4 + B^8 = \frac{1}{2\zeta(4)}E_4(\tau)$.

7.7 Let $C \subset \mathbb{F}_2^n$ be a linear code. Define its *weight enumerator polynomial* by

$$W_C(X,Y) = \sum_{x \in C} X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)} = \sum_{i=0}^{n} A_i X^{n-i} Y^i,$$

where A_i is the number of $x \in C$ with $\mathrm{wt}(x) = i$.

(i) Show that

$$\theta_{L_C} = W_C(A,B).$$

(ii) Prove *MacWilliams's Identity*:

$$W_{C^\perp}(X,Y) = \frac{1}{2^{\dim C}} W_C(X+Y, X-Y).$$

(iii) Using Theorem 7.1 show that for any self-dual doubly even code the enumerator polynomial $W_C(X,Y)$ can be written as a polynomial in $X' = X^8 + 14X^4Y^4 + Y^8$ and $Y' = X^4Y^4(X^4 - Y^4)^4$ (*Gleason' Theorem*). where A, B are defined in the previous problem.

(iv) Deduce from (iii) that the enumerator polynomial $W_C(X,Y)$ of any doubly even self-dual linear code is a symmetric polynomial in X, Y (i.e. $W_C(X,Y) = W_C(Y,X)$). Give it an independent proof using only the definition of $W_C(X,Y)$.

7.8 Let C be a self-dual doubly even linear code in $\mathbb{F}_2^{24}$ and $\theta_{L_C}(\tau) = \sum r_{L_C}(m) q^m$ be the theta function of the even unimodular lattice L_C associated to it and $W_C(X,Y) = \sum A_i X^i Y^{24-i}$ be its weight enumerator polynomial.

(i) Show that

$$r_{L_C}(2) = 48 + 16A_4, \quad r_{L_C}(4) = 2^8 A_8 + 640 A_4 + 1104.$$

(ii) Using (7.13) show that $A_8 = 759 - 4A_4$.

7.9 Let $A = \oplus_{n=-\infty}^{\infty} A_n$ be a commutative graded algebra over a field F. Assume A has no zero divisors, $A_0 = F \cdot 1$ and $\dim A_N > 1$ for some $nN > 0$. Show that $A_n = 0$ for $n < 0$. Apply this to give another proof that $\mathcal{M}_k(\Gamma) = 0$ for $k < 0$.

7.10 Find an explicit linear relation between the modular forms E_{16}, E_8^2 and $E_4 E_{10}$, where E_{2k} denotes the Eisenstein series. Translate this relation into a relation between the values of the functions $\sigma_d(m)$.

7.11 Let $f(\tau)$ be a parabolic modular form of weight k with respect to $\Gamma(1)$.

(i) Show that the function $\phi(\tau) = |f(\tau)|(\mathrm{Im}\ \tau)^k$ is invariant with respect to $\Gamma(1)$.

(ii) Show that $\phi(\tau)$ is bounded on $\mathcal{H}$ (it is not true if f is not cuspidal).

(iii) Show that the coefficient a_n in the Fourier expansion $f(\tau) = \sum a_n q^n$ can be computed as the integral

$$a_n = \int_0^1 f(x+iy) e^{-2\pi i n(x+iy)} dx.$$

(iv) Using (iii) prove that $|a_n| = O(n^k)$ (Hecke's Theorem).

7.12 Let L be an even unimodular lattice in $\mathbb{R}^{8k}$ and $r_L(m)$ be defined as in Example 7.2. Using the previous exercise show that

$$r_L(m) = \frac{8k}{B_{2k}}\sigma_{4k-1}(m) + O(m^{2k}).$$

7.13 Let $L = E_8 \oplus E_8 \oplus E_8$. Show that

$$\theta_L = \frac{1}{\zeta(12)}E_{12} + \frac{432000}{691}\Delta.$$

Lecture 8

The Modular Curve

8.1 In this lecture we shall give an explicit formula for the dimension of the spaces $\mathrm{M}_k(\Gamma)$, where Γ is any subgroup of finite index in $\mathrm{SL}(2,\mathbb{Z})$. For this we have to apply some techinique from algebraic geometry. We shall start with equipping $\mathcal{H}^*/\Gamma$ with a structure of a compact Riemann surface.

Let Γ be a subgroup of $\mathrm{SL}(2,\mathbb{R})$. We say that Γ is a *discrete subgroup* if the usual topology in $\mathrm{SL}(2,\mathbb{R})$ (considered as a subset of $\mathbb{R}^4$) induces a discrete topology in Γ. The latter means that any point of Γ is an open subset in the induced topology. Obviously $\mathrm{SL}(2,\mathbb{Z})$ is a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$. We shall consider the natural action of $\mathrm{SL}(2,\mathbb{R})$ on the upper half-plane $\mathcal{H}$ by Moebius transformations.

Lemma 8.1. *Any discrete subgroup Γ of $\mathrm{SL}(2,\mathbb{R})$ acts on $\mathcal{H}$ properly discontinuously.*

Proof. Observe that the group $\mathrm{SL}(2,\mathbb{R})$ acts transitively on $\mathcal{H}$ (view the latter as a subset of $\mathbb{R}^2$ of vectors with positive second coordinate). For any point $z \in \mathcal{H}$ the stabilizer group is conjugate to the stabilizer of say $z = i$. The latter consists of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{R})$ such that $a = d, b = -c$. It follows that this group is diffeomorphic to the circle $\{(a,b) \in \mathbb{R}^2 : a^2 + b^2 = 1\}$. This shows that the map $f : \mathrm{SL}(2,\mathbb{R}) \to \mathcal{H}$ defined by $f(g) = g \cdot i$ is diffeomorphic to a circle fibration over $\mathcal{H}$. This easily implies that pre-image of a compact set is compact. Let A, B be two compact subsets in $\mathcal{H}$. We have to check that $X = \{g \in \Gamma : g(A) \cap B \neq \emptyset\}$ is finite. Clearly, $g(A) \cap B \neq \emptyset$ if and only if $gg' = g''$ for some $g' \in f^{-1}(A), g'' \in f^{-1}(B)$. Since $A' = f^{-1}(A)$ and $B' = f^{-1}(B)$ are compact subsets of the group $\mathrm{SL}(2,\mathbb{R})$ the set $B' \cdot A'^{-1}$ is also compact. In fact, this set is the image of the compact subset $B' \times A'$ of $\mathrm{SL}(2,\mathbb{R}) \times \mathrm{SL}(2,\mathbb{R})$ under the continuous map $(g', g'') \to g'g''^{-1}$. Thus X is equal to the intersection of the discrete subset Γ with a compact subset of $\mathrm{SL}(2,\mathbb{R})$, hence it is a finite set. $\square$

Applying the previous Lemma and Theorem 2.2 we obtain that $\mathcal{H}/\Gamma$ has a structure of a Riemann surface and the canonical map

$$\pi_\Gamma : \mathcal{H} \to \mathcal{H}/\Gamma \tag{8.1}$$

is a holomorphic map.

Example 8.1. Let $\Gamma = \Gamma(1)$. Let us show that there exists a holomorphic isomorphism

$$\mathcal{H}/\mathrm{SL}(2,\mathbb{Z}) \cong \mathbb{C}.$$

This shows that the set of isomorphism classes of elliptic curves has a natural structure of a complex manifold of dimension 1 isomorphic to the complex plane $\mathbb{C}$. Since g_2^3 and Δ are of the same weight, the map

$$\mathcal{H} \to \mathbb{P}^1(\mathbb{C}), \quad \tau \to (g_2(\tau)^3, \Delta(\tau))$$

is a well defined holomorphic map. Obviously it is constant on any orbit of $\Gamma(1)$, hence factors through a holomorphic map

$$f : \mathcal{H}/\Gamma(1) \to \mathbb{P}^1(\mathbb{C}).$$

Since Δ does not vanish on $\mathcal{H}$, its image is contained in $\mathbb{P}^1(\mathbb{C}) \setminus \{\infty\} = \mathbb{C}$. I claim that f is one-to-one onto $\mathbb{C}$. In fact, for any complex number c the modular form $f = g_2^3 - c\Delta$ is of weight 6. It follows from Lemma 7.1 that f has either one simple zero, or one zero of multiplicity 2 at the elliptic point of order 2, or a triple zero at the elliptic point of index 3. This shows that each $c \in \mathbb{Z}$ occurs in the image of j on $\mathcal{H}/\Gamma$ and only once.

We leave to the reader the simple check that a bijective map between two complex manifolds of dimension 1 is an isomorphism.

Notice that the explicit isomorphism $\mathcal{H}/\mathrm{SL}(2,\mathbb{Z}) \to \mathbb{C}$ is given by the holomorphic function $\tau \to g_2^3/(g_2^3 - 27g_3^2)$. The function

$$j(\tau) = \frac{1728 g_2^3}{g_2^3 - 27g_3^2} = \frac{1728(2\pi)^{12} g_2^3}{\Delta} \tag{8.2}$$

is called the *absolute invariant*. The constant factor $1728 = 12^3$ is inserted here to normalize the coefficient at q^{-1} for the Fourier expansion of j at ∞:

$$j(\tau) = q^{-1} + 744 + \sum_{n=1}^{\infty} c_n q^n, \quad q = e^{2\pi i \tau}. \tag{8.3}$$

We have proved that

$$E_\tau \cong E_{\tau'} \iff j(\tau) = j(\tau'). \tag{8.4}$$

The coefficients c_n in (8.3) have been computed for $n \leq 100$. The first three are

$$c_1 = 196884, \quad c_2 = 21493760, \quad c_3 = 864299970.$$

They are all positive and equal to the dimensions of linear representations of the Griess-Fisher finite simple group (also called the *Monster group*).

8.2 The Riemann surface $\mathcal{H}/\Gamma$ is not compact. To compactify it we shall define a complex structure on

$$\mathcal{H}^*/\Gamma = H/\Gamma \cup \{\text{cusps}\}. \tag{8.5}$$

First we make $\mathcal{H}^*$ a topological space. We define a basis of open neighborhoods of ∞ as the set of open sets of the form

$$U_c = \{\tau \in \mathcal{H} : \mathrm{Im}\ \tau > c\} \cup \{\infty\}, \tag{8.6}$$

where c is a positive real number. Since $\mathrm{SL}(2,\mathbb{Z})$ acts transitively on $\mathcal{H}^* \setminus \mathcal{H}$ we can take for a basis of open neighborhoods of each $x \in \mathbb{Q}$ the set of g-translates of the sets U_c for all $c > 0$ and all $g \in \mathrm{SL}(2,\mathbb{Z})$ such that $g \cdot \infty = x$. Each $g(U_c)$ is equal to the union of the point x and the interior the circle of radius $r = \frac{1}{2\gamma^2 c}$ touching the real line at the point x. In fact, if $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, we have $x = \alpha/\gamma$ and

$$\begin{gathered} g(U_c) = \{\tau \in \mathcal{H} : \mathrm{Im}\ g^{-1} \cdot \tau > c\} = \{\tau \in \mathcal{H} : \frac{\mathrm{Im}\ \tau}{|-\gamma\tau + \alpha|^2} > c\} = \\ \{\tau = x + iy : (x - \frac{\alpha}{\gamma})^2 + (y - \frac{1}{2\gamma^2 c})^2 < \frac{1}{4\gamma^4 c^2}\}. \end{gathered} \tag{8.7}$$

Now the topology on $\mathcal{H}^*/\Gamma$ is defined as the usual quotient toplogy: an open set in $\mathcal{H}^*/\Gamma$ is open if and only if its pre-image in $\mathcal{H}$ is open. Since $|\gamma| \geq 1$ in (8.7) unless $g \in \Gamma_\infty$, we can find a sufficiently large c such that

$$\Gamma_\infty = \{g \in \Gamma : g(U_c) \cap U_c \neq \emptyset\}.$$

Now, if $x = g_1 \cdot \infty$ we deduce from this that

$$\Gamma_x = g_1 \Gamma_\infty g_1^{-1} = \{g \in \Gamma : g(g_1(U_c)) \cap g_1(U_c) \neq \emptyset\}. \tag{8.8}$$

This shows that the pre-image of some open neighborhood of a cusp on $\mathcal{H}^*/\Gamma$ is equal to the disjoint sum of open neighborhoods of the representatives of this cusp.

Theorem 8.1. *Let Γ be a subgroup of finite index in* $\mathrm{SL}(2,\mathbb{Z})$. *The topological space $\mathcal{H}^*/\Gamma$ admits a unique structure of a compact complex manifold of dimension 1 such that $\mathcal{H}/\Gamma$ is an open submanifold.*

Proof. To warm up let us first see this in the case $\Gamma = \mathrm{SL}(2,\mathbb{Z})$. We saw in Example 1 that $\mathcal{H}/\Gamma(1) \cong \mathbb{C}$. The complex plane $\mathbb{C}$ admits a natural compactification. It is the Riemann sphere $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$. The point ∞ represents the unique cusp of $\Gamma(1)$. Thus we see that

$$\mathcal{H}^*/\Gamma \cong \mathbb{P}^1(\mathbb{C}). \tag{8.9}$$

Now let us consider the general case. The canonical holomorphic map $\pi_{\Gamma(1)} : \mathcal{H} \to \mathcal{H}/\Gamma(1)$ is equal to the composition of the holomorphic maps $\pi_\Gamma : \mathcal{H} \to \mathcal{H}/\Gamma$ and $\pi_{\Gamma/\Gamma(1)} : \mathcal{H}/\Gamma \to \mathcal{H}/\Gamma(1)$. It extends to the composition of continuous maps

$$\pi^*_{\Gamma(1)} : \mathcal{H}^* \xrightarrow{\pi^*_\Gamma} \mathcal{H}^*/\Gamma \xrightarrow{\pi^*_{\Gamma/\Gamma(1)}} \mathcal{H}^*/\Gamma(1) \cong \mathbb{P}^1(\mathbb{C}).$$

First we see that the orbit space $\mathcal{H}^*/\Gamma$ is a Hausdorff topological space. This is obviously true in the case $\Gamma = \Gamma(1)$. Since $\mathcal{H}/\Gamma$ is Hausdorff, we can separate any two points which are not cusps. Since we can separate ∞ on $\mathcal{H}^*/\Gamma(1)$ from any finite point, we can separate any pre-image of ∞ in $\mathcal{H}^*/\Gamma(1)$, which is a cusp on $\mathcal{H}^*/\Gamma(1)$, from a point on $\mathcal{H}/\Gamma$. Finally we can separate any two cusps in $\mathcal{H}/\Gamma$ since the pre-image ${\pi^*_{\Gamma(1)}}^{-1}(U)$ of an open neighborhood U of $\infty \in \mathcal{H}^*/\Gamma(1)$ is equal to the disjoint union of open neighborhoods of points in $\mathcal{H}^* \setminus \mathcal{H} = \mathbb{P}^1(\mathbb{Q})$. The pre-image $\pi^*_\Gamma(V(\mathfrak{c}))$ of an open neighborhood $V(\mathfrak{c})$ of a cusp $\mathfrak{c} = \Gamma \cdot x \in \mathcal{H}^*/\Gamma$ is the disjoint union of open neighborhoods of points belonging to the orbit $\Gamma \cdot x$. Obviously for two different Γ-orbits $\mathfrak{c}$ and $\mathfrak{c}'$ these sets are disjoint. Thus the open sets $V(\mathfrak{c})$ and $V(\mathfrak{c}')$ are disjoint.

Let $U = g_1(U_c)$ be a neighborhood of a representative $x = g_1 \cdot \infty$ of some cusp $\mathfrak{c}$ of Γ. The natural inclusion $U \to \mathcal{H}^*$ factors through the map $U/\Gamma_x \to \mathcal{H}^*/\Gamma_x$. Taking c small enough and using (8.8) we see that this map is injective. Its image is an open neighborhood $\bar{U}$ of the cusp $\mathfrak{c} \in \mathcal{H}^*/\Gamma$. Let h be the index of the cusp. Then Γ_x consists of matrices $\pm\begin{pmatrix}1 & mh\\ 0 & 1\end{pmatrix}$ and hence the map $\tau \to e^{2\pi i\tau/h}$ sends U/Γ_x into $\mathbb{C}$ with the image isomorphic to an open disk. This defines a natural complex structure on the neighborhood $\bar{U}$. Notice that it is consistent with the complex structure on $\bar{U} \cap \mathcal{H}/\Gamma = \bar{U} \setminus \{\mathfrak{c}\}$. Also it is easy to see that the map $\pi^*_{\Gamma(1)}$ extends to the composition of holomorphic maps.

It remains to prove the last assertion, the compactness of $\mathcal{H}^*/\Gamma$. First of all, we replace Γ by a subgroup of finite index Γ' which is normal in $\Gamma(1)$. Then

$$\mathcal{H}^*/\Gamma = (\mathcal{H}^*/\Gamma')/(\Gamma/\Gamma), \quad \mathcal{H}^*/\Gamma(1) = (\mathcal{H}^*/\Gamma')/(\Gamma/\Gamma(1))$$

It remains to use the following simple fact from topology: □

Lemma 8.2. *Let G be a finite group acting continuously on a topological space X. Then X is compact if and only if X/G is compact.*

Proof. Consider the projection $\pi : X \to X/G = Y$. It is a surjective map. It is obvious that the image of a compact space is compact. Assume that Y is compact. Take an open cover $\{U_i\}$ of X. Then replacing U_i with $\cup_{g\in G} g(U_i)$ we may assume that each U_i is G-invariant. Since $U_i = \pi^{-1}(\pi(U_i))$ the sets $\pi(U_i)$ are open in Y. Since Y is compact we can find a finite subcover of $\{\pi(U_i)\}$. This will give us a finite subcover of $\{U_i\}$. □

Remark 8.1. The assertion of the previous theorem does not extend to any discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$. For example, if we take $\Gamma = \{1\}$, the space $\mathcal{H}^* = \mathcal{H}^*/\{1\}$ does not have any complex structure. In fact, any open neighborhood U of ∞, after deleting ∞, must be isomorphic to the punctured open unit disk $\{z \in \mathbb{C} : 0 < |z| < 1\}$. The latter space is not simply-connected (its fundamental group is isomorphic to $\mathbb{Z}$). However $U \setminus \{\infty\}$ can be always chosen to be equal to $\mathrm{Im}\ \tau > c$ which is simply-connected. However, there is a large class of discrete subgroups of $\mathrm{SL}(2,\mathbb{R})$, including subgroups of finite index in $\mathrm{SL}(2,\mathbb{Z})$, for which the assertion of the theorem remains true. These groups are called *fuchsian groups of the first kind.*

Definition. The compact Riemann surface $\mathcal{H}^*/\Gamma$ is called the *modular curve* associated to the subgroup Γ of $\mathrm{SL}(2,\mathbb{Z})$ and is denoted by $X(\Gamma)$.

8.3 Now let us discuss some generalities from the theory of compact Riemann surfaces. Let X be a connected compact Riemann surface and f be a *meromorphic function* on X. This means that the restriction of f to any open neighborhood U is equal to the quotient of two holomorphic functions on U. Assume $f \neq 0$. For each point $x \in X$ we can define the *order* $\nu_x(f)$ of f at x as follows. First we identify a small neighborhood U of x with a small neighborhood V of 0 in $\mathbb{C}$. Then f is equal to the pre-image of a meromorphic function on V which admits a Laurent expansion $a_n z^n + a_{n+1}z^{n+1} + \ldots$ with $a_n \neq 0$ for some integer n. We set

$$\nu_x(f) = n.$$

It is easy to see that this definition does not depend on the choice of an isomorphism between U and V. When $\nu_x(f) > 0$ (resp. $\nu_x(f) < 0$) we say that $\nu_x(f)$ is the *order of* *zero* (resp. the *order of pole*) of f at x. We have the following easily verified properties of $\nu_x(f)$:

Lemma 8.3. *Let $x \in X$ and f, g be two meromorphic functions on X. Then*

(i) $\nu_x(fg) = \nu_x(f) + \nu_x(g)$;

(ii) $\nu_x(f+g) = \min\{\nu_x(f), \nu_x(g)\}$ *if* $f + g \neq 0$.

A meromorphic function on X is called a *local parameter* at x if $\nu_x(f) = 1$. Lemma 8.3 (i) allows us to give an equivalent definition of $\nu_x(f)$. It is an integer such that for any local parameter t at x, there exists an open neighborhood U in which

$$f = t^{\nu_x(f)}\epsilon$$

for some invertible function $\epsilon \in \mathcal{O}(U)$.

Let $\mathrm{Div}(X)$ be the free abelian group generated by the set X. Its elements are called *divisors*. One may view a divisor as a function $D : X \to \mathbb{Z}$ with finite support. It can be written as formal finite linear combinations $D = \sum a_x x$, where $a_x = D(x) \in \mathbb{Z}, x \in X$. For any $D = \sum a_x x \in \mathrm{Div}(X)$ we define its *degree* by the formula:

$$\deg(D) = \sum a_x. \tag{8.10}$$

There is an obvious order in $\mathrm{Div}(X)$ defined by choosing positive elements defined by positive valued divisors. We say $D \geq 0$ if D is positive or equal to 0.

For any nonzero meromorphic function f we define the *divisor of the function* f by

$$\mathrm{div}(f) = \sum_{x \in X} \nu_x(f)x. \tag{8.11}$$

Here we use the compactness of X to see that this sum is finite. Using Lemma 8.3, we see that divisors of functions (*principal divisors*) form a subgroup $\mathrm{P}(X)$ of $\mathrm{Div}(X)$. Two divisors from the same coset are called *linearly equivalent*. The group $\mathrm{Div}(X)/\mathrm{P}(X)$ is called the *group of classes of divisors*.

Finally we introduce the space

$$L(D) = \{f \in \mathcal{M}(X)^* : (f) + D \geq 0\}. \tag{8.12}$$

The famous Riemann-Roch theorem provides a formula for the dimension of this space. In order to state it we need two more ingredients in this formula. The first one is the notion of the canonical class of divisors.

Definition. Let U be an open subset of a Riemann surface X and $t : U \to \mathbb{C}$ is a holomorphic function defining an isomorphism from U to an open subset of $\mathbb{C}$. A meromorphic differential on U is an expression ω of the form

$$\omega = f(t)dt,$$

where $f(t)$ is a meromorphic function on U. A *meromorphic differential* on X is a collection $\omega = \{f(t_U)dt_U\}$ of differentials on open subsets U as above which cover X. It must satify the following compatibility property: if two open sets U and U' overlap then

$$f_U = f'_U \frac{dt_{U'}}{dt_U}$$

when restricted to $U \cap U'$. Here $\frac{dt_{U'}}{dt_U}$ is the derivative of the function $g_{U,U'} = t_{U'} \circ t_U^{-1} : t_U(U \cap U') \to t_{U'}(U \cap U')$.

Two meromorphic differentials are said be equal if they coincide when restricted to the subcover formed by intersections of their defining covers.

Let $\omega = \{f(t_U)dt_U\}$ be a meromorphic function on X. Define

$$\nu_x(\omega) = \nu_x(f_U). \tag{8.13}$$

Since the function $\frac{dt_{U'}}{dt_U}$ is invertible at x, we see that this definition is independent of the choice of an open neighborhood U of x. The divisor

$$\operatorname{div}(\omega) = \sum_x \nu_x(\omega)x. \tag{8.14}$$

is called the *divisor of the meromorphic differential* ω

Since X is compact and hence can be covered by a finite set of locally compact subsets, we see that $\operatorname{div}(\omega)$ is well-defined.

Lemma 8.4. *Let ω and ω' be two meromorphic differentials on X. Then their divisors $\operatorname{div}(\omega)$ and $\operatorname{div}(\omega')$ are linearly equivalent.*

Proof. Without loss of generality we may assume that ω and ω' are defined on the same open cover and use the same local parameter functions t_U. If $\omega = f_U dt_U$ and $\omega' = f_{U'} dt_U$ then the collection of meromorphic functions f_U/f'_U define a meromorphic function F on the whole X (since $f_U/f_{U'} = f'_U/f'_{U'}$ for any two overlapping open subsets in the cover). It follows from the definition that

$$\operatorname{div}(\omega) = \operatorname{div}(\omega') + \operatorname{div}(F).$$

This proves the assertion. □

Definition. The class of linear equivalence of the divisor $\operatorname{div}(\omega)$ of a meromorphic differential is called the *canonical class* of X and is denoted by K_X.

8.4 We can state (without proof) the following:

Theorem 8.2. *(Riemann-(Roch) For any divisor on X,*

$$\dim L(D) = \deg(D) + \dim L(K_X - D) + 1 - g$$

for some non-negative integer g, called the genus *of X.*

Note that the space $L(D)$ depends only on the linear equivalence class of D. In fact, if $D' = D + \operatorname{div}(f)$, then the map $g \to gf$ establishes a bijective linear map from $L(D')$ onto $L(D)$. We use this remark to explain the notation $L(K_X - D)$ (where K_X is not a divisor but rather a class of divisors). This remark, together with the Riemann-Roch formula proves the following:

Corollary 8.1. *Linearly equivalent divisors have the same degree. In particular, for every non-zero meromorphic function f on X,*

$$\deg(\operatorname{div}(f)) = 0. \tag{8.15}$$

Proof. Replacing D with $D + \mathrm{div}(f)$, we do not change the dimensions of the spaces $L(D)$ and $L(K_X - D)$ but change $\deg(D)$ by $\deg(D + \mathrm{div}(f)) = \deg D + \deg(\mathrm{div}(f))$. It follows from Riemann-Roch that $\deg(\mathrm{div}(f)) = 0$. □

Corollary 8.2.

$$\deg K_X = 2g - 2.$$

Proof. Take $D = 0$ and use that $L(0) = \mathcal{O}(X) = \mathbb{C}$. Here we use that a holomorphic function on compact Riemannian surface is constant. This gives

$$g = \dim L(K_X). \tag{8.16}$$

Now take $D = K_X$ and get $\deg(K_X) = 2g - 2$. □

Theorem 8.3. *Let $b_i(X) = \dim H_i(X, \mathbb{R})$ be the Betti numbers of X. Then*

$$b_1 = 2g, \quad b_0 = b_2 = 1.$$

Proof. Since X is a connected compact manifold of dimension 2, this is equivalent to

$$e(X) = \sum_{i=0}^{2} (-1)^i b_i(X) = 2 - 2g = -\deg(K_X). \tag{8.17}$$

Let f be a non-constant meromorphic function on X (its existence follows from the Riemann-Roch theorem). It defines a holomorphic map $f : X \to \mathbb{P}^1(\mathbb{C})$. For any point $x \in X$ set

$$e_x(f) = \begin{cases} \nu_x(f - z) & \text{if } f(x) = z \neq \infty \\ -\nu_x(f) & \text{if } f(x) = \infty. \end{cases} \tag{8.18}$$

It is a positive integer. Since $\deg(\mathrm{div}(f - z)) = 0$ we obtain

$$\sum_{x \in f^{-1}(z)} e_x(f) = \sum_{x \in f^{-1}(\infty)} e_x(f). \tag{8.19}$$

Notice that, for any $x \in X$,

$$\nu_x(df) = \begin{cases} e_x(f) - 1 & \text{if } f(x) \neq \infty \\ -e_x(f) - 1 & \text{if } f(x) = \infty. \end{cases} \tag{8.20}$$

Here df is the meromorphic differential defined locally by $\frac{df}{dt}dt$, where t is a local parameter at x. Since the degree of df is finite we obtain that there are only finitely many points $x \in X$ such that $e_x(f) > 1$. In particular, there is a finite subset of points $S = \{y_1, \dots, y_s\}$ in $\mathbb{P}^1(\mathbb{C})$ such that, for any $y \notin S$

$$\sum_{x : f(x) = y} e_x(f) = n = \#f^{-1}(y). \tag{8.21}$$

Taking into account the formulas (??)-(8.21), we obtain

$$2g-2=\sum_{x\in X}\nu_x(\mathrm{div}(df))=\sum_{y:f(y)\neq\infty}(e_x(f)-1)+\sum_{y:f(y)=\infty}(-e_x(f)-1)=$$
$$\sum_{x\in X}(e_x(f)-1)-2\sum_{f(x)=\infty}e_x=\sum_{x\in X}(e_x(f)-1)-2n= \tag{8.22}$$
$$\sum_{y\in Y}(n-\#f^{-1}(y))-2n.$$

This is called the *Hurwitz formula.* The number n here is called the *degree* of the meromorphic function f. Formula (8.21) says that this number is equal to $\#f^{-1}(y)$ for almost all $y\in\mathbb{P}^1(\mathbb{C})$.

We shall define the triangulation of X as follows. Take a triangulation $\mathcal{T}$ of $\mathbb{P}^1(\mathbb{C})$ in which each point y_j is a vertex. Consider the pre-image $\mathcal{T}'$ of this triangulation in X. Since, the restriction of f to $\mathbb{P}^1(\mathbb{C})\setminus S$ is a covering map, the open cell of our triangulation are equal to connected components of the pre-images of open cells of the triangulation of the sphere. Let d_0,d_1,d_2 be the number of 0-,1-, and 2-cells $\mathcal{T}$. Then we have nd_1 1- and nd_2 2-cells in $\mathcal{T}'$. We also have $\sum_{y\in S}\#f^{-1}(y)$ 0-cells in $\mathcal{T}'$. By the Euler formula we have

$$e(X)=\sum_{y\in S}\#f^{-1}(y)-nd_1+nd_2=$$
$$\sum_{y\in S}\#f^{-1}(y)+n(e(\mathbb{P}^1(\mathbb{C}))-n\#S=2n-\sum_{y\in S}(n-\#f^{-1}(y)).$$

Comparing this with (8.22) we obtain the assertion of the Theorem. □

Example 8.2. Let $X=\mathbb{P}^1(\mathbb{C})$. Take $\omega=dz$ on the complement of ∞ and $\omega=-z^2d\frac{1}{z}$ on the complement to 0. Then $\mathrm{div}(\omega)=-2\infty$. Hence $\deg(K_X)=-2$. This shows that $g=0$ for the Riemann sphere. Of course this agrees with the topological definition of the genus.

Example 8.3. Let $X=E_\tau$ be a complex torus. The holomorphic differential form $\omega=dz$ on $\mathbb{C}$ is invariant with respect to translations. Hence it descends to a 1-differential on X. Obviously its divisor is zero. Thus $\deg(K_X)=0$ and the genus equals 1. Again this agrees with the topological definition.

8.5 Let us compute the genus of the Riemann surface $X=\mathcal{H}^*/\Gamma$. Consider the meromorphic function $j(\tau)$. Since it is a meromorphic modular form of weight 0 with respect to $\Gamma(1)$ it is a also a meromorphic modular form of weight 0 with respect to Γ. Hence it can be considered as a meromorphic function on X. Let $\pi:X\to\mathcal{H}^*/\Gamma(1)$ be the canonical projection. Since j, considered as a function on $\mathcal{H}^*/\Gamma(1)$ has a unique simple pole at ∞, we may identify j with the pull-back $\pi^*(z)$ of the coordinate function z on $\mathbb{P}^1(\mathbb{C})$. We use the Hurwitz formula (8.22) from the proof of Theorem 8.4. Let $x=\Gamma\cdot\tau\in X$. If $\tau\notin\Gamma(1)\cdot i\cup\Gamma(1)\cdot\rho\cup\Gamma(1)\cdot\infty$, then x has an open neighborhood holomorphically isomorphic to an open neighborhood of τ and an open neighborhood of $\pi(x)$. Since $j-j(x)=\pi^*(z-j(x))$, we see that $e_x(j)=1$. If $\tau\in\Gamma(1)\cdot i$, and $\Gamma_\tau=\{1\}$, then x has an open neighborhood isomorphic to an open neighborhood U of τ but $j(x)=j(\tau)$ has an open neighborhood isomorphic to $U/\Gamma(1)_\tau$. This shows that $j-j(x)=\pi^*(z-j(x))$ vanishes at x with order 2, i.e. $e_x(j)=2$. If $\tau\in\Gamma(1)\cdot i$, but $\Gamma_\tau\neq\{1\}$, then x has an open neighborhood isomorphic to an open neighborhood U

of $j(x)$, hence $e_x(f) = 1$. Similarly we find that $e_x(f) = 3$ if $\tau \in \Gamma(1)\cdot\rho$ and $\Gamma_\tau = \{1\}$ and $e_x(j) = 1$ if $\tau \in \Gamma(1)\cdot\rho$ and $\Gamma_\tau \neq \{1\}$. Finally, if x is a cusp of index h, then x has an open neighborhood U isomorphic to $U_c/(T^h)$, where $U_c = \{\tau : \text{Im } \tau > c\} \cup \infty$, and $j(x) = \infty$ has an open neighborhood V isomorphic to $U_c/(T)$. The restriction of π to U is given by sending a local parameter in V to the h-th power of a local parameter in U. Since $1/z$ is a local parameter ∞, j has a pole at x of order h. This shows that $\nu_x(j) = h$ and hence $e_x(j) = h$.

To collect everything together and state a formula for the genus of X, let us make the following:

Definition. Let $X = \mathcal{H}^*/\Gamma$. A point $x = \Gamma\cdot\tau$ is called an *elliptic point* of order 2 (resp, of order 3) if $\tau \in \Gamma(1)\cdot i$ (resp. $\tau \in \Gamma(1)\cdot\rho$) and $\Gamma_\tau \neq 1$.

Theorem 8.4. *The genus of $\mathcal{H}^*/\Gamma$ is equal to*

$$g = 1 + \frac{\mu_\Gamma}{12} - \frac{r_2}{4} - \frac{r_3}{3} - \frac{r_\infty}{2},$$

where μ_Γ is the index of $\Gamma/\Gamma\cap(\pm 1)$ in $\Gamma(1)/(\pm 1)$, r_2 is the number of elliptic points of Γ of order 2, r_3 is the number of elliptic points of Γ of order 3, and r_∞ is the number of cusps of Γ.

Proof. Notice first that the number μ_Γ is equal to the degree of the meromorphic function $X(\Gamma) \to X(\Gamma(1)) \cong \mathbb{P}^1(\mathbb{C})$ defined by the j-function $j : H \to \mathbb{C}$. In fact, the number of the points in the pre-image of a general $z \in \mathbb{C}$ is equal to the number of Γ-orbits in $\mathcal{H}$ contained in a $\Gamma(1)$-orbit. Applying (8.22), we have

$$2g - 2 = -2\mu + \sum_{x\in X}(e_x(j) - 1) =$$

$$-2\mu + \sum_{j(x)=j(i)}(e_x(j) - 1) + \sum_{j(x)=j(\rho)}(e_x(j) - 1) + \sum_{j(x)=\infty}(e_x(j) - 1).$$

We have $(\mu - r_2)/2$ points over $j(i)$ with $e_x(j) = 2$ and $(\mu - r_3)/3$ points over $j(\rho)$ with $e_x(j) = 3$. Also by (8.21), the sum of indices of cusps is equal to μ. This gives

$$2g - 2 = -2\mu + (\mu - r_2)/2 + 2(\mu - r_3)/3 + (\mu - r_\infty),$$

hence

$$g = 1 + \frac{\mu}{12} - \frac{r_2}{4} - \frac{r_3}{3} - \frac{r_\infty}{2}.$$

□

We shall concentrate on the special subgroups Γ of $\Gamma(1)$ introduced earlier. They are the principal congruence subgroup $\Gamma(N)$ of level N and

$$\Gamma_0(N) = \{\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : N|\gamma\}.$$

Obviously

$$\Gamma(N) \subset \Gamma_0(N).$$

Lemma 8.5.

$$\mu_N := \mu_{\Gamma(N)} = \begin{cases} \frac{1}{2}N^3 \prod_{p|N}(1-p^{-2}) & \text{if } N > 2, \\ 6 & \text{if } N = 2, \end{cases} \tag{8.23}$$

$$\mu_{0,N} := \mu_{\Gamma_0(N)} = [\Gamma(1) : \Gamma_0(N)] = N \prod_{p|N}(1+p^{-1}),$$

where p denotes a prime number.

Proof. This easily follows from considering the action of the group $\mathrm{SL}(2, \mathbb{Z}/N)$ on the set $(\mathbb{Z}/N)^2$. The isotropy subgroup of the vector $(1,0)$ is isomorphic to the group of $\Gamma_0(N)/\Gamma(N) \subset \mathrm{SL}(2, \mathbb{Z}/N)$. It consists of matrices of the form $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$. The number of invertible elements a in the ring $\mathbb{Z}/N$ is equal to the value of the Euler function $\phi(N)$. The number of elements b is N. This gives the index of $\Gamma(N)$ in $\Gamma_0(N)$. The index of $\Gamma_0(N)$ in $\Gamma(1)$ is equal to the number of elements in the orbit of $(1,0)$. It is the set of pairs $(a,b) \in \mathbb{Z}/N$ which are coprime modulo N. This is easy to compute. ☐

Lemma 8.6. *There are no elliptic points for $\Gamma(N)$ if $N > 1$. The number of cusps is equal to μ_N/N. Each of them is of order N.*

Proof. The subgroup $\Gamma = \Gamma(N)$ is normal in $\Gamma(1)$. If $\Gamma_\tau \neq \{\pm 1\}$, then $g\Gamma g^{-1} = \Gamma_i$ for any $g \in \Gamma(1)$ which sends τ to i. Similarly for elliptic points of order 3 we get a subgroup of Γ fixing $e^{2\pi i/3}$. It is easy to see that only the matrices 1 or -1 , if $N = 2$, from $\Gamma(N)$ satisfy this property. We leave to the reader to prove the assertion about the cusps. ☐

Next computation will be given without proof. The reader is referred to [**Shimura**].

Lemma 8.7. *The number of elliptic points and cusps for the group $\Gamma_0(N)$ is given by the following formula:*

(i)

$$r_2 = \begin{cases} 0 & \text{if } 4|N, \\ \prod_{p|N}(1 + (\frac{-1}{p})) & \text{otherwise.} \end{cases} \tag{8.24}$$

(ii)

$$r_3 = \begin{cases} 0 & \text{if } 9|N, \\ \prod_{p|N}(1 + (\frac{-3}{p})) & \text{otherwise.} \end{cases} \tag{8.25}$$

(iii)

$$r_\infty = \sum_{d|N, d>0} \phi((d, \frac{N}{d})).$$

Here ϕ is the Euler function and $(\frac{\cdot}{p})$ is the Legendre symbol of quadratic residue. We have

$$(\frac{-1}{p}) = \begin{cases} 0 & \text{if } p = 2, \\ 1 & \text{if } p \equiv 1 \bmod 4, \\ -1 & \text{if } p \equiv 3 \bmod 4, \end{cases} \tag{8.26}$$

$$(\frac{-3}{p}) = \begin{cases} 0 & \text{if } p = 3, \\ 1 & \text{if } p \equiv 1 \bmod 3, \\ -1 & \text{if } p \equiv 2 \bmod 3. \end{cases} \tag{8.27}$$

Applying the previous lemmas we obtain

Corollary 8.3. *The genus g_N of the Riemann surface $X(N) = \mathcal{H}^*/\Gamma(N)$ is given by the formula*

$$g_N = \begin{cases} 1 + \frac{\mu_N(N-6)}{12N} & \textit{if } N > 1, \\ 0 & \textit{if } N = 1. \end{cases} \tag{8.28}$$

Here we use that $-I \notin \Gamma(N)$ for $N > 1$. We know that the Riemann surface $X(1) = \mathcal{H}^*/\Gamma(1)$ parametrizes isomorphism clases of elliptic curves.

For any elliptic curve E we denote by ${}_NE$ the subgroup of N-torsion points. If $E = \mathbb{C}/\Lambda$ we have

$${}_NE = \frac{1}{N}\Lambda/\Lambda$$

Theorem 8.5. *There is a natural bijective map between the set of points of $X(N)' = X(N) \setminus \{\text{cusps}\}$ and isomorhism classes of pairs (E, ϕ), where E is an elliptic curve and $\phi : (\mathbb{Z}/N)^2 \to {}_NE$ is an isomorphism of groups. Two pairs (E, ϕ) and (E', ϕ') are called isomorphic if there exists an isomorphism $f : E \to E'$ of elliptic curves such that $f \circ \phi = \phi'$.*

Proof. Let $E = \mathbb{C}/\Lambda$. Then ${}_NE = \frac{1}{N}\Lambda/\Lambda$. An isomorphism $\phi : (\mathbb{Z}/N)^2 \to {}_NE$ is defined by a choice of a basis in ${}_NE$. A representative of a basis is an ordered pair of vectors (a, b) from Λ such that (Na, Nb) is a basis of Λ. Replacing E by an isomorphic curve, we may assume that $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ for some $\tau \in \mathcal{H}$ and $(Na, Nb) = (1, \tau)$. This defines a surjective map from $\mathcal{H}$ to the set of isomorphism classes of pairs (E, ϕ). Assume the pair $(E_\tau, (\frac{1}{N}, \frac{\tau}{N}))$ is isomorphic to the pair $(E_{\tau'}, (\frac{1}{N}, \frac{\tau'}{N}))$. Since E'_τ is isomorphic to E_τ we get $\tau' = \frac{\alpha\tau+\beta}{\gamma\tau+\delta}$ for some $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma(1)$. The corresponding isomorphism is induced by the isomorphism of $\mathbb{C}$, $z \to z(\gamma\tau + \delta)$. It sends $1/N$ to $(\gamma\tau + \delta)/N$ and τ'/N to $(\alpha\tau + \beta)/N$. It is easy to see that

$$(\alpha\tau + \beta)/N \equiv \tau/N \quad \text{modulo } \Lambda \quad \Longleftrightarrow \alpha \equiv 1 \quad \text{modulo } N, \quad \beta \equiv 0 \quad \text{modulo } N$$

$$(\gamma\tau + \delta)/N \equiv 1/N \quad \text{modulo } \Lambda \quad \Longleftrightarrow \delta \equiv 1 \quad \text{modulo } N, \quad \gamma \equiv 0 \quad \text{modulo } N.$$

This shows that τ and τ' define isomorphic pairs $(E_\tau, \phi), (E_{\tau'}, \phi')$ if and only if they differ by an element of $\Gamma(N)$. $\square$

Remark 8.2. Since $\Gamma(N)$ is an invariant subgroup of $\Gamma(1)$ the factor group $\Gamma(1)/\Gamma(N) \cong \mathrm{SL}(2,\mathbb{Z}/N)$ acts naturally on $X(N)$ and the orbit space is isomorphic to $X(1)$. If one uses the interpretation of $\mathcal{H}/\Gamma(N)$ given in the theorem, then it is easy to see that the action of an element $\sigma \in \mathrm{SL}(2,\mathbb{Z}/N)$ is defined by sending the isomorphism class of a pair (E,ϕ) to the isomorphism class of the pair $(E,\sigma\circ\phi)$.

Theorem 8.6. *There is a natural bijective map between the set of points of $X_0(N)' = X_0(N)\setminus\{\text{cusps}\}$ and isomorhism classes of pairs (E,H), where E is an elliptic curve and H is a cyclic subgroup of order N of ${}_NE$ Two pairs (E,H) and (E',H') are called isomorphic if there exists an isomorphism $f: E\to E'$ of elliptic curves such that $f(H)=H'$.*

Proof. It is similar to the previous proof and is left to the reader. □

Remark 8.3. There is a natural interpretation of the cusp points as the isomorphism classes of certain degenerate pairs (E,H) but to explain this is beyond of the scope of these lectures.

8.6 Finally we interpret the spaces $\mathcal{M}_k(\Gamma)$ as the spaces $L(D)$ for some D on the Riemann surface $X(\Gamma)$. To state it in a convenient form let us generalize divisors to admit rational coefficients. We define a $\mathbb{Q}$-divisor as a function $D: X\to\mathbb{Q}$ with a finite support. We continue to write D as a formal linear combination $D=\sum a_x x$ of points $x\in X$ with rational coefficients a_x. The set of $\mathbb{Q}$-divisors form an abelian group which we shall denote by $\mathrm{Div}(X)_{\mathbb{Q}}$. For any $x\in\mathbb{Q}$ we denote by $\lfloor x\rfloor$ the largest integer less or equal than x. For any $\mathbb{Q}$-divisor $D=\sum a_x x$ we set

$$\lfloor D\rfloor = \sum \lfloor a_x\rfloor x.$$

Theorem 8.7. *Let*

$$D = \frac{1}{2}\sum_{i=1}^{r_2} x_i + \frac{2}{3}\sum_{i=r_1+1}^{r_3} x_i + \sum_{i=1}^{r_\infty} c_i, \quad D^c = D - \frac{1}{k}\sum_{i=1}^{r_\infty} c_i,$$

where $x_1,\dots,x_{r_1}$ are elliptic points of order 2, $x_{r_1+1},\dots,x_{r_1 2+r_2}$ are elliptic points of order 3 and $c_1,\dots,r_\infty$ are cusps. There is a canonical isomorphism of vector spaces

$$\mathcal{M}_k(\Gamma) \cong L(kK_X + \lfloor kD\rfloor)), \quad \mathcal{M}_k(\Gamma)^0 \cong L(kK_X + \lfloor kD^c\rfloor).$$

Proof. Let $F\in\mathcal{M}_k(\Gamma)$. We define its divisor

$$\mathrm{div}(F) = \sum_{x\in X} \nu_x(F)x \in \mathrm{Div}(X)_{\mathbb{Q}},$$

by setting

$$\nu_x(F) = \begin{cases} \frac{1}{e}\nu_\tau(F) & \text{if } x=\Gamma\cdot\tau \text{ is an elliptic point of order } e,\\ \nu_c(F) & \text{if } c \text{ is a representative of a cusp } x.\\ \nu_\tau(F) & \text{if } x=\Gamma\cdot\tau \text{ is neither an elliptic point nor a cusp.}\end{cases}$$

Here $\nu_\tau(F)=n$, where $a_n(z-\tau)^n+\dots, a_n\neq 0$ is the the Taylor expansion of F at τ. Similarly, $\nu_c(F)$ is the smallest non-zero power of $q=e^{2\pi i/h}$ which occurs in the Fourier expansion of F at the cusp c of order h.

Consider the j-function $j : \mathcal{H} \to \mathbb{P}^1(\mathbb{C})$ as a meromorphic Γ-invariant function on $\mathcal{H}$. Its derivative satifies

$$j(\tau)' = \frac{d}{d\tau} j(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = j'(\frac{\alpha\tau+\beta}{\gamma\tau+\delta})\frac{d}{d\tau}(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^{-2} j'(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}).$$

This shows that $\Phi(\tau) = j'(\tau)^k$ satisfies

$$\Phi(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^{2k}\Phi(\tau).$$

So if we consider the ratio $F(\tau)/\Phi(\tau)$ we obtain a Γ-invariant meromorphic function on $\mathcal{H}$. Obviously Φ is meromorphic at the cusps. So this function descends to a meromorphic function on X. Let us compute its divisor. Let $x = \Gamma \cdot \tau \in X$ and t be a local parameter at x. We know that $\nu_\tau(\pi_\Gamma^*(t)) = e(x)$ where $e(x) = 1, 2$ or 3 dependent on whether x is not an elliptic point, an elliptic point of order 2, or an elliptic point of order 3. Thus

$$\nu_x(F/\Phi) = \frac{\nu_\tau(F) - \nu_\tau(\Phi)}{e(x)} = \nu_x(F) - \nu_x(\Phi).$$

Let us compute $\nu_\tau(\Phi)$. We know that

$$\nu_\tau(j - j(\tau)) = \begin{cases} 2 & \text{if } i \in \Gamma(1)\tau, \\ 3 & \text{if } e^{2\pi i/3} \in \Gamma(1)\tau, \\ 1 & \text{otherwise.} \end{cases}$$

This immediately implies that

$$\nu_\tau(j') = \begin{cases} 1 & \text{if } i \in \Gamma(1)\cdot\tau, \\ 2 & \text{if } e^{2\pi i/3} \in \Gamma(1)\cdot\tau, \\ 0 & \text{otherwise.} \end{cases}$$

Thus

$$\nu_x(\Phi) = k(e_x(j) - 1)/e(x).$$

Now, let $x = c_i$ be a cusp represented by $c \in \mathbb{P}^1(\mathbb{Q})$. We used the local parameter $e^{2\pi i\tau/h}$ to define $\nu_c(F)$. Since j admits the Fourier expansion $e^{-2\pi i\tau} + 744 + c_1 e^{2\pi i\tau} + \ldots$ at ∞, we see that j' has the expansion $-2\pi i e^{-2\pi i\tau} + c_2 2\pi i e^{2\pi i\tau} + \ldots$ at the cusp c. This shows that $\nu_c(\Phi) = -kh$. So we get

$$\operatorname{div}(F/\Phi) = \operatorname{div}(F) - k\sum_x(\frac{e_x(j)-1}{e(x)})x + \sum_{i=1}^{r_\infty} h_i c_i.$$

Comparing this with the computation of $\operatorname{div}(dj)$ in the proof of Theorem 8.5, we get

$$\operatorname{div}(F) = \operatorname{div}(F/\Phi) + k\operatorname{div}(dj) + k\sum_{\text{elliptic } x}(1 - e(x)^{-1})x + k\sum_{i=1}^{r_\infty} c_i.$$

Since $\operatorname{div}(F) \geq 0$ we obtain that $F/\Phi \in L(D')$, where D' is linearly equivalent to $kK_X + \lfloor kD \rfloor$ as in the assertion of the theorem. Conversely, if $\Psi \in L(D')$ we easily get that $F = \Psi\Phi \in \mathcal{M}_k(\Gamma)$. Finally, if F is a cuspidal modular form, we have $\nu_x(F) > 0$ at cusps. This easily implies that $F/\Phi \in L(D' - c_1 - \ldots - c_{r_\infty})$. This proves the theorem. $\square$

Corollary 8.4.

$$\dim \mathcal{M}_k(\Gamma) = \begin{cases} (2k-1)(g-1) + kr_\infty + r_2\lfloor k/2 \rfloor + r_3\lfloor 2k/3 \rfloor & \textit{if } k > 1, \\ g + r_\infty - 1 & \textit{if } k = 1. \end{cases}$$

$$\dim \mathcal{M}_k(\Gamma)^0 = \begin{cases} (2k-1)(g-1) + (k-1)r_\infty + r_2\lfloor k/2 \rfloor + r_3\lfloor 2k/3 \rfloor & \textit{if } k > 1, \\ g & \textit{if } k = 1. \end{cases}$$

Proof. This follows immediately from the Riemann-Roch theorem (since $\deg(kK_X + \lfloor kD \rfloor) > \deg K_X$, the space $L(K_X - (kK_X + \lfloor kD \rfloor)) = \{0\}$). □

Corollary 8.5. *Let $f_0, \ldots, f_N$ be a basis of the space $\mathcal{M}_6(\Gamma)$. Then the map*

$$f : \mathcal{H} \to \mathbb{P}^N(\mathbb{C}), \quad \tau \to (f_0(\tau), \ldots, f_N(\tau))$$

defines an isomorphism from $X(\Gamma)$ onto a projective algebraic curve in $\mathbb{P}^N(\mathbb{C})$.

Proof. We know this already when $\Gamma = \Gamma(1)$. So we may assume that $\mu_\Gamma > 1$. By Theorem 8.5 we can identify the space $\mathcal{M}_6(\Gamma)$ with $L(D)$, where

$$\deg D = 6 \deg K_X + 6r_\infty + 3r_2 + 4r_3 = 12g - 12 + 6r_\infty + 3r_2 + 4r_3.$$

I claim that $\deg D > 2g + 1$. If $g \geq 0$ this is obvious. If $g = 0$ we use the formula for the genus from Theorem 8.4. It easily gives that

$$-12 + 6r_\infty + 3r_2 + 4r_3 = \mu > 2g + 1 = 1.$$

It follows from the proof of Theorem 8.8 that

$$\nu_x(f_i) = \nu_x(f_i/{j'}^6) + D(x). \tag{8.29}$$

Now we use the standard argument from the theory of algebraic curves. First of all the map is well-defined. In fact, if all functions f_i vanish at the same point x, we obtain $\nu_x(f_i) > 0$ for all $i = 0, \ldots, N$, and hence $\nu_x(f_i/{j'}^6) + D(x) - 1 \geq 0$ for $i = 0, \ldots, N$. This implies that $L(D) = L(D - x)$. However, this contradicts the Riemann-Roch theorem: since

$$\deg(K_X - D) < \deg(K_X - (D - x)) = 2g - 2 - \deg\ D + 1 < 0,$$

it gives $\dim L(D) = \deg\ D + 1 - g > \dim L(D - x) = \deg\ D - 1 + 1 - g$. Suppose $f(x) = f(x') = p \in \mathbb{P}^N(\mathbb{C})$ for some $x \neq x'$. Without loss of generality we may assume that $p = (1, 0, \ldots, 0)$ (to achieve this we make a linear transformation of coordinates). It follows from (8.23) that $f_i/{j'}^6 \in L(D - x - x'), i = 1, \ldots, N$. This contradicts again Riemann-Roch. We have

$$\deg(K_X - (D - x - x')) = 2g - 2 - \deg\ D + 2 = 2g - \deg\ D < 0.$$

Thus $N \leq \dim L(D - x - x') = \deg\ D - 2 + 1 - g = \dim L(D) - 2 = N - 1$. This contradiction proves that our map is injective. To show that it is an isomorphism onto the image, we have to check that its derivative at each point does not vanish. It is easy to see that this is equivalent to the fact that $L(D - x) \neq L(D - 2x)$ for any $x \in X$. This is proved by the similar argument as before using the Riemann-Roch theorem. □

Corollary 8.6. *Let $\mathcal{R}(X(\Gamma))$ be the field generated by homogeneous fractions f/g, where f, g are modular forms of the same weight. Then*

$$\mathcal{R}(X(\Gamma)) = \mathcal{M}(X(\Gamma)).$$

Proof. It is easy to see that $\mathcal{R}(X(\Gamma))$ is the field of rational functions on the image of the curve $X(\Gamma)$ in $\mathbb{P}^N(\mathbb{C})$. Now we apply the Chow theorem that says that any meromorphic function on a projective algebraic variety is a rational function. □

Exercises

8.1 Show that $\mathcal{H}^*$ is not locally compact.

8.2 Find all N for which the modular curve $X(N) = X(\Gamma(N))$ has genus 0 and 1.

8.3 Find all N for which the modular curve $X_0(N) = X(\Gamma_0(N))$ has genus 0.

8.4 Find all normal subgroups Γ of $\Gamma(1)$ for which the genus of the modular curve $X(\Gamma)$ is equal to 0. [Hint: Use Theorem 10.4 and prove that $r_2 = \mu_\Gamma/2, r_3 = \mu_\Gamma/3, r_\infty|\mu_\Gamma$].

8.5 Generalize the Hurwitz formula to any non-constant holomorphic map $f : X \to Y$ of compact Riemann surfaces.

8.6 Show that the Moebius transformation $\tau \to -1/N\tau$ defines a holomorphic automorphism of finite order 2 of the modular curve $X_0(N)$. Give an interpretation of this automorphism if one identifies the points of $X_0(N)$ with isomorphism clases of pairs (E, H) as in Theorem 8.7.

8.7 Let

$$\Gamma_1(N) = \{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0(N) : \alpha \equiv 1 \mod N\}.$$

Give an analogue of Theorems 8.6 and 8.7 for the curve $\mathcal{H}/\Gamma_1(N)$.

8.8 Using Riemann-Roch theorem prove that any compact Riemann surface of genus 0 is isomorphic to $\mathbb{P}^1(\mathbb{C})$.

8.9 Using Riemann-Roch theorem prove that any compact Riemann surface of genus 1 is isomorphic to a complex torus $\mathbb{C}/\Lambda$.

8.10 Compute the dimension of the space $\mathcal{M}_1(X_0(11))$.

8.11 Using the fact that $\mathcal{H}/\Gamma(1) \cong \mathbb{C}$ prove that any nonsingular plane curve of degree 3 in $\mathbb{P}^2(\mathbb{C})$ is isomorphic to a complex torus.

8.12 Show that any modular curve of positive genus has at least two cusps.

8.13 Find the genus of the curve $X(7)$. Show that the cuspidal forms of weight 1 define an isomorphism from $X(7)$ onto a plane curve of degree 4.

8.14 Let $N = 2, 3, 4, 6, 12$ and $k = 12/N$. Show that the space of cuspidal forms $\mathcal{M}_k(\Gamma(N))^0$ is spanned by the function $\Delta(\tau)^{\frac{1}{N}}$

8.15 Consider the Hesse equation $x^3 + y^3 + z^3 + \gamma xyz = 0$ from Lecture 3.

(i) Show that it defines an elliptic curve $E(\gamma)$ together with an isomorphism $\phi : (\mathbb{Z}/3)^3 \to {}_3E$.

(ii) Show that the coefficient γ considered as a function on $\mathcal{H}/\Gamma(3)$ is a modular function generating the field $\mathcal{M}(X(3))$.

(iii) Show that the value of the absolute invariant function $j(\tau)$ on the isomorphism class of $E(\gamma)$ is equal to

$$j(\gamma) = \frac{(216-\gamma^3)^3\gamma^3}{(\gamma^3-27)^3}.$$

[Hint: Find its Weierstrass equation by projecting the curve from the point $(0,1,-1)$.]

8.16 Desribe explictly the action of $\mathrm{SL}(2,\mathbb{Z}/3)$ on the field $\mathcal{M}(X(3))$ (see Remark 8.2) as follows:

(i) Show that $-I \in \mathrm{SL}(2,\mathbb{Z}/3)$ acts identically.

(ii) Show that $\mathrm{PSL}(2,\mathbb{F}_3) =$ is generated by the elements $\bar{T} = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\bar{S} = \left(\begin{smallmatrix}0&2\\1&0\end{smallmatrix}\right)$.

(viii) Show that $\mathrm{PSL}(2,\mathbb{F}_3)$ acts on the field $\mathcal{M}(X(3))$ by transforming its generator γ as follwos:$\bar{T} : a \to e^{2\pi i/3}a$, $\bar{T} : \gamma \to \frac{6-\gamma}{6+2\gamma}$.

Lecture 9

Absolute Invariant and Cross-Ratio

9.1 Let

$$x_1 = (a_1, b_1), \quad x_2 = (a_2, b_2), \quad x_3 = (a_3, b_3), \quad x_4 = (a_4, b_4)$$

be four distinct points on $\mathbb{P}^1(\mathbb{C})$. The expression

$$R = \frac{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \begin{vmatrix} a_3 & b_3 \\ a_4 & b_4 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_3 & b_3 \end{vmatrix} \begin{vmatrix} a_2 & b_2 \\ a_4 & b_4 \end{vmatrix}} \tag{9.1}$$

is called the *cross-ratio* of the four points. As is easy to see it does not depend on the choice of projective coordinates of the points. Also it is unchanged under the projective linear transformation of $\mathbb{P}^1(\mathbb{C})$:

$$(x, y) \to (ax + by, cx + dy).$$

If none of the points is equal to the infinity point $\infty = (0, 1)$ we can write each x_i as $(1, z_i)$ and rewrite R in the form

$$R = \frac{(z_2 - z_1)(z_4 - z_3)}{(z_3 - z_1)(z_4 - z_2)}. \tag{9.2}$$

One can view the cross-ratio function as a function on the space

$$X = (\mathbb{P}^1(\mathbb{C}))^4 \setminus \Delta$$

of ordered fourtuples of distinct points in $\mathbb{P}^1(\mathbb{C})$. Here Δ denotes the "diagonal", the set of 4-tuples with at least two coordinates equal. The group $\mathrm{GL}(2, \mathbb{C})$ acts naturally on X by transforming each (x_1, x_2, x_3, x_4) in $(g \cdot x_1, g \cdot x_2, g \cdot x_3, g \cdot x_4)$ and R is an invariant function with respect to this action. In other words, R descends to a function on the orbit space

$$R : X/\mathrm{GL}(2, \mathbb{C}) \to \mathbb{C}.$$

The following is a classical result from the theory of invariants:

Theorem 9.1. *The cross-ratio R defines a bijective map*

$$R : X/\mathrm{GL}(2,\mathbb{C}) \to \mathbb{C} \setminus \{0,1\}.$$

Proof. Let $(x_1, x_2, x_3, x_4) \in X$. Solving a system of three linear equations with 4 unknowns a, b, c, d we find a transformation $g : (x, y) \to (ax + by, cx + dy)$ such that

$$g \cdot (a_2, b_2) = (1, 0), \quad g \cdot (a_3, b_3) = (0, 1),$$

$$g \cdot (a_4, b_4) = (1, 1), \quad g \cdot (a_1, b_1) = (1, \lambda),$$

for some $\lambda \neq 0, 1$. We recall that two proportional vectors define the same point. This allows us to choose a representative of each orbit in the form $(\lambda, 0, \infty, 1)$, where we now identify points in $\mathbb{P}^1(\mathbb{C}) \setminus \{\infty\}$ with complex numbers. Since the cross-ratio does not depend on the representative of an orbit, we obtain from (9.1)

$$R(x_1, x_2, x_3, x_4) = \lambda.$$

Since λ takes any value except 0 and 1, we obtain that the image of R is equal to $\mathbb{C}\setminus\{0, 1\}$. Also it is immediate to see that λ and hence the orbit is uniquely determined by the value of R. $\square$

Now let us take an orbit from $X/\mathrm{GL}(2,\mathbb{Z})$ represented by $(\lambda, 0, \infty, 1)$ and assign to it the cubic curve given in affine coordinates by the *Legendre equation* :

$$E(\lambda) : y^2 - x(x - 1)(x - \lambda) = 0. \tag{9.3}$$

This equation can be easily transformed to a Weierstrass equation by a linear change of variables $x' = x + \frac{1+\lambda}{3}, y' = 2y$. In particular, we see that the functions $(\wp(z) - \frac{1+\lambda}{3}, \wp(z)'/2)$ define an isomorphism from a torus $E_\tau = \mathbb{C}/\Lambda_\tau$ to $E(\lambda)$ for an appropriate $\tau \in \mathcal{H}$. We know that the zeroes of $\wp(z)'$ are the points in $\frac{1}{2}\Lambda$ and hence the points $(x, y) = (0, 0), (1, 0), (\lambda, 0)$ are the non-trivial 2-torsion points on $E(\lambda)$ (the trivial one goes to the infinity point $(0, 1, 0) \in \mathbb{P}^2(\mathbb{C})$). If we take the first two points as a basis in the group of 2-torsion points ${}_2E(\lambda)$ we obtain that $E(\lambda)$ defines an isomorphism class of an elliptic curve together with a basis of its group of 2-torsion points. In other words, $E(\lambda)$ represents a point in the moduli space $\mathcal{H}/\Gamma(2)$. Conversely, given a point in $\mathcal{H}/\Gamma(2)$, we can represent it by the isomorphism class of some E_τ with a basis of ${}_2E$ given by $(\frac{1}{2}, \frac{\tau}{2})$ modulo Λ. The points

$$(x_1, x_2, x_3, x_4) = (\wp(\frac{\tau}{2} + \frac{1}{2}), \wp(\frac{1}{2}), \infty, \wp(\frac{\tau}{2})) \tag{9.4}$$

define an ordered 4-tuple of points in $\mathbb{P}^1(\mathbb{C})$, and hence an orbit from X. Replacing τ with $\tau' = \frac{\alpha\tau+\beta}{\gamma\tau+\delta}$, where $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \Gamma(2)$, the point x_i changes to $(\gamma\tau + \delta)^2 x_i, i = 2, 3, 4$ (see Example 6.5). This shows that the cross-ratio $R(x_1, x_2, x_3, x_4)$ does not depend on the choice of τ representing a point in $\mathcal{H}/\Gamma(2)$. Together with Theorem 9.1, this proves

Theorem 9.2. *There is a natural bijection between the set of ordered 4-tuples of distinct points in $\mathbb{P}^1(\mathbb{C})$ modulo projective transformation and the points in $\mathcal{H}/\Gamma(2)$.*

9.2 In view of this theorem the cross-ratio R can be thought as a function

$$R : \mathcal{H}/\Gamma(2) \to \mathbb{C}.$$

The next theorem shows that this function extends to a meromorphic function on $X(2) = \mathcal{H}^*/\Gamma(2)$:

Theorem 9.3. *The cross-ratio function R extends to a meromorphic function λ on $X(2)$ which generates the field $\mathcal{M}(X(2))$. It can be explicitly given by the formula*

$$\lambda(\tau) = \vartheta_{0\frac{1}{2}}(0;\tau)^4/\vartheta_{00}(0;\tau)^4.$$

Proof. It follows from the previous discussion that, as a function on $\mathcal{H}$, the cross-ratio is given by

$$R = R(\wp(\frac{\tau}{2}+\frac{1}{2}), \wp(\frac{1}{2}), \infty, \wp(\frac{\tau}{2})) = \frac{\wp(\frac{\tau}{2}+\frac{1}{2}) - \wp(\frac{1}{2})}{\wp(\frac{\tau}{2}) - \wp(\frac{1}{2}+\frac{\tau}{2})}. \tag{9.5}$$

We have

$$\dim \mathcal{M}_k(\Gamma(2)) = 1 - 2k + k\mu_2/2 = k+1. \tag{9.6}$$

In particular

$$\dim \mathcal{M}_1(\Gamma(2)) = 2.$$

We have seen in Lecture 6 that $\vartheta_{00}^4, \vartheta_{\frac{1}{2}0}^4, \vartheta_{0\frac{1}{2}}^4$ and $\wp(\frac{\tau}{2}), \wp(\frac{\tau}{2}), \wp(\frac{1}{2})$ are examples of modular forms of weight 1 with respect to the group $\Gamma(2)$. There must be some linear relation between these functions. The explicit relation between the first set is known as *Jacobi's identity between theta constants*:

$$\vartheta_{00}^4 = \vartheta_{\frac{1}{2}0}^4 + \vartheta_{0\frac{1}{2}}^4. \tag{9.7}$$

The proof easily follows from the transformation formulas for the theta constants from Lecture 5. Write $\vartheta_{00}^4 = c_1\vartheta_{\frac{1}{2}0}^4 + c_2\vartheta_{0\frac{1}{2}}^4$ for some constants c_1, c_2. Replace τ with $-1/\tau$ and use (5.8),(5.9) to obtain that $c_1 = c_2$. Next replace τ with $\tau+1$ and use (5.3), (5.4) to see that $c_1 = c_2 = 1$.

The relation between the functions from the second set is the obvious one:

$$\wp(\frac{\tau+1}{2}) + \wp(\frac{\tau}{2}) + \wp(\frac{1}{2}) = 0. \tag{9.8}$$

It follows from the Weierstrass equation (the sum of zeroes of the cubic polynomial $4x^3 - g_2x - g_3$ is equal to zero).

Now let us find the relations between functions from the first set and and the second one. We must have $\wp(\frac{1}{2}) = c_1\vartheta_{0\frac{1}{2}}^4 + c_2\vartheta_{\frac{1}{2}0}^4$ for some constants c_1, c_2. Applying the transformation $\tau \to 1+\tau$ and using formulae (5.2)-(5.4) from Lecture 5, we see that $c_1 = 2c_2$. Using the Fourier expansion of $\wp(\frac{1}{2};\tau)$ given in Lecture 6, we obtain that $c_1 = \frac{-(2\pi i)^2}{6}$. Thus

$$\wp(\frac{1}{2}) = -(2\pi i)^2(\frac{1}{6}\vartheta_{0\frac{1}{2}}^4 + \frac{1}{12}\vartheta_{\frac{1}{2}0}^4). \tag{9.9}$$

Similarly we obtain

$$\wp(\frac{\tau}{2}) = (2\pi i)^2(\frac{1}{12}\vartheta_{0\frac{1}{2}}^4 + \frac{1}{6}\vartheta_{\frac{1}{2}0}^4). \tag{9.10}$$

$$\wp(\frac{\tau}{2}+\frac{1}{2}) = (2\pi i)^2(\frac{1}{12}\vartheta_{0\frac{1}{2}}^4 - \frac{1}{12}\vartheta_{\frac{1}{2}0}^4). \tag{9.11}$$

Adding up we check the relation (9.8). Subtracting we obtain *Thomae's Formulae:*

$$\begin{aligned}\pi^2\vartheta_{00}^4 &= \wp(\frac{1}{2}) - \wp(\tau/2),\\ \pi^2\vartheta_{\frac{1}{2}0}^4 &= \wp(\frac{\tau}{2}+\frac{1}{2}) - \wp(\tau/2),\\ \pi^2\vartheta_{0\frac{1}{2}}^4 &= \wp(\frac{1}{2}) - \wp(\frac{\tau}{2}+\frac{1}{2}).\end{aligned} \tag{9.12}$$

Now we can find an expression for the cross-ratio:

$$R = \frac{\wp(\frac{\tau}{2}+\frac{1}{2}) - \wp(\frac{1}{2})}{\wp(\frac{\tau}{2}) - \wp(\frac{1}{2})} = \vartheta_{0\frac{1}{2}}^4/\vartheta_{00}^4. \tag{9.13}$$

It remains to show that the function $\lambda = \vartheta_{\frac{1}{2}0}^4/\vartheta_{00}^4$ generates the field of meromorphic functions on $X(\Gamma(2))$. The algebra $\mathcal{M}(\Gamma(2))$ contains the subalgebra $\mathbb{C}[\vartheta_{0\frac{1}{2}}^4, \vartheta_{00}^4]$. Using (9.6) we can compare the dimensions of the subspaces of homogeneous elements of degree k to see that the algebras coincide. Thus

$$\mathcal{M}(\Gamma(2)) = \mathbb{C}[\vartheta_{0\frac{1}{2}}^4, \vartheta_{00}^4]. \tag{9.14}$$

By Corollary 8.6, the field $\mathcal{M}(X(\Gamma))$ is isomorphic to the field of quotients of the algebra $\mathcal{M}(\Gamma)$. This implies that λ generates the field $\mathcal{M}(X(\Gamma(2))$. □

Definition. The modular function

$$\lambda = \vartheta_{0\frac{1}{2}}^4/\vartheta_{00}^4$$

with respect to $\Gamma(2)$ is called the *lambda-function.*

Let $\pi : X(2) \to X(1)$ be the natural holomorphic map defined by the inclusion $\Gamma(2) \subset \Gamma(1)$. The pre-image of the absolute invariant $\pi^*(j)$ is a meromorphic function on $X(2)$ and hence must be a rational function in λ. Let us find the explicit expression for this rational function.

Theorem 9.4.

$$j = 2^8\frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}.$$

Proof. We know that $\wp(\frac{1}{2}), \wp(\frac{\tau}{2})$ and $\wp(\frac{1}{2}+\frac{\tau}{2})$ are the three roots x_1, x_2, x_3 of the equation $4x^3 - g_2x - g_3 = 0$. Thus

$$g_2 = -4(x_1x_2 + x_1x_3 + x_2x_3) = -2[(x_1+x_2+x_3)^2 -$$

$$(x_1^2 + x_2^2 + x_3^2)] = 2(x_1^2 + x_2^2 + x_3^2).$$

Applying formulas (9.9)-(9.11), we obtain

$$g_2 = 2(\wp(\frac{1}{2})^2 + \wp(\frac{\tau}{2})^2 + \wp(\frac{1}{2} + \frac{\tau}{2})^2) = \frac{(2\pi)^4}{12}(\vartheta_{\frac{1}{2}0}^8 + \vartheta_{0\frac{1}{2}}^8 + \vartheta_{\frac{1}{2}0}^4\vartheta_{0\frac{1}{2}}^4). \tag{9.15}$$

Using the Jacobi Theorem from Lecture 4 , we have

$$g_2^3 - 27g_3^2 = (2\pi)^{12}\Delta = (2\pi)^{12}(2\pi)^{-8}\theta'_{\frac{1}{2}\frac{1}{2}}{}^8 = (2^4)\pi^{12}\vartheta_{0\frac{1}{2}}^8\vartheta_{\frac{1}{2}0}^8\vartheta_{00}^8.$$

Using (9.7), we get

$$j = \frac{1728g_2^3}{g_2^3 - 27g_3^2} = \frac{(2\pi)^{12}(\vartheta_{\frac{1}{2}0}^8 + \vartheta_{0\frac{1}{2}}^8 + \vartheta_{\frac{1}{2}0}^4\vartheta_{0\frac{1}{2}}^4)^3}{(2^4)\pi^{12}\vartheta_{0\frac{1}{2}}^8\vartheta_{\frac{1}{2}0}^8\vartheta_{00}^8} =$$

$$\frac{2^8(\vartheta_{00}^8 - \vartheta_{0\frac{1}{2}}^4(\vartheta_{00}^4 - \vartheta_{0\frac{1}{2}}^4))^3}{\vartheta_{0\frac{1}{2}}^8\vartheta_{00}^8(\vartheta_{00}^4 - \vartheta_{0\frac{1}{2}}^4)^2} = 2^8\frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}.$$

□

Note that there are exactly $6 = 3!$ values of λ (counting with appropriate multiplicities) which give the same value of j. This corresponds to the orbit of $\Gamma(1)/\Gamma(2) \cong \mathrm{SL}(2, \mathbb{F}_2) \cong S_3$ in its natural action on $X(2)$. This shows that there are 6 values of the parameter λ in the equation (9.3) which define isomorphic elliptic curves.

Exercises

9.1 Let $p \in \mathbb{P}^2(\mathbb{C})$ and l_1, l_2, l_3, l_4 be four distinct lines passing through p. For any line l in the plane not passing through p let $p_i = l \cap l_i, i = 1, 2, 3, 4$. Show that the cross-ratio of the four points p_1, p_2, p_3, p_4 does not depend on the choice of an isomorphism $l \cong \mathbb{P}^1(\mathbb{C})$ and also does not depend on the choice of the line l.

9.2 Find the expression for g_3 in terms of the fourth powers of theta constants.

9.3

(i) Show that an unordered set of four points defines at most 6 different cross-ratia.

(ii) Find the sets of unordered 4 points for which the cross-ratio takes less than 6 values.

(iii) Show that the exceptional sets of points from (ii) correspond to harmonic or anharmonic elliptic curves.

(iv) Verify that the function $j = j(\lambda)$ from Theorem 9.4 takes the same value at all six cross-ratia.

(v) Show that there is a natural bijection between the sets of 4 distinct points in $\mathbb{P}^1(\mathbb{C})$ modulo projective transformation and isomorphism classes of elliptic curves.

9.4

(i) Show that the permutation group S_4 contains a normal subgroup H of order 4 which acts identically on $\mathbb{P}^1(\mathbb{C})^4/\mathrm{GL}(2,\mathbb{C})$ via its natural action on $\mathbb{P}^1(\mathbb{C})^4$ by permuting the factors.

(ii) Show that $S_4/H \cong S_3 \cong \mathrm{SL}(2,\mathbb{F}_2)$ and the action of S_4/H on the orbit space $(\mathbb{P}^1(\mathbb{C})^4 \setminus \Delta)/\mathrm{GL}(2,\mathbb{C})$ corresponds to the action of $\mathrm{SL}(2,\mathbb{F}_2)$ on $X(2)$ under the identification of $(\mathbb{P}^1(\mathbb{C})^4 \setminus \Delta)/\mathrm{GL}(2,\mathbb{C})$ with $X(2)$.

9.5

(i) Show that the affine curve $y^2 = (1-x^2)(1-\lambda x^2)$ is birationally isomorphic to the curve $y^2 = x(x-1)(x+\lambda x)$. Show that the exists an elliptic function $\mathrm{sn}(z)$ (called the *Jacobi sine function*) such that $(\mathrm{sn}(z)')^2 = (1-\mathrm{sn}(z))^2(1+\lambda \mathrm{sn}(z)^2)$.

(ii) Define the *Jacobi cosine function* $\mathrm{cn}(z)$ by $\mathrm{cn}(z) = \mathrm{sn}(z)'$. Prove the addition formula

$$\mathrm{sn}(z+w) = \frac{\mathrm{sn}(z)\mathrm{cn}(w) + \mathrm{sn}(w)\mathrm{cn}(v)}{1 + \lambda \mathrm{sn}(z)^2 \mathrm{sn}(w)^2}.$$

Lecture 10

The Modular Equation

10.1 In this lecture we shall prove that the modular curve $X_0(N)$ can be defined by homogeneous algebraic equations with coefficients in $\mathbb{Z}$. By reducing the coefficients modulo a prime p we obtain a nonsingular projective algebraic curve over a finite field $\mathbb{F}_p$ for all prime p except finitely many.

We shall start with the following

Lemma 10.1. *Let Γ and Γ' be subgroups of finite index in $\Gamma(1)$. Assume that there exists a matrix $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2, \mathbb{R})$ such that $\Gamma' \subset A^{-1} \cdot \Gamma \cdot A$. Then, for any $f \in \mathcal{M}_k(\Gamma)$,*

$$f|_k A = f(\frac{\alpha\tau + \beta}{\gamma\tau + \delta})(\gamma\tau + \delta)^{-2k} \in \mathcal{M}(\Gamma')_k.$$

Proof. We have checked it in Chapter 6 for the case $A \in \mathrm{SL}(2, \mathbb{Z})$. But this assumption has not been used in the proof. $\square$

Corollary 10.1. *For $f(\tau) \in \mathcal{M}(\Gamma(1))_k$ we have*

$$f(N\tau) \in \mathcal{M}(\Gamma_0(N))_k.$$

In particular,

$$f(N\tau)/f(\tau) \in \mathcal{M}(X_0(N)).$$

Proof. Take

$$F = \begin{pmatrix} 0 & -1/\sqrt{N} \\ \sqrt{N} & 0 \end{pmatrix}. \tag{10.1}$$

We have, for any $M \in \Gamma(1)$,

$$F \cdot M \cdot F^{-1} = \begin{pmatrix} 0 & -1/\sqrt{N} \\ \sqrt{N} & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 0 & 1/\sqrt{N} \\ -\sqrt{N} & 0 \end{pmatrix} =$$

$$\begin{pmatrix} \delta & -\gamma/N \\ -N\beta & \alpha \end{pmatrix}.$$

Clearly, this implies that $\Gamma_0(N) \subset F \cdot \Gamma(1) \cdot F^{-1}$. Now

$$f|_k F = f(-1/N\tau)(N^{\frac{1}{2}}\tau)^{-2k} = f(N\tau)(N\tau)^{2k}(N\tau)^{-2k} = N^k f(N\tau).$$

This checks the assertion. $\square$

Example 10.1. Take $N = 2$ and $f = \Delta(\tau) \in \mathcal{M}(\Gamma(1))_6$. We see that $\Delta(2\tau)/\Delta(\tau)$ belongs to the space $\mathcal{M}(X_0(2))$. Observe that $q = e^{2\pi i\tau}$ changes to q^2 when we replace τ with 2τ. So

$$\Delta(2\tau)/\Delta(\tau) = \frac{q^2\prod_{m=1}^{\infty}(1-q^{2m})^{24}}{q\prod_{m=1}^{\infty}(1-q^m)^{24}} = q\prod_{m=1}^{\infty}(1+q^m)^{24} = 2^{-12}\mathfrak{f}_2(\tau)^{24}, \tag{10.2}$$

where $\mathfrak{f}_2(\tau)$ is the Weber function defined in (4.13). In particular, we see that

$$\mathfrak{f}_2^{24} = 2^{12}\Delta(2\tau)/\Delta(\tau) \tag{10.3}$$

is a modular function with respect to $\Gamma_0(2)$. It follows from (10.2) that $\mathfrak{f}_2^{24}$ has a simple zero at the cusp ∞. The index of this cusp is equal to 1 since $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right) \in \Gamma_0(2)$. We know from Lemma 8.5 that $\mu_{0,2} = [\bar{\Gamma}(1) : \Gamma_0(2)] = 3$. Thus $\Gamma_0(2)$ has another cusp of index 2. Since $0 \notin \Gamma_0(2)\cdot\infty$ we can represent it by 0. We have

$$\mathfrak{f}_2^{24}(-1/\tau) = 2^{12}\Delta(-2/\tau)/\Delta(-1/\tau) = 2^{12}\Delta(-1/(\tau/2))/\Delta(-1/\tau) =$$

$$2^{12}(\tau/2)^{12}\Delta(\tau/2)/\tau^{12}\Delta(\tau) = \Delta(\tau/2)/\Delta(\tau) =$$

$$\frac{q^{\frac{1}{2}}\prod_{m=1}^{\infty}(1-q^{m/2})^{24}}{q\prod_{m=1}^{\infty}(1-q^m)^{24}} = q^{-\frac{1}{2}}\prod_{m=1}^{\infty}(1+q^{m/2})^{-24}.$$

This shows that $\mathfrak{f}_2^{24}$ has a simple pole at the second cusp. Since $\mathfrak{f}_2^{24}$ is obviously holomorphic on $\mathcal{H}$ we conclude that it has a single pole of order 1. This implies that the meromorphic function $\mathfrak{f}_2^{24} : X_0(2) \to \mathbb{P}^1(\mathbb{C})$ has degree 1 and hence maps $X_0(2)$ isomorphically onto $\mathbb{P}^1(\mathbb{C})$. In particular, $\mathfrak{f}_2^{24}$ being the inverse transform of the rational function z on $\mathbb{P}^1(\mathbb{C})$ generates the field of rational function on $X_0(2)$:

$$\mathcal{M}(X_0(2)) = \mathbb{C}(\Delta(2\tau)/\Delta(\tau)) = \mathbb{C}(\mathfrak{f}_2^{24}). \tag{10.4}$$

10.2 It follows from the Corollary 10.1 that $j(N\tau)$ belongs to the field $\mathcal{M}(X_0(N))$. This field contains the field $\mathcal{M}(X(1)) = \mathbb{C}(j(\tau))$ as a subfield and the degree of the extension is equal to $\mu_{0,N}$. We shall prove that $j(N\tau)$ generates the extension, i.e. $\mathcal{M}(X_0(N)) = \mathbb{C}(j(\tau), j(N\tau))$. We will also describe the algebraic relation between $j(\tau)$ and $j(N\tau)$.

Lemma 10.2. *For any natural N,*

$$\Gamma(1)\cdot\begin{pmatrix}N&0\\0&1\end{pmatrix}\cdot\Gamma(1) = \bigsqcup_{A\in\mathcal{A}_N}\Gamma(1)A,$$

where $\mathcal{A}_N$ is the set of integral matrices $\left(\begin{smallmatrix}a&b\\0&d\end{smallmatrix}\right)$ with $d > 0, ad = N, 0 \le b < d, (a,b,d) = 1$. The number of elements in $\mathcal{A}_N$ is equal to $\mu_{0,N}$.

Proof. First of all the right-hand side is the set $M(N)$ of integral primitive (i.e. with g.c.d of entries equal to 1) matrices with determinant N. In fact, for any such matrix we can apply row transformations with matrices from $\Gamma(1)$ to reduce it to upper triangular form. By further row operations we can make d positive and b satisfy $0 \leq b < d$. The number a will be the greatest common divisor of the first column of the matrix, so is defined uniquely. Then d will be defined uniquely by the condition $ad = N$ and b will be defined uniquely by the above condition. It is obvious that the left-hand side is contained in $M(N)$. To prove the opposite inclusion, it suffices to show that each matrix A from $\mathcal{A}_N$ is contained in the left-hand-side. This follows from the well known fact that each integral matrix can be transformed by integral row and column transformations to the unique matrix of the form $\left(\begin{smallmatrix} n & 0 \\ 0 & n' \end{smallmatrix}\right)$, where $n|n'$. The last assertion can be checked by using elementary number theory. When $N = p$ is prime, we obviously have $\#\mathcal{A}_p = p + 1$. Now, if N is not prime we have

$$\#\mathcal{A}_N = \psi(N) = N \prod_{p|N} (1 + p^{-1}) = \mu_{0,N}.$$

This can be proved by using the multiplicative property of the function $\psi(n)$ and the formula

$$\psi(N) = \sum_{d|N} \frac{d}{(d, \frac{N}{d})} \phi((d, \frac{N}{d})),$$

where ϕ is the Euler function. $\square$

Lemma 10.3. *Let $f(\tau)$ be a modular function with respect to $\Gamma(1)$ which is holomorphic on $\mathcal{H}$ and admits the Fourier expansion $f = \sum_{n=-r}^{\infty} c_n q^n$. Then f is a polynomial in $j(\tau)$ with coefficients in the subring of $\mathbb{C}$ generated by the Fourier coefficients $c_0, \ldots, c_{-r}$.*

Proof. Observe first that $r > 0$ unless f is constant. Since the Fourier expansion of j starts as $q^{-1} + \ldots$ we can subtract $c_{-r} j^r$ from f to decrease the order of its pole at ∞. Then we do it again, if needed, untill we get that the difference g has Fourier expansion of the form $q^m + \ldots$ with $m > 0$. Since g is holomorphic at infinity and vanishes there, it must be zero. Since all the coefficients of the Fourier expansion of j are integers, as a result we subtract from f a polynomial in j with coefficients in $\mathbb{Z}[c_{-r}, \ldots, c_0]$ and obtain 0. $\square$

Lemma 10.4. *Let $f : X \to Y$ be a holomorphic map of compact Riemann surfaces. Then $f^* : \mathcal{M}(Y) \to \mathcal{M}(X)$ defines an algebraic extension of the field of meromorphic functions. The degree of this extension is equal to the number of points in the pre-image $f^{-1}(y)$ (counting with multiplicities equal to the ramification indices) for any $y \in Y$.*

Proof. We skip the proof of this lemma. One can learn about this fact in any intruduction book in algebraic geometry. $\square$

Theorem 10.1. *The field $\mathcal{M}(X_0(N))$ is generated by $j(\tau)$ and $j(N\tau)$. There exists a polynomial $\Phi_N[X, Y] \in \mathbb{Z}[X, Y]$ such that $F(j(N\tau), j(\tau)) \equiv 0$. The polynomial $\Phi_N[X, j] \in \mathbb{C}(j)[X]$ is a minimal polynomial for $j(N\tau)$ in the fields extension $\mathcal{M}(X_0(N))/\mathcal{M}(X(1))$. Its degree is $\mu_{0,N}$. When $N > 1$, $\Phi_N[X, Y]$ is symmetric in X and Y, and if $N = p$ is prime,*

$$\Phi_N(X, Y) \equiv X^{p+1} + Y^{p+1} - X^p Y^p - XY \mod p.$$

Proof. Let $\mathcal{A}_N$ be the set of matrices from Lemma 10.2. Consider the polynomial

$$\Phi = \prod_{A\in\mathcal{A}_N}(X - j(A\cdot\tau)) = \sum_{m=0}^{\psi(N)} s_m X^m$$

Its coefficients s_m are symmetric functions in $j(A\cdot\tau)$ and hence are holomorphic functions on $\mathcal{H}$. It folows from Lemma 10.2 that, for each $M \in \Gamma(1)$ and $A \in \mathcal{A}_N$, we have $AM = M'A'$ for some $M' \in \Gamma(1), A' \in \mathcal{A}_N$. Thus $j(A\cdot(M\cdot\tau)) = j(M'\cdot(A'\cdot\tau)) = j(A'\cdot\tau)$. Thus replacing τ by $M\cdot\tau$ defines a permutation among the functions $j(A\cdot\tau)$. This implies that s_m are modular functions with respect to $\Gamma(1)$. By Lemma 10.3, each s_m is a polynomial in $j(\tau)$ with coefficients belonging to the subring of $\mathbb{C}$ generated by its Fourier coefficients. However, for any $A = \left(\begin{smallmatrix} a & b\\ 0 & d\end{smallmatrix}\right) \in \mathcal{A}_N$, we have

$$e^{\frac{2\pi i(a\tau+b)}{d}} = e^{\frac{2\pi i a\tau}{d}} e^{\frac{2\pi i b}{d}} = q^{\frac{a}{d}}\zeta_d^b,$$

where $q = e^{2\pi i\tau}$, as usual, and ζ_d is the primitive d-th root of unity equal to $e^{2\pi i/d}$. Now, using the Fourier expansion of $j(\tau)$ we obtain

$$j(\frac{a\tau+b}{d}) = \frac{1}{q^{a/d}\zeta_d^b} + \phi(q^{\frac{a}{d}}\zeta_d^b), \tag{10.5}$$

where ϕ is holomorphic at infinity. Since the coefficients of j are integers we see that the coefficients of the Fourier expansion of each $j(A\cdot\tau)$ belong to the ring $\mathbb{Z}[\zeta_d]$. By Lemma 10.3, the coefficients s_m are polynomials in $j(\tau)$ with coefficients in $\mathbb{Z}[\zeta_N]$. Consider the automorphism of the cyclotomic field $\mathbb{Q}(\zeta_N)$ which acts by sending ζ_N to ζ_N^k, where $(k, N) = 1$. It is clear from (10.5) that this automorphism transforms $j(A\cdot\tau)$ to $j(A'\cdot\tau)$ for some other $A' \in \mathcal{A}_N$. This shows that the functions s_m are invariant with respect to all such automorphisms, hence must be polynomials in j with coefficients in $\mathbb{Z}$.

Thus we can consider Φ as an element of the ring $\mathbb{Z}[X, j]$. Replacing the variable j with Y we obtain the polynomial $\Phi_N(X,Y) \in \mathbb{Z}[X,Y]$. This will be the polynomial from the assertion of the theorem. First of all, taking $A = \begin{pmatrix} N & 0\\ 0 & 1\end{pmatrix} \in \mathcal{A}_N$ we obtain $\Phi_N(j(N\tau)), j) = 0$. The polynomial $\Phi_N[X, j]$ is of degree $\psi(N)$ and is irreducible since its roots $j(A\cdot\tau)$ are permuted transitively by the group $\Gamma(1)$. By Lemma 10.4, its degree is equal to the degree of the extension $\mathcal{M}(X_0(N))/\mathcal{M}(X(1))$. Since $\Phi_N[X, j]$ is the minimal polynomial for $j(N\tau)$ over the field $\mathbb{C}(j) = \mathcal{M}(X(1))$, and its degree is equal to the degree of the extension, we see that $j(\tau)$ and $j(N\tau)$ generate $\mathcal{M}(X_0(N))$. Next, replacing τ with $-1/N\tau$ in the identity $\Phi_N(j(N\tau), j) \equiv 0$, we obtain

$$\Phi_N(j(-1/\tau), j(-1/N\tau)) = \Phi_N(j, j(N\tau)) \equiv 0.$$

Since $\Phi_N(X, j)$ is irreducible as a polynomial in X, the polynomial $\Phi_N(j, X)$ must be divisible by $\Phi_N(X, j)$. It follows from the Gauss lemma that
$\Phi_N(X,Y) = c\Phi_N(Y,X)$, where $c = \pm 1$. If $c = -1$, we have $\Phi_N(X,X) = 0$, hence $\Phi_N(j,j) = 0$. However, $\Phi_N(X, j)$ is irreducible over $\mathbb{C}(j)$ hence j cannot be its zero. So $c = 1$ and we obtain that $\Phi_N(X,Y)$ is symmetric in X, Y. It remains to prove the last property (*Kronecker's congruence relation*).

Assume $N = p$ is prime. Then the set $\mathcal{A}_p$ consists of matrices $A_s = \begin{pmatrix} 1 & s\\ 0 & p\end{pmatrix}$, $0 \leq s < p$, and $A_p = \begin{pmatrix} p & 0\\ 0 & 1\end{pmatrix}$. It follows from the formula (10.5) and the Fermat theorem that we have the following congruence for the Fourier expansion of $j(A_s \cdot \tau)$ in $q^{\frac{1}{p}}$

$$j(A_s \cdot \tau)(q) \equiv j(q)^{1/p} \mod (1-\zeta_p),$$

$$j(A_p \cdot \tau)(q) \equiv j(q)^p \mod p.$$

Here the congruence means that the corresponding Fourier coefficients satisfy the congruence. The principal ideal $(1-\zeta_p)$ in the ring $\mathbb{Z}[\zeta_p]$ is prime and $(1-\zeta_p)|p$ (since $(\sum_{i=1}^{p-1} i\zeta_p^i)(1-\zeta_p) = -p$). This implies

$$\Phi_p(X, j(q)) \equiv (X - j(q)^p)(X^p - j(q)) \mod (1-\zeta_p).$$

Let $\Phi_p(X,j) - (X-j^p)(X^p-j) = \sum_m a_m X^m$. The previous congruence shows that the coefficients a_m are all divisible by $(1-\zeta_p)$, and since they are integers, they must be divisible by p. This proves the theorem. □

Definition. The equation $\Phi_N(X,Y) = 0$ from the previous theorem is called the *modular equation* .

Example 10.2. Let $p = 2$. The modular equation in this case is

$$F(X,Y) = (X-Y^2)(X^2-Y) + 2^4\cdot 3\cdot 31XY(X+Y) - 2^4 3^4 5^3(X^2+Y^2)+$$

$$2^8\cdot 7\cdot 61\cdot 373XY + 2^8 3^7\cdot 5^6(X+Y) - 2^{12}3^9 5^9 = 0.$$

For $N = 3$ the modular equation was computed by Stephen Smith in 1878. It has the form

$$F(x,y) = x(x+2^7\cdot 3\cdot 5^3)^3 + y(y+2^7\cdot 3\cdot 5^3)^3 - 2^{16}x^3y^3+$$

$$2^{11}\cdot 3^2\cdot 31x^2y^2(x+y) - 2^2\cdot 3^3\cdot 9907xy(x^2+y^2) + 2\cdot 3^4\cdot 13\cdot 193\cdot 6357x^2y^2+$$

$$2^8\cdot 3^5\cdot 5^3\cdot 4471xy(x+y) - 2^{15}\cdot 5^6\cdot 22973xy = 0,$$

where one has to make the substitution $X = \frac{27}{4}x, Y = \frac{27}{4}y$.

Other cases where it was computed explicitly are $N = 5, 7, 11$. The last case took 20 hours on a VAX-780. It is a polynomial of degree 21 with some coefficients of order 10^{60}.

Corollary 10.2. *The modular curve $X_0(N)$ is isomorphic to a nonsingular projective algebraic curve defined over $\mathbb{Q}$.*

Proof. We assume that the reader is familiar with some basic notions in algebraic geometry (first two chapters of **[Shafarevich]** suffices). The theorem says that $X_0(N)$ is birationally isomorphic to the plane affine curve $\Phi_N(x,y) = 0$ defined over $\mathbb{Q}$ (i.e. its equation is given by a polynomial with rational coeffcients). By homogenizing the equation we obtain a projective curve defined over $\mathbb{Q}$. Now we use the normalization process. Since this process can be done over the same ground field, the normalized nonsingular curve is also defined over $\mathbb{Q}$. □

Remark 10.1. In fact, one can choose the equations defining $X_0(N)$ with coefficients in $\mathbb{Z}$. This allows one to reduce the coefficients modulo a prime number p to obtain a projective algebraic curve over a finite field $\mathbb{F}_p$. It follows from the Kronecker congruence that the prime numbers p dividing N are "bad primes", i.e. the reduction is a singular algebraic curve. One can show that all others primes are "good primes", i.e. the reduction is a nonsingular algebraic curve. The reductions of the modular curve $X_0(N)$ modulo a good prime p are examples of curves over a finite field with "many rational points" and are used in coding theory.

Definition. A holomorphic map between elliptic curves $E' \to E$ is called an *isogeny* of order n if it is a homomorphism of groups whose kernel is a group of order n.

Let $E = \mathbb{C}/\Lambda$, $E' = \mathbb{C}/\Lambda'$. It follows from the definition that any isogeny $f : E' \to E$ can be lifted to a map $\tilde{f} : \mathbb{C} \to \mathbb{C}$, $z \to \alpha z$ such that $\tilde{f}(\Lambda') \subset \Lambda$. The kernel of this map is the group $\alpha^{-1}\Lambda/\Lambda' \subset \mathbb{C}/\Lambda'$. So its order is equal to the determinant of the matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that

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

Here $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \Lambda' = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'$. We can change the bases to assume that $A = \left(\begin{smallmatrix} d_1 & 0 \\ 0 & d_2 \end{smallmatrix}\right)$ is diagonal with $d_1|d_2$ and $d_1d_2 = n$. The pair (d_1, d_2) is defined uniquely by the previous property and is called the *type* of the isogeny. The isogeny is called *cyclic* if $d_1 = 1$. In this case the kernel of the isogeny is a cyclic group of order n.

Corollary 10.3. *Let E_τ be a complex torus corresponding to the lattice $\mathbb{Z} + \tau\mathbb{Z}$. Then the set of isomorphism classes of elliptic curves admitting a cyclic isogeny $f : E' \to E$ of order N consists of the isomorphism classes of elliptic curves $E_{\tau'}$ where*

$$\Phi_N(j(\tau'), j(\tau)) = 0.$$

Proof. Let $E' \to E$ be a cyclic isogeny of order N. As we have explained before, replacing the curves by isomorphic curves, we may assume that

$$E = \mathbb{C}/\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \quad E' = \mathbb{C}/\mathbb{Z}\omega_1 + \mathbb{Z}N\omega_2.$$

Further replacing them by isomorphic curves we may assume that $\omega_1 = 1, \omega_2 = \tau \in \mathcal{H}$. Thus the isomorphism class of E is determined by the value of j at τ, and isomorphism class of E' is determined by the value of j at $N\tau$. But the pair $(j(N\tau), j(\tau))$ satisfies the modular equation $\Phi_N(x, y) = 0$. Conversely, if $(j(\tau'), j(\tau))$ satisfies the modular equation, then $j(\tau') = j(A \cdot \tau)$ for some matrix $A = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathcal{A}_N$. This implies that $E_\tau' \cong E_{A\cdot\tau'}$. Since τ and $A \cdot \tau$ are both in the upper half-plane, we must have $\tau' = A \cdot \tau = (a\tau + b)/d$. Replacing $\mathbb{Z} + \mathbb{Z}\tau'$ with $d\mathbb{Z} + (a\tau + b)\mathbb{Z}$ which defines an isomorphic curve, we see that $d\mathbb{Z} + (a\tau + b)\mathbb{Z} \subset \mathbb{Z} + \mathbb{Z}\tau$ and hence there exists an isogeny $E_\tau' \to E_\tau$ whose kernel is given by the matrix A. Since $(a, b, d) = 1$, the elementary divisors of this matrix are $(1, ad)$. This shows that f is a cyclic isogeny. ☐

Corollary 10.4. *Let $\tau \in \mathbb{Q}(\sqrt{-d})$ where d is a positive rational number. Then the value $j(\tau)$ is an algebraic integer.*

Proof. Let $\mathcal{O}$ be the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{-d})$. It admits a basis $1, \omega$. Let $\alpha \in \mathcal{O}$ such that its norm N is square-free. Then

$$\alpha\omega = a\omega + b, \quad \alpha = c\omega + d.$$

Here the matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has determinant equal to the norm of α. Since the latter is equal to the determinant of the matrix and is square-free, we have $(a,b,c,d) = 1$. Also observe that $\omega = A \cdot \omega = \frac{a\omega+b}{c\omega+d}$. By Lemma 10.2, $M = M'A$, where $M' \in \Gamma(1)$, and $A \in \mathcal{A}_N$. This shows that

$$j(\omega) = j(M \cdot \omega) = j(M'A \cdot \omega) = j(A \cdot \omega).$$

and hence $j(\omega)$ satisfies the equation $\Phi_N(X,X) = 0$. This equation is a monic polynomial over $\mathbb{Z}$, so that $j(\omega)$ is an algebraic integer. We can write $n\tau = \alpha\omega + \beta$ for some integers n, α, β. Since $\Phi_n(j(\tau), j(n\tau)) = 0$, $j(\tau)$ is integral over the ring $\mathbb{Z}[j(n\tau]$. So, it suffices to show that $j(n\tau)$ is an algebraic integer. Since $j(n\tau) = j(\alpha\omega + \beta) = j(\alpha\omega) = j(-\alpha\omega)$, we obtain, by the previous argument, that $j(n\tau)$ is integral over $j(\omega)$. Since the latter is an algebraic integer, $j(\tau)$ is an algebraic integer as well. □

Remark 10.2. Notice that $\tau \in \mathbb{Q}(\sqrt{-d})$ if and only if the lattice Λ_τ has complex multiplication (see Lecture 2). By Exercise 2.6 this is equivalent to that E_τ has endomorphism ring larger than $\mathbb{Z}$. An elliptic curve with this property is called an *elliptic curve with complex multiplication* . Viewing j as a function on the set of isomorphism classes of elliptic curves, the previous corrollary says that the value of j at the isomorphism class of an elliptic curve with complex multiplication is an algebraic integer.

Remark 10.3. The classical *Kronecker Theorem* asserts that any finite abelian extension of $\mathbb{Q}$ with abelian Galois group can be obtained by joining roots of unity to $\mathbb{Q}$. Observe that a nth root of unity is the value of the function $f(z) = e^{2\pi iz/n}$ on $\mathbb{Z}$. Let K be an imaginary quadratic extension of $\mathbb{Q}$ and let $\mathfrak{a}$ be an ideal in the ring of integers of K. Then the set $j(\mathfrak{a})$ generates a maximal non-ramified extension of the field K with abelian Galois group. This is the celebrated "Jügendtraum" of Leopold Kronecker which was proven by himself when he had passed his youth age.

Corollary 10.5. *A modular function $f \in \mathbb{C}(j, j_N)$ belongs to $\mathbb{Q}(j, j_N)$ if and only if its Fourier expansion at ∞ has all coefficients in $\mathbb{Q}$.*

Proof. Since j and j_N has rational Fourier coefficients, we only need to prove the sufficiency. Let $f = R(j, j_N)$ where $R = P(x,y)/Q(x,y)$ is a rational function with coefficients in $\mathbb{C}$. Any automorphism σ of $\mathbb{C}$ acting on $\mathbb{C}(j, j_N)$ sends R to R^σ by replacing the coefficients of R with its σ-conjugates. This is independent of the choice of R since the modular equation relating j and j_N has coefficients in $\mathbb{Q}$. Let f^σ denotes the image of f under the action of σ. I claim that

$$f^\sigma(\tau) = \sum_{n=-r}^{\infty} \sigma(c_n) q^n,$$

where $f(\tau) = \sum_{n=-r}^{\infty} c_n q^n$ is the Fourier expansion of f at ∞. Since

$$\mathbb{C}(j, j_N) = \sum_{i=0}^{\psi(N)-1} \mathbb{C}(j) j_N^i,$$

it suffices to prove the assertion for $f \in \mathbb{C}(j)$. Write

$$f = \frac{a_0 + a_1 j + \ldots + a_n j^n}{b_0 + b_1 j + \ldots + b_m j^m}. \tag{10.6}$$

Replacing f with f^{-1} we may assume $n \geq m$. Multiplying by some integer power of j, we may assume that $a_0, b_0 \neq 0$. Since a_0/b_0 is equal to the value of f at ∞, it must be a rational number. The difference $(f - \frac{a_0}{b_0})/j$ has Fourier coefficients in $\mathbb{Q}$, and has representation in the form (10.16) with smaller n. Continuing in this way we arrive at the case $n = m = 0$ where the assertion is obvious. □

10.3 Let us explain the meaning of the symmetry property of the modular equation. Consider the map $\mathcal{H} \to \mathcal{H}$ defined by the formula $\tau \to -1/N\tau$. It is easy to see that the matrix $F = \begin{pmatrix} 0 & 1/\sqrt{N} \\ -\sqrt{N} & 0 \end{pmatrix}$ belongs to the normalizer of the group $\Gamma_0(N)$ in $\mathrm{SL}(2, \mathbb{R})$, i.e. $FMF^{-1} \in \Gamma_0(N)$ for any $M \in \Gamma_0(N)$. This implies that the previous map factors to a map of the quotient $\mathcal{H}/\Gamma_0(N) \to \mathcal{H}/\Gamma_0(N)$. It can be shown using some basic algebraic geometry that it extends uniquely to a holomorphic map

$$\mathrm{Fr} : X_0(N) \to X_0(N).$$

Observe also that $F^2 = -1$ so that $\mathrm{Fr}^2 =$ identity. It is called the *Fricke involution.* By taking the inverse transform of functions, the Fricke involution acts on modular functions of weight k by

$$\mathrm{Fr}^*(f)(\tau) = f(-1/N\tau) = (N\tau)^{2k} f(N\tau).$$

In particular,

$$\mathrm{Fr}^*(j(\tau)) = j(N\tau), \quad \mathrm{Fr}^*(j(N\tau)) = j(-1/\tau) = j(\tau).$$

This implies that the Fricke involution acts on the modular equation by switching X and Y.

Remark 10.4. Let $X_0(N)^+ = X_0(N)/(Fr)$ be the quotient of the curve $X_0(N)$ by the cyclic group generated by the Fricke involution. One can find all numbers N such that the genus of this curve is equal to 0. It was observed by A. Ogg that the list of corresponding primes is the same as the list of all prime divisors of the order of the Monster group, the largest simple sporadic finite group. This has been explained now.

Example 10.3. We know that $R = \Delta(2\tau)/\Delta(\tau)$ generates the field $\mathcal{M}(X_0(2))$. The Fricke involution acts on this generator as follows:

$$\mathrm{Fr}^*(R) = \frac{\Delta(-1/\tau)}{\Delta(-1/2\tau)} = \frac{\Delta(\tau)(\tau)^{12}}{\Delta(2\tau)(2\tau)^{12}} = \frac{\Delta(\tau)}{2^{12}\Delta(2\tau)} = 2^{-12}R^{-1}.$$

We know that every modular function with respect to the field $\Gamma_o(N)$ can be written as a rational function in j and j_N with complex coefficients. In other words, it belongs to the field $\mathbb{C}(j, j_N)$. The next theorem characterizes functions which belong to the field $\mathbb{Q}(j, j_N)$.

Exercises

10.1 Prove that there exists exactly $\psi(N)$ isomorphism classes of elliptic curves admitting a cyclic isogeny of order N onto a fixed elliptic curve.

10.2 Let $f : E' \to E$ be an isogeny between elliptic curves of order N. Show that there exists an isogeny $f' : E \to E'$ of the same order.

10.3 Show that the Fricke involution of $\mathcal{H}/\Gamma_0(N)$ sends the point representing the isomorphism class of the pair (E, A) (E is an elliptic curve and A is its cyclic subgoup of orer N) to the pair (E', A'), where $E' = E/A, A' = {}_NE/A$.

10.4 Let f, g be two modular forms of the same weight with respct to $\Gamma(1)$. Show that, for any $A \in \mathcal{A}_N$ the function $f(A \cdot \tau)/g(\tau)$ is a modular function with respect to $(A^{-1}\Gamma(1)M) \cap \Gamma(1)$.

10.5 Show that $\Phi(j(\tau), j(\tau)) = 0$ for some $N > 1$ if and only if E_τ has complex multiplication.

10.6 Let $N = 2, 3, 5, 11$ and $k = 12/(N+1)$. Show that the space of cuspidal forms $\mathcal{M}_k(\Gamma_0(N))^0$ is spanned by the function $(\Delta(\tau)\Delta(N\tau))^{\frac{1}{N+1}}$.

10.7 Let $N = 2, 3, 6$ and $k = 6/N$. Show that the space of parabolic forms $\mathcal{M}_k(\Gamma(N))^0$ is spanned by the function $\Delta(\tau)^{1/N}$.

10.8 Show that $\mathcal{M}(X_0(2)) = \mathbb{C}(\frac{\wp(\frac{1}{2}+\frac{\tau}{2};\tau)}{\wp(\frac{\tau}{2};\tau)})$ [Hint: use that $\mathfrak{f}^{24} = \vartheta_{\frac{1}{2}0}^{12}/\eta^{12}$ and apply the six crss-ratia formulas].

10.9 Generalize Example 10.1 by proving that the function $\Phi(\tau) = (\frac{\Delta(N\tau)}{\Delta(\tau)})^{\frac{1}{N-1}}$ generates the field $\mathcal{M}(X_0(N))$ for $N = 2, 3, 5, 7, 13$ [Hint: Check that Φ^{N-1} has one zero and one pole of multiplicity $N-1$ and use the formula for the genus of $X_0(N)$ to check that $X_0(N) \cong \mathbb{P}^1(\mathbb{C})$]

10.10 A modular function $f \in \mathcal{M}(X(\Gamma))$ is called a *Hauptfunction* for Γ if it generates the field $\mathcal{M}(X(\Gamma))$ and admits a Fourier expansion at the cusp ∞ (of index h) of the form $q^{-1/h} + \sum_{m\geq 0} a_m q^{m/h}$, where a_m are integers. An example of a Hauptfunction is the absolute invarinat j.

(i) Show that the functions $(\frac{\Delta(N\tau)}{\Delta(\tau)})^{\frac{1}{N-1}}$ are Hauptfunctions for the group $\Gamma_0(N)$ when $N = 2, 3, 5, 7$.

(ii) Show that the function γ^3, where γ is the parameter in the Hesse equation (see Problem 3.6) is a Hauptfunction for $\Gamma_0(3)$.

(iii) Show that the $2^{-4}\lambda$ is a Hauptfunction for $\Gamma(2)$ (see Lecture 10).

(iv) Show that the function $4\frac{\vartheta_{00}(0;\tau)^2+\vartheta_{0\frac{1}{2}}(0;\tau)^2}{\vartheta_{\frac{1}{2}0}(0;\tau)^2}$ is a Hauptfunction for $\Gamma(4)$.

10.11 Show that the fundamental domain for $\Gamma_0(p)$ where p is prime, can be obtained as the union of the fundamental domain for $\Gamma(1)$ and its translates by transformations ST^k, where $k = 0, \ldots, p$.

10.12 Find the expression of the absolute invariant j in terms of the generator Φ of the field of modular functions for $\Gamma_0(2)$.

10.13 Prove that the cosets of $\Gamma(1)$ modulo $\Gamma_0(N)$ can be represented by the matrices $\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}$ where $(c,d) = 1, d|Nm0 \leq c < N/d$.

10.14 Prove the *doubling identities*:

$$2\vartheta_{\frac{1}{2}0}(2\tau)^2 = \vartheta_{00}(\tau)^2 - \vartheta_{0\frac{1}{2}}(\tau)^2,$$

$$2\vartheta_{00}(2\tau)^2 = \vartheta_{00}(\tau)^2 + \vartheta_{0\frac{1}{2}}(\tau)^2.$$

Lecture 11

Hecke Operators

11.1 Let S and S' be two sets. A *correspondence* between S and S' is a subset $Z \subset S \times S'$. For example, Z could be the graph Γ_f of a map $f : S \to S'$. One can view Z as a multi-valued map from S to S' as follows. Take $s \in S$, and consider the intersection $\{s\} \times S' \cap Z$. Then take the image $Z(s)$ of this set under the second projection $pr_{S'} : S \times S' \to S'$. This is called the image of s under Z. We will assume that Z is a *finite correspondence* meaning that each set $Z(s)$ is finite (maybe empty). Clearly, Z is completely determined by its images. When $Z = \Gamma_f$ is the graph correspondence we obtain the usual value of the map on s. The analog of compositions of maps for correspondences is the following operation. Let $Z' \subset S' \times S''$ be another correspondence. Set

$$Z' \circ Z = pr_{13}((Z \times S'') \times (S \times Z')),$$

where p_{13} is the projection map $S \times S' \times S'' \to S \times S''$. It is called the *composition of the correspondences* Z and Z'. It is easy to see that the value of $Z' \circ Z$ at $s \in S$ is equal to the union $\cup_{s' \in Z(s)} Z'(s')$. In particular, when Z' is a function $f : S' \to S''$ (identified with its graph), we have $f \circ Z(s) = f(Z(s))$.

One can view any finite correspondence as a map $f : S \to \mathcal{P}(S')_{fin}$, where $\mathcal{P}(S')_{fin}$ is the finite Boolean of the set S', i.e. the set of finite subsets of S'. Using the characteristic function of a set we can identify $\mathcal{P}(S')_{fin}$ with the set of functions with finite support which take values 0 or 1. Now let K be any commutative ring. For any set X denote by K^X the ring of functions $X \to K$ with finite support. Its basis consists of characteristic functions $\chi_{\{x\}}$ and can be identified with elements of X. This allows us to write its elements as finite linear combinations of elements of X with coefficients in K. We have encountered this notion when we defined divisors on Riemann surfaces. By including $0, 1$ in K we can identify any correspondence $Z \subset S \times S'$ with a function $Z : S \to K^{S'}$. We have

$$Z(s) = \sum_{s' \in Z(s)} 1 \cdot s'. \tag{11.1}$$

Now we extend the notion of a correspondence by making the following:

Definition. Let K be a commutative ring and let S, S' be two sets. A *finite K-correspondence* on the set $S \times S'$ is a function $Z : S \to K^{S'}$.

We have a natural function

$$\deg : K^S \to K, \quad \phi \to \sum_{s \in s} \phi(s) \tag{11.2}$$

which is an analog of the degree of a divisor. If Z is a correspondence as in (11.1), then $\deg(Z(s)) = \#Z(s)$, where Z is considered as a multivalued map.

Since $K^{S'}$ is an abelian group with respect to the operation of addition of functions, we see that the set of finite K-correspondences on $S \times S'$ forms an abelian group. In particular, take $S = S'$ and denote the set of finite correspondences on $S \times S$ by $\mathrm{Corr}(S)_K$. It has two operations: an addition and the composition. The latter generalizes the operation of composition of correspondences from above. For any $f : S \to K^S$ denote by $\tilde{f}$ its extension to a map $K^S \to K^S$ defined uniquely by additivity:

$$\tilde{f}(\sum_{s \in S} a_s s) = \sum_{s \in S} a_s f(s).$$

For any $f, g \in \mathrm{Corr}(S)_K$ we set

$$f \circ g(s) = \tilde{f}(g(s)). \tag{11.3}$$

We leave to the reader to verify that this defines a structure of an associative ring on $\mathrm{Corr}(S)_K$. It is called *ring of finite K-correspondences* on the set S with values in K. In fact, it is obviously an algebra over K (since K^S is a K-algebra). When $K = \mathbb{Z}$ we skip the subscript in the notation.

Let Z be a finite K-correspondence on $S \times S'$. Any function $\phi : S' \to R$ with values in a K-algebra R can be extended by additivity to a function $\tilde{\phi} : K^{S'} \to R$ using the formula

$$\tilde{\phi}(\sum_{s' \in S'} a_{s'} s') = \sum_{s' \in S'} a_{s'} \phi(s').$$

This allows us to define the *inverse transform* of ϕ under the correspondence Z:

$$Z^*(\phi) = \tilde{\phi} \circ Z.$$

If $Z(s) = \sum_{s' \in S'} a_{s'} s'$, then

$$Z^*(\phi)(s) = \sum_{s' \in S'} a_{s'} \phi(s'). \tag{11.4}$$

Example 11.1. Let $f : X \to Y$ be a holomorphic map of compact Riemann surfaces. Define a function $r : X \to \mathbb{Z}$ by $r(x) =$ ramification index of f at x. Recall that this means that, taking a local parameter t at $f(x)$, the function $t \circ f$ has a zero at x of order $r(x)$. Consider f^{-1} as a correspondence on $Y \times X$ given by the inverse f^{-1}. More precisely, $f^{-1} = \{(y, x) \in Y \times X : f(x) = y\}$. Then

$$(f^{-1})^*(r)(y) = \sum_{f(x)=y} r(x) = n$$

does not depend on y and is equal to the degree of the map f.

11.2 We will be interested in the following situation. Let S be the set $\mathcal{L}$ of lattices in $\mathbb{C}$. Define a correspondence on $\mathcal{L}$ as follows

$$T(n) = \{(\Lambda, \Lambda') \in \mathcal{L} \times \mathcal{L} : \Lambda' \subset \Lambda, [\Lambda : \Lambda'] = n\}. \tag{11.5}$$

We take the natural inclusion of $T(n)$ in the product $\mathcal{L} \times \mathcal{L}$.

Lemma 11.1. *Let $\mathcal{A}'_n$ be the set of integral matrices $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $ad = n$ and $0 \le b < d$. Fix a basis (ω_1, ω_2) of a lattice Λ. For any $A \in \mathcal{A}'_n$ denote by $\Lambda(A)$ the sublattice $\mathbb{Z}(a\omega_2 + b\omega_1) + \mathbb{Z}d\omega_2$. Then the map $A \to \Lambda(A)$ is a bijection from the set $\mathcal{A}'_n$ onto the set $T(n)(\Lambda)$.*

Proof. Note that the set $\mathcal{A}'_n$ differs from the set $\mathcal{A}_n$ used in the previous lecture only by abandoning the primitivity property of the matrix. As in the proof of Lemma 2 in this lecture, we show that any integral matrix with determinant n can be transformed to a unique $A \in \mathcal{A}'_n$ by integral row transformations. This shows that any sublattice $\Lambda' \in T(n)(\Lambda)$ has a unique basis of the form $\omega'_1 = d\omega_1, \omega'_2 = b\omega_1 + a\omega_2$, and hence is equal to a unique $\Lambda(A)$ with $A \in \mathcal{A}'_n$. □

Corollary 11.1.

$$\deg T(n)(\Lambda) = \sum_{d|n} d. \tag{11.6}$$

For any nonzero complex number c consider the correspondence R_c on $\mathcal{L}$ defined by the function $\Lambda \to c\Lambda$.

Lemma 11.2. *The correspondences $T(n)$ and R_c form a subring of the ring* $\mathrm{Corr}(\mathcal{L})$. *They satisfy the following relations:*

(i) $T(m) \circ T(n) = T(mn)$ *if* $(m, n) = 1$;

(ii) $T(p^n) \circ T(p) = T(p^{n+1}) + pT(p^{n-1}) \circ R_p$, *where p is prime;*

(iii) $T(n) \circ R_a = R_a \circ T(n)$;

(iv) $R_a \circ R_b = R_{ab}$.

Proof. The last two properties are obvious. To prove (i) we observe that

$$T(n) \circ T(m) = \{(\Lambda, \Lambda'') \in \mathcal{L} \times \mathcal{L} : [\Lambda : \Lambda'] = n, [\Lambda' : \Lambda''] = m \quad \text{for some } \Lambda'\}.$$

If $(m, n) = 1$, the finite abelian group Λ/Λ'' contains a unique subgroup of order m. Its pre-image in Λ must be Λ'. This shows that

$$T(n) \circ T(m) = \{(\Lambda, \Lambda'') \in \mathcal{L} \times \mathcal{L} : [\Lambda : \Lambda''] = mn\} = T(mn).$$

This proves (i). We have

$$T(p^n) \circ T(p)(\Lambda) = \sum_{[\Lambda:\Lambda'] = p^{n+1}} a_{\Lambda'} \Lambda',$$

where

$$a_{\Lambda'} = \#\{\Lambda'' : [\Lambda : \Lambda''] = p, [\Lambda'' : \Lambda'] = p^n\}.$$

Now

$$T(p^{n+1})(\Lambda) = \sum_{[\Lambda:\Lambda']=p^{n+1}} \Lambda',$$

$$pT(p^{n-1}) \circ R_p(\Lambda) = pT(p^{n-1})(p\Lambda) = p \sum_{[\Lambda:\Lambda']=p^{n+1}} b_{\Lambda'}\Lambda',$$

where

$$b_{\Lambda'} = \begin{cases} 1 & \text{if } \Lambda' \subset p\Lambda. \\ 0 & \text{if } \Lambda' \not\subset p\Lambda. \end{cases} \tag{11.7}$$

Comparing the coefficients at Λ' we have to show that

(a) $a_{\Lambda'} = 1$ if $\Lambda' \not\subset p\Lambda$;

(b) $a_{\Lambda'} = p+1$ if $\Lambda' \subset p\Lambda$.

Recall that $a_{\Lambda'}$ counts the number of Λ'' of index p in Λ which contain Λ' as a sublattice of index p^n. We have $p\Lambda \subset \Lambda'' \subset \Lambda$. Thus the image $\bar{\Lambda}'$ of Λ'' in $\Lambda/p\Lambda$ is a subgroup of index p. In case (a) the image of Λ' in the same group is a non-trivial group contained in $\bar{\Lambda}'$. Since the order of $\bar{\Lambda}$ is equal to p, they must coincide. This shows that Λ'' in $\Lambda/p\Lambda$ is defined uniquely, hence there is only one such Λ'', i.e. $a_{\lambda'} = 1$.

In case (b), $\bar{\Lambda}''$ could be any subgroup of order p in $\Lambda/p\Lambda$. The number of subgroups of order p in $(\mathbb{Z}/p\mathbb{Z})^2$ is obviously equal to $p+1$. □

Corollary 11.2. *The correspondences $T(n)$ are polynomials in $T(p)$'s and R_p's, where p runs through the set of prime numbers. In particular, $T(n)$'s and R_n's generate a commutative subring H of* Corr.

Definition. The subring H of Corr generated by the correspondences $T(n)$ and R_n is called the *Hecke ring* of $\Gamma(1)$.

11.3 Consider a function f on $\mathcal{L}$; using definition (11.4) , we have

$$T(n)^*(f)(\Lambda) = \sum_{[\Lambda:\Lambda']=n} f(\Lambda'). \tag{11.8}$$

We apply it to the case when f is defined by a modular form of weight $2k$ with respect to Γ. Choose a basis (ω_1, ω_2) of Λ with $\tau = \omega_2/\omega_1 \in \mathcal{H}$. Then set

$$\tilde{f}(\Lambda) = (\omega_1)^{-2k} f(\tau). \tag{11.9}$$

This definition is independent of the choice of the basis as above. In fact, if $\omega_2' = \alpha\omega_2 + \beta\omega_1, \quad \omega_1' = \gamma\omega_2 + \delta\omega_1$ with some $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$, we have

$$(\omega_1')^{-2k} f(\omega_2'/\omega_1') = (\gamma\omega_2 + \delta\omega_1)^{-2k} f(\frac{\alpha\omega_2 + \beta\omega_1}{\gamma\omega_2 + \delta\omega_1}) =$$

$$\omega_1^{-2k}(\gamma\tau + \delta)^{-2k} f(M \cdot \tau) = \omega_1^{-2k} f(\tau).$$

This function satisfies the property

$$f(a\Lambda) = a^{-2k}\tilde{f}(\Lambda). \tag{11.10}$$

Conversely given a function $\tilde{f}$ on $\mathcal{L}$ satisfying this property we can set $f(\tau) = \tilde{f}(\mathbb{Z}+\mathbb{Z}\tau)$. Then

$$f(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = \tilde{f}(\mathbb{Z}+\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = (\gamma\tau+\delta)^{-2k}f((\gamma\tau+\delta)\mathbb{Z}+(\alpha\tau+\beta)\mathbb{Z}) =$$

$$(\gamma\tau+\delta)^{-2k}\tilde{f}(\mathbb{Z}+\tau\mathbb{Z}) = (\gamma\tau+\delta)^{-2k}f(\tau).$$

By property (iii) of Lemma 1, we obtain that $T(n)$ leave the set of functions $\tilde{f}$ on $\mathcal{H}$ satisfying (11.6) invariant.

Let $\mathcal{F}_k$ be the space of functions on $\mathcal{L}$ of the form $\tilde{f}$ where $f \in \mathcal{M}(\Gamma(1))_k$.

Theorem 11.1. *For any positive integer n and any non-negatve integer k,*

$$T_n(\mathcal{F}_k) \subset \mathcal{F}_k.$$

Proof. Let $f \in \mathcal{M}(\Gamma(1))_k$ and $\tilde{f} \in \mathcal{F}_k$. We know that

$$T(n)\tilde{f}(c\Lambda) = \sum_{[\Lambda:\Lambda']=n}\tilde{f}(c\Lambda') = c^{-2k}\sum_{[\Lambda:\Lambda']=n}\tilde{f}(\Lambda').$$

This shows that $T(n)\tilde{f} = \tilde{g}$, where g is a function on $\mathcal{H}$ satisfying $g(\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)\tau) = (\gamma\tau+\delta)^{-2k}g(\tau)$ for any $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \Gamma(1)$. We have to check that g is a holomorphic function on $\mathcal{H}$ and at infinity. Applying Lemma 2, we have

$$g(\tau) = T(n)\tilde{f}(\mathbb{Z}+\tau\mathbb{Z}) = \sum_{A\in\mathcal{A}'_n}\tilde{f}((a\tau+b)\mathbb{Z}+d\mathbb{Z}) = \sum_{A\in\mathcal{A}'_n}d^{-2k}f(\frac{a\tau+b}{d}).$$

Thus

$$g(\tau) = \sum_{A\in\mathcal{A}'_n}d^{-2k}f(\frac{a\tau+b}{d}) = \sum_{A\in\mathcal{A}'_n}f|_kA. \tag{11.11}$$

Clearly, g is holomorphic on $\mathcal{H}$ as soon as f is holomorphic. It remains to find its behavior at infinity. Let

$$f = \sum_{m=0}^{\infty}c_m e^{2\pi i m\tau}$$

be the Fourier expansion of f at ∞. Then

$$g = \sum_{A\in\mathcal{A}'_n}d^{-2k}(\sum_{m=0}^{\infty}c_m e^{2\pi i m(a\tau+b)/d}).$$

Observe that

$$\sum_{0\le b<d}e^{2\pi i m b/d} = \begin{cases} d & \text{if } d|m,\\ 0 & \text{otherwise.}\end{cases} \tag{11.12}$$

This gives

$$g = \sum_{ad=n,a\geq 1} d^{-2k+1}\left(\sum_{m'\in\mathbb{Z}} c_{m'd}e^{2\pi i m' a\tau}\right) = \sum_{ad=n,a\geq 1} d^{-2k+1}\left(\sum_{m'\in\mathbb{Z}} c_{m'd}q^{am'}\right).$$

Now let $m = am'$ we have $d = n/a$, so we can rewrite it as follows:

$$g = \sum_{m\in\mathbb{Z}} q^m\left(\sum_{a|(n,m),a\geq 1} (n/a)^{-2k+1}c_{mn/a^2}\right) = \sum_{m\in\mathbb{Z}} b_m q^m. \tag{11.13}$$

Since $c_k = 0$ for $k < 0$ we get $b_m = 0$ for $m < 0$, so that g is holomorphic at ∞. Also we see that, if $c_0 = 0$, then $b_0 = 0$, i.e. $T(n)$ maps a parabolic form to a parabolic form. □

From now on we shall identify $\mathcal{M}(\Gamma(1))_k$ with $\mathcal{F}_k$. So we have linear operators $T(n)$ in each space $\mathcal{M}(\Gamma(1))_k$ which also leave the subspace $\mathcal{M}(\Gamma(1))_k^0$ invariant.

To avoid denominators in the formulas one redefines the action of operators $T(n)$ on the vector space $\mathcal{M}(\Gamma(1))_k$ by setting

$$T(n)f = n^{2k-1}T(n)^*(f) = n^{2k-1}\sum_{A\in\mathcal{A}'_n} f|_k A \tag{11.14}$$

These operators are called the *Hecke operators.* Let

$$T(n)\left(\sum_{m=0}^{\infty} c_m q^m\right) = \sum_{m=0}^{\infty} b_m q^m. \tag{11.15}$$

It follows from (11.9) that for prime $n = p$, we have

$$b_m = \begin{cases} c_{pm} & \text{if } p \not| m, \\ c_{mp} + p^{2k-1}c_{m/p} & \text{if } p|m. \end{cases} \tag{11.16}$$

Also, for any n,

$$b_0 = \sigma_{2k-1}(n)c_0, \quad b_1 = c_n. \tag{11.17}$$

11.4 We will be interested in common eigenfunctions of operators $T(n)$, that is, functions $f \in \mathcal{M}_k(\Gamma(1)$ satisfying

$$T(n)f = \lambda(n)f \quad \text{for all } n.$$

Lemma 11.3. *Suppose f is a non-zero modular form of weight $2k$ with respect to $\Gamma(1)$ which is a simultaneous eigenfunction for all the Hecke operators and let $\sum c_n q^n$ be its Fourier expansion. Then $c_1 \neq 0$ and*

$$T(n)f = \frac{c_n}{c_1}f.$$

Moreover, if $c_0 \neq 0$ we have

$$c_n/c_1 = \sigma_{2k-1}(n).$$

Conversely, if $c_0 \neq 0$ and the coefficients c_n satisfy the previous equality, then f is a simultaneous eigenfunction of Hecke operators.

Proof. In the notation of (11.11) we have

$$b_m = \lambda(n)c_m, \quad \forall m, n.$$

If $c_1 = 0$, then $b_1 = \lambda(n)c_1 = 0$. But, by (11.12) we have $c_n = b_1$. This shows that $c_n = 0$ for all $n \neq 0$. Thus f is constant, contradicting the assumption. So, $c_1 \neq 0$, and $c_n = b_1 = \lambda(n)c_1$ implies

$$\lambda(n) = c_n/c_1.$$

If $c_0 \neq 0$, we use (11.12) to get $b_0 = \sigma_{2k-1}(n)c_0 = \lambda(n)c_0$. This gives

$$\lambda(n) = \sigma_{2k-1}(n).$$

□

Corollary 11.3. *Keep the notation from the previous lemma. Assume f is normalized so that $c_1 = 1$. Then*

$$c_m c_n = c_{mn} \quad \textit{if } (m, n) = 1,$$

$$c_p c_{p^n} = c_{p^{n+1}} + p^{2k-1} c_{p^{n-1}}$$

where p is prime and $n \geq 1$.

Proof. The coefficient c_n is equal to the eigenvalue of $T(n)$ on $\mathcal{M}_k(\Gamma(1))$. Obviously $c_m c_n$ is the eigenvalue of $T(n)T(m)$ on the same space. Now we apply assertion (ii) taking into account that the correspondence R_p acts as multiplication by p^{-2k} and remember that we have introduced the factor n^{2k-1} in the definition of the operator $T(n)$. □

Example 11.2. Let $E_k(\tau)$ be the Eisenstein modular form of weight $2k$, $k \geq 2$. We have seen in (6.21) that its Fourier coefficients are equal to

$$c_n = \frac{2(2\pi)^k \sigma_{2k-1}(n)}{(k-1)!}, \quad n \geq 1,$$

$$c_0 = 2\zeta(k) = \frac{2^{2k-1}\pi^k B_k}{(2k)!}.$$

Thus $c_n = c_1 \sigma_{2k-1}(n)$, and therefore $E_k(\tau)$ is a simultaneous eigenvalue of all the Hecke operators.

Corollary 11.4.

$$\sigma_{2k-1}(m)\sigma_{2k-1}(m) = \sigma_{2k-1}(mn) \quad \textit{if } (m, n) = 1,$$

$$\sigma_{2k-1}(p)\sigma_{2k-1}(p^n) = \sigma_{2k-1}(p^{n+1}) + p^{2k-1}\sigma_{2k-1}(p^{n-1}),$$

where p is prime and $n \geq 1$.

Example 11.3. Let $f = \Delta$. Since f spans the space of cusp forms of weight 6 and this space is $T(n)$-invariant for all n, we obtain that f is a simultaneous eigenfunction for all the Hecke operators. We have

$$\Delta = q\prod_{m=1}^{\infty}(1-q^m)^{24} = \sum_{m=1}^{\infty}\tau(n)q^n.$$

We see that the Ramanujan function $n \to \tau(n)$ satisfies

$$\tau(m)\tau(n) = \tau(mn) \quad \text{if } (m,n) = 1, \tag{11.18}$$

$$\tau(p)\tau(p^n) = \tau(p^{n+1}) + p^{11}\tau(p^{n-1}) \quad \text{if } p \text{ is prime and } n \geq 1, \tag{11.19}$$

Recall from Number Theory that a function $f : \mathbb{N} \to \mathbb{C}$ is called *multiplicative* if $f(mn) = f(m)f(n)$ if $(m,n) = 1$. It follows from above that the Fourier coefficients c_n of any modular form which is a simultaneous eigenfunction of all the Hecke operators and normalized with the condition that $c_1 = 1$ define a multiplicative function. Example 2 provides the function $\sigma_{2k-1}(n)$. Of course, the fact that is multiplicative is well-known and can be found in any text-book in number theory. The fact that the Ramanujan function is multiplicative is not easy, and does not follow immediately from its definition.

11.5 One can say more about the Fourier coefficients of a cuspidal modular form which is a simultaneous eigenfunction of Hecke operators. This is done by introducing an inner product in the space $\mathcal{M}(\Gamma(1))_k^0$.

Definition. Let f, g be two parabolic modular forms of weight k with respect to Γ. Let $\mathcal{D} \subset \mathcal{H}$ be the modular figure. The formula

$$\langle f, g\rangle = \frac{i}{2}\int_{\mathcal{D}} f(\tau)\overline{g(\tau)}\text{Im }(\tau)^{2k-2}d\tau d\bar{\tau} = \int_{\mathcal{D}} f(x+iy)\overline{g(x+iy)}y^{2k-2}dxdy$$

defines a Hermitian inner product in the space $\mathcal{M}_k(\Gamma)^0$. It is called the *Petersson inner product* .

Observe that the integral converges because at the cusps $f(\tau)\overline{g(\tau)}$ behaves like $O(e^{-cy})$ for some $c > 0$. This is why we have to restrict ourselves to parabolic forms only.

Lemma 11.4. *For any* $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{R})$ *with* $\det A > 0$,

$$\langle f|_k A, g_k A\rangle = \langle f, g\rangle.$$

Proof. We have

$$\langle f|_k A, g|_k A\rangle = \frac{i}{2}\int_{\mathcal{D}} f(A\tau)(c\tau+d)^{-2k}\overline{g(A\tau)(c\tau+d)^{-2k}}\text{Im }(\tau)^{2k-2}d\tau d\bar{\tau} =$$

$$\frac{i}{2}\int_{\mathcal{D}} f(A\tau)\overline{g(A\tau)}|c\tau+d|^{-4k}\text{Im }(\tau)^{2k-2}d\tau d\bar{\tau} =$$

$$\frac{i}{2}\int_{\mathcal{D}} f(A\tau)\overline{g(A\tau)}\text{Im }(A\tau)^{2k-2}d(A\tau)d(\overline{A\tau}) =$$

$$\frac{i}{2}\int_{A(\mathcal{D})} f(\tau)\overline{g(\tau)}\text{Im }(\tau)^{2k-2}d\tau d\bar{\tau}.$$

In particular, when we take $A \in \Gamma$ we get that in the definition of the inner product we can integrate over $A(\mathcal{D})$ which is another fundamental domain for Γ. In fact, this computation shows that for any measurable subset Q of $\mathcal{H}$ and any $A \in \Gamma$, we have

$$\int_{\mathcal{D}} f(\tau)\overline{g(\tau)}\text{Im }(\tau)^{2k-2}d\tau d\bar{\tau} = \int_{A(\mathcal{D})} f(\tau)\overline{g(\tau)}\text{Im }(\tau)^{2k-2}d\tau d\bar{\tau}.$$

This allows one to view $\langle f, g\rangle$ as the integral of the differential form

$$\omega = \frac{i}{2}f(\tau)\overline{g(\tau)}\text{Im }(\tau)^{2k-2}d\tau d\bar{\tau}$$

over $\mathcal{H}/\Gamma$. Since for any $A \in \text{GL}(2,\mathbb{R})$ with $\det A > 0$, the set $A(\mathcal{D})$ is another fundamental domain for Γ, the see that the last integral in (11.14) is also equal to the integral of ω over $\mathcal{H}/\Gamma$. Hence, it is equal to $\langle f, g\rangle$. □

Theorem 11.2. *The Hecke operators are Hermitian operators on the space $\mathcal{M}_k(\Gamma(1))^0$ with respect to the Petersson inner product.*

Proof. We have to check that

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

In view of Lemma 2 it is enough to check it when $n = p$ is prime. We have

$$\langle T(p)f, g\rangle = \sum_{A\in\mathcal{A}'_p}\langle f|_k, g\rangle = \sum_{A\in\mathcal{A}'_p}\langle f, g|_k A^{-1}\rangle.$$

Note that for any $A \in \mathcal{A}'_p$ we have pA^{-1} is an integral matrix of determinant p. Thus we can write as MA' for some $M \in \Gamma(1)$ and $A \in \mathcal{A}'_p$. This gives us that

$$\langle T(p)f, g\rangle = \sum_{A'\in\mathcal{A}'_p}\langle f, g|_k MA'\rangle = \sum_{A'\in\mathcal{A}'_p}\langle f, g|_k A'\rangle = \langle f, T(p)g\rangle.$$

□

Corollary 11.5. *The space of parabolic modular forms $\mathcal{M}_k(\Gamma(1)^0$ admits an orthonormal basis which consists of eigenfunctions of all the Hecke operators $T(n)$.*

Proof. This follows from a well-known fact in linear algebra: a finite-dimensional Hilbert space admits an orthonormal basis of eigenvalues of any set of commuting normal operators. □

Corollary 11.6. *Let f be a cuspidal modular form which is a simultaneous eigenfunction for Hecke operators and let c_n be its Fourier coefficients. Then c_n/c_1 are totally real algebraic numbers.*

Proof. The numbers c_n/c_1 are eigenvalues of a Hermitian operator. They must be real. To prove the algebraicity, let us consider the set $M_k(\mathbb{Z})$ of modular form of weight k for $\Gamma(1)$ with integral Fourier coefficients. Examples of such forms are the normalized Eisenstein series $E_k^* = \frac{(k-1)!}{2(2\pi)^k}E_k(\tau)$. This set is a $\mathbb{Z}$-module and invariant with respect to Hecke operators (as it follows from the formula for the Fourier coefficients of transformed functions). We can find a basis in this module which is a subset of monomials $(E_2^*)^a(E_3^*)^b, a+b=2k$. Thus the egenvalues of $T(n)$ being the roots of the characteristic polynomial with integer coefficients must be algebraic numbers. □

Exercises

11.1 Let S be the set of finite-dimensional vector spaces over a finite field $\mathbb{F}_q$ of q elements. For each positive integer n consider the correspondence $T(n) = \{(V,W) : W \subset V, \dim V/W = n\}$. Show that the operators $T(n)$ generate a commutative subring of the ring of correspondences $\mathrm{Corr}(S)$. Show that $T(n)T(m) = k(n,m)T(n+m)$, where $k(n,m) = \#G(n,n+m)(\mathbb{F}_q)$ ($G(n,n+m)$ is the Grassmann variety of linear subspaces of dimension n in $\mathbb{F}_q^{n+m}$).

11.2 Show that the Hecke operators $T(n)$ together with operators R_c generate a commutative algebra H over $\mathbb{C}$ which is freely generated by the operators $T(p)$ and R_p, where p is prime. The algebra H is called the *Hecke algebra* of the group $\Gamma(1)$.

11.3 Show that the vector subspace of $\mathrm{Corr}(\mathcal{L})_{\mathbb{Q}}$ spanned by the Hecke operators $T(n)$ is a subalgebra of $\mathrm{Corr}(\mathcal{L})_{\mathbb{Q}}$.

11.4 Consider the formal infinite series $\sum_{n=1}^{\infty} T(n)n^{-s}$ with coefficients in the Hecke algebra H of $\Gamma(1)$. Show that

$$\sum_{n=1}^{\infty} T(n)n^{-s} = \prod_{p \text{ prime}} [1 - T(p)p^{-s} + R_p p^{1-2s}]^{-1}.$$

11.5 Show that for any lattice L in $\mathbb{C}$ and a complex number s with Re $s > 1$, we have

$$\sum_{n=1}^{\infty} \#T(n)(L)n^{-s} = \zeta(s)\zeta(s-1),$$

where $\zeta(s)$ is the Riemann zeta function.

11.6 Let Γ be a subgroup of finite index in $\Gamma(1)$ and Δ be a subsemigroup of the group $\mathrm{GL}(2,\mathbb{Q})^+$ of rational 2×2-matrices with positive determinant which contains Γ and satisfies the property that, for any $\alpha \in \Delta$, $\alpha \cdot \Gamma \cdot \alpha^{-1} \cap \Gamma$ is of finite index in Γ (e.g. $\Gamma = \Gamma(1)$ and $\Delta = \{\sigma \in M_2(\mathbb{Z}) : \det \sigma > 0\}$). Let $H(\Gamma, \Delta)$ be the free abelian group with the basis formed by the double cosets $[\sigma] = \Gamma\sigma\Gamma, \sigma \in \Delta$.

(i) Show that, for any $\sigma \in \Delta$, the double coset $[\sigma]$ is equal to a finite union of right cosets $\Gamma\sigma_i$, where $\sigma_i \in \Delta$.

(ii) If $[\sigma] = \cup\Gamma_{i\in I}\sigma_i, [\sigma'] = \cup\Gamma_{j\in J}\sigma'_j$, let $c^{\alpha}_{\sigma,\sigma'}$ denote the number of pairs $(i,j) \in I \times J$ such that $\Gamma\sigma_i\sigma'_j = \Gamma\alpha$ for a fixed $\alpha \in \Delta$. Show that the formula

$$[\sigma]\cdot[\sigma'] = \sum_{\alpha:\Gamma\alpha\Gamma\subset\Gamma\sigma\Gamma\sigma'\Gamma} c^{\alpha}_{\sigma,\sigma'}[\alpha]$$

togeher with the addition law defines a stucture of an associative ring on $H(\Gamma, \Delta)$. This ring is called the *Hecke ring* of (Γ, Δ).

(iii) Let ι be the adjugation involution in $M_2(\mathbb{Z})$ (i.e. $\iota(M)M = \det(M)I_2$).Assume that Δ is invariant with respect to ι. Show that $H(\Gamma, \Delta)$ is commutative if and only if $[\iota(\sigma)] = [\sigma]$ for any $\sigma \in \Delta$.

11.7 Let S be the set of right cosets $\Gamma \cdot \sigma, \sigma \in \Delta$. For any $\sigma \in \Delta$ set $Z_\sigma = \{(\Gamma\alpha, \Gamma\beta) \in S \times S : \Gamma \cdot \beta \subset \Gamma\sigma\Gamma\alpha\}$.

(i) Show that Z_σ depends only on the double coset $[\sigma]$ of σ, so we can denote it by $Z_{[\sigma]}$.

(iii) Show that $[\sigma] \to Z_{[\sigma]}$ defines a homomorphism of the Hecke ring $H(\Gamma, \Delta)$ to the ring $\mathrm{Corr}^{\mathrm{f}}(S)$ of finite correspondences on the set S.

11.8 For any $\sigma \in \Delta$ let $\Gamma_\sigma = (\sigma\Gamma\sigma^{-1}) \cap \Gamma$. Let $\pi : \mathcal{H}/\Gamma_\sigma \to \mathcal{H}/\Gamma$ correspond to the natural inclusion $\Gamma_\sigma \subset \Gamma$ and let $\pi_\sigma : \mathcal{H}/\Gamma_\sigma \to \mathcal{H}/\Gamma$ be the composition of an isomorphism $\mathcal{H}/\sigma^{-1}\Gamma\sigma \cong \mathcal{H}/\Gamma$ induced by the Möebius transformation $\tau \to \sigma \cdot \tau$ and the natural projection map $\mathcal{H}/\Gamma_\sigma \to \mathcal{H}/\sigma^{-1}\Gamma\sigma$.

(i) Show that the composition of the correspondences $\pi \circ \pi_\sigma^{-1}$ defines a finite correspondence C_σ on $\mathcal{H}/\Gamma$. Here π_σ^{-1} is defined as in Example 1 from the lecture.

(ii) Show that C_σ depends only on the double coset $\Gamma\sigma\Gamma$. Denote it by $C_{[\sigma]}$.

(iii) Show that $Z_{[\sigma]} \to C_{[\sigma]}$ defines a homomorphism from the Hecke ring $H(\Gamma, \Delta)$ to the ring $\mathrm{Corr}(\mathcal{H}/\Gamma)$.

11.9 Consider the Hecke ring $H(\Gamma(1), M_2(\mathbb{Z})^+)$. For any pair of positive integers a, b with $a|b$ denote by $T(a, b)$ the double coset of the matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$. For any positive integer n set $T(n) = \sum_{ab=n} T(a, b)$.

(i) Show that $T(a, b)T(a', b') = T(aa', bb')$ if $(b, b') = 1$.

(ii) Show that $T(p^k, p^m) = T(p, p)T(p^{k-1}, p^{m-1})$, where p is prime.

(iii) Show that there exists an isomorphism of algebras $H(\Gamma(1), M_2(\mathbb{Z})^+) \otimes \mathbb{C}$ and the Hecke algebra H of $\Gamma(1)$ as defined in Exercise 11.2. Under this isomorphism each element $T(n)$ is mapped to the Hecke operator $T(n)$, and each element $T(a, a)$ is mapped to the operator R_a.

11.10 Let $\Delta(N) \subset M_2(\mathbb{Z})^+$ be the set of integral matrices with positive determinant prime to N. Prove that the map $\Gamma(N)\sigma\Gamma(N) \to \Gamma(1)\sigma\Gamma(1)$ defines an isomorphism from $H(\Gamma(N), \Delta(N))$ onto $H(\Gamma(1), M_2(\mathbb{Z})_0{}^+)$.

11.11 Let $N > 1$ and A be a fixed subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$. Let Δ be the semigroup of matrices $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})^+$ such that $(\det \sigma, N) = 1, N|c$ and the image of a in $\mathbb{Z}/N\mathbb{Z}$ belongs to A. Let Γ be the group of invertible elements in Δ. For example, $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$. Consider the Hecke ring $H(\Gamma, \Delta)$. For any $d \in (\mathbb{Z}/N\mathbb{Z})^*$ let σ_d denote any representative of $\left(\begin{smallmatrix} d & 0 \\ 0 & d^{-1} \end{smallmatrix}\right)$ in $\mathrm{SL}(2, \mathbb{Z})$. For any pair of positive integers a, b such that $a|b$ and $(b, N) = 1$, denote by $T(a, b)$ the double coset of the matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$. For any positive integer n let $T(n)$ be the sum of the double cosets $Z_{[\sigma]}$, where $\det \sigma = n$. Show that

(i) any $Z_\sigma \in H(\Gamma, \Delta)$ can be uniquely expressed as the product $T(m)T(a, b)$, where each prime factor of m divides N (we write it as $m|N^\infty$);

(ii) if $(m, n) = 1$ or $m|N^\infty$ or $n|N^\infty$, then $T(mn) = T(m)T(n)$;

(iii) $H(\Gamma, \Delta)$ is a polynomial ring over $\mathbb{Z}$ in the variables $T(p, p)$ for all primes $p \not| N$ and $T(p)$ for all prime p;

(iv) $H(\Gamma, \Delta) \otimes \mathbb{Q}$ is generated as an algebra over $\mathbb{Q}$ by $T(n)$ for all n;

(v) the map $H(\Gamma(1), M_2(\mathbb{Z})^+) \to H(\Gamma, \Delta)$ defined by sending $T(p)$ to $T(p)$ if p is any prime, $T(p,p)$ to $T(p,p)$ if p is a prime with $p \not| N$, and sending $T(p,p)$ to zero if p is prime with $p|N$, is a surjective homomorphism of rings;

(vi) $H(\Gamma, \Delta)$ is a commutative ring.

11.12 Define the action of $[\sigma] \in H(\Gamma, \Delta)$ on $\mathcal{M}_k(\Gamma)$ by $f|[\sigma] = \det(\sigma)^{k-1} \sum_i f|_k\sigma_i$, where $[\sigma] = \cup_i \Gamma\sigma_i$ and $f|_k\sigma_i$ is defined as in (6.5) (which applies to not necessary unimodular matrices).

(i) Show that, extending by linearity, this defines a linear representation $T \to T^*$ of the ring $H(\Gamma, \Delta)$ in $\mathcal{M}_k(\Gamma)$ and in $\mathcal{M}_k(\Gamma)^0$.

(ii) Let (Γ, Δ) be as in Exercise 11.11. Show that, for any $n > 0$ and $f \in \mathcal{M}_k(\Gamma)$,

$$T(n)^*(f) = \sum_{ad=n,(a,N)=1,0\le b<d} f|_k\sigma_a \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

11.13 Let us identify the set of points of $X_0(N)' = \mathcal{H}/\Gamma_0(N)$ with the set of isomorphism classes of pairs (E, H), where E is an elliptic curve and H is a cyclic subgroup of order N of its group of N-torsion points (see Theorem 8.6). Let p be a prime number not dividing N and let $T(p)$ be the Hecke correspondence on $X_0(N)'$ (see Exercise 11.7). Show that $T(p)((E,H)) = \{(E/A_i, A_i + H/A_i), i = 0, \dots, p\}$, where $A_0, \dots, A_p$ is the set of cyclic subgroups of order p in E.

Lecture 12

Dirichlet Series

12.1 A *Dirichler series* is an infinite series of the form

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where s is a complex number. It absolutely converges for Re $s > 1 + c$, where

$$a_n = O(n^c).$$

An absolutely convergent Dirichlet series in a domain D is a holomorphic function in D. The most notorious example of a Dirichlet series is the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

It converges for Re $s > 1$. We will be interested in Dirichlet series for which the coefficients a_n are the Fourier coefficients of a modular form.

Let $f \in \mathcal{M}(\Gamma)_k$ and let

$$f = \sum_{n=0}^{\infty} a_n e^{2\pi i n\tau/h} \tag{12.1}$$

be its Fourier series at ∞. For any complex number s we define the formal expression

$$Z_f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \sum_{n=1}^{\infty} a_n e^{-s\log n} \tag{12.2}$$

and call it the *Dirichlet series associated to* f. Let us first invesigate the convergence of this series.

Lemma 12.1. *Let* $f \in \mathcal{M}_k(\Gamma)$. *Then* f *is parabolic if and only if*

$$|f(x+iy)| \leq Cy^{-k} \tag{12.3}$$

for some constant C *independent of* x.

Proof. Let $\phi(x+iy) = |f(x+iy)|y^k$. It is immediately seen that this function is Γ-invariant. Let α be a representative of a cusp with respect to Γ. Choose $A \in \Gamma(1)$ such that $A \cdot \alpha = \infty$. Then $f|_k A = \Phi(e^{2\pi i\tau/h})$ for some function Φ holomorphic in a domain Re $\tau > c$. We also have $\phi(A\cdot(x+iy)) = |\Phi(e^{2\pi(ix-y)/h})|y^k$. Assume f vanishes at α. Then $\Phi = e^{2\pi(ix-y)/h}\Phi_0$, where $\lim_{y\to\infty}\Phi_0 \neq 0$. Thus $\lim_{y\to\infty}\phi(A\cdot(x+iy)) = \lim_{y\to\infty} e^{-2\pi y}y^k = 0$. This implies that the function $\phi(x+iy)$ converges to zero when $\tau = x+iy$ converges to a cusp. Hence it is a continuous function on a compact topological space $\mathcal{H}^*/\Gamma$. It must be bounded. Conversely, if the inequality (12.3) holds, then $\phi(x+iy)$ must be bounded and hence Φ must be vanishing at 0. $\square$

Corollary 12.1. *Let $f \in \mathcal{M}_k(\Gamma)^0$ and a_n be the coefficient at $e^{2\pi in/h}$ in its Fourier expansion at ∞. Then*

$$|a_n| = O(n^k).$$

In particular, $Z_f(s)$ converges for Re $s > k+1$.

Proof. Let $q = e^{2\pi i(x+iy)/h}$. Fix y and let x vary from 0 to h. Then q moves along the circle $C(y)$ of radius $e^{-2\pi y/h}$ with center at 0. By Cauchy's residue formula

$$a_n = \frac{1}{2\pi i}\int_{C(y)} f(\tau)q^{-n-1}dq = \frac{1}{h}\int_0^h f(x+iy)q^{-n}dx.$$

By Lemma 12.1, $|f(x+iy)| \leq Cy^{-k}$ for some constant C. We have

$$|a_n| \leq \frac{1}{h}\int_0^h |f(x+iy)||q|^{-n}dx \leq Cy^{-2k}e^{2\pi ny/h}.$$

Taking $y = 1/n$, we get $|a_n| \leq Mn^k$. $\square$

12.2 We shall now find a functional equation for the Dirichlet series $Z_f(s)$.

Lemma 12.2. *Let $f \in \mathcal{M}_k(\Gamma)$ and $F_N = \begin{pmatrix} 0 & -1/\sqrt{N} \\ \sqrt{N} & 0 \end{pmatrix}$. Assume that $\Gamma' = F_N^{-1}\cdot\Gamma\cdot F_N$ is a subgroup of finite index in* $\mathrm{SL}(2,\mathbb{Z})$. *Then*

$$W_N(f) := f|_k F_N = f(-1/N\tau)N^{-k}\tau^{-2k} \in \mathcal{M}_k(\Gamma').$$

Moreover, if $f \in \mathcal{M}_k(\Gamma)^0$, then $W_N(f) \in \mathcal{M}_k(\Gamma')^0$.

Proof. For any $A \in \Gamma'$ we have $F_N A = BF_N$ for some $B \in \Gamma$. Hence

$$W_N(f)|_k A = (f|_k F_N)|_k A = f|_k F_N A =$$

$$f|_k BF_N = (f|_k B)|_k F_N = f|_k F_N = W_N(f).$$

We leave the proof of the last assertion to the reader. $\square$

Example 12.1. Let $f \in \mathcal{M}_k(\Gamma_0(n))$. Assume that $N|n$. Then

$$W_N(f) = f(-1/N\tau)N^{-k}\tau^{-2k} \in \mathcal{M}_k(\Gamma_0(N)).$$

To see this we use that

$$\begin{pmatrix} 0 & -1/\sqrt{N} \\ \sqrt{N} & 0 \end{pmatrix} \begin{pmatrix} a & b \\ nc & d \end{pmatrix} \begin{pmatrix} 0 & -1/\sqrt{N} \\ \sqrt{N} & 0 \end{pmatrix}^{-1} = \begin{pmatrix} d & -cn/N \\ -bN & a \end{pmatrix} \in \Gamma_0(N). \tag{12.4}$$

The same equality shows that

$$f \in \mathcal{M}_k(\Gamma(n)) \Longrightarrow W_N(f) \in \mathcal{M}_k(\Gamma(n/N) \cap \Gamma_0(nN)).$$

Theorem 12.1. *(Erich Hecke) Let $f \in \mathcal{M}_k(\Gamma)^0$ and let $g = W_N(f)$. Assume that ${F_N}^{-1} \cdot \Gamma \cdot F_N$ is a subgroup of finite index in $\mathrm{SL}(2, \mathbb{Z})$. Let h be the index of the cusp ∞ of Γ and h' be the same for Γ'. The Dirichlet series $Z_f(s)$ can be extended to a holomorphic function on the whole complex plane. Setting*

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

we have the functional equation

$$h^s R(s, f) = (-1)^k {h'}^{2k-s} R(2k - s; g),$$

Here $\Gamma(s)$ is the Gamma-function.

Proof. We shall use the *Mellin transform* which carries a function $\phi(y)$ defined on the positive ray of real numbers, and bounded at 0 and ∞, to a holomorphic function $M\phi(s)$ defined by $M\phi = F$, where

$$F(s) = \int_0^\infty \phi(y) y^{s-1} dy.$$

It is inverted by

$$\phi(y) = \frac{1}{2\pi} \int_{y-i\infty}^{y+i\infty} F(s) y^{-s} ds, \quad y > 0.$$

Take $\phi(y) = f(iy)$ and let $f = \sum_{n=1}^\infty a_n e^{2\pi i n\tau/h}$ be its Fourier expansion at ∞. We have

$$M\phi(s) = \sum_{n=1}^\infty a_n \int_0^\infty e^{-2\pi n y/h} y^{s-1} dy =$$

$$\sum_{n=1}^\infty a_n \int_0^\infty e^{-t} t^{s-1} \frac{h^s dt}{(2\pi n)^s} = (h/2\pi)^s \Gamma(s) Z_f(s).$$

Here we have used the integral formula for the Gamma-function:

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt. \tag{12.5}$$

We leave to the reader to justify the possibility of the term-by-term integration of the infinite series (we have to use Lemma 12.2). Now let us do the same for the function $g = W_N(f) \in \mathcal{M}_k(\Gamma')^0$, where $\Gamma' = F_N{}^{-1}\Gamma F_N$. We have

$$M\phi(s) = \int_0^\infty f(iy)y^{s-1}dy = \int_0^A f(iy)y^{s-1}dy + \int_A^\infty f(iy)y^{s-1}dy,$$

where the first summand converges for Re $s > k+1$ and the second one converges everywhere. The Fricke transformation transforms $f(iy)$ to $f(i/Ny) = N^k(iy)^{2k}g(iy)$. So changing the variable y to $1/Ny$ we obtain

$$\int_0^A f(iy)y^{s-1}dy = \int_A^\infty f(i/Ny)N^{-s}y^{-s-1}dy = (-1)^k N^{k-s}\int_A^\infty g(iy)y^{2k-1-s}dy. \tag{12.6}$$

This converges for all $s \in \mathbb{C}$. Similarly,

$$\int_A^\infty f(iy)y^{s-1}dy = (-1)^k N^{k-s}\int_0^A g(iy)y^{2k-1-s}dy.$$

This converges for Re $s > k+1$. This shows that each summand in (12.6) can be holomorphically extended to the whole complex plane. After summing up we get

$$M\phi(s) = (h/2\pi)^s\Gamma(s)Z_f(s) = (-1)^k N^{k-s} Mg(iy)(2k-s) =$$

$$(-1)^k N^{k-s}(h'/2\pi)^{2k-s}\Gamma(2k-s)Z_g(2k-s).$$

Thus if we set $R(s,f) = N^{s/2}(2\pi)^{-s}\Gamma(s)Z_f(s)$ we obtain

$$h^s R(s,f) = (-1)^k h'^{2k-s}R(2k-s,g)$$

for Re $s > k+1$. □

It follows from Example 1 that the Fricke transformation F_N defines a linear operator W_N on the space $\mathcal{M}_k(\Gamma_0(N))$. It satisfies

$$W_N^2 = 1.$$

In fact we have

$$W_N^2(f) = W_N(N^{-k}\tau^{-2k}f(-1/N\tau)) = N^{-k}\tau^{-2k}N^{-k}(-1/N\tau)^{-2k}f(\tau) = f(\tau).$$

Thus we can decompose $\mathcal{M}_k(\Gamma_0(N))$ into the direct sum of two eigensubspaces

$$\mathcal{M}_k(\Gamma_0(N)) = \mathcal{M}_k(\Gamma_0(N))_+ \oplus \mathcal{M}_k(\Gamma_0(N))_-$$

with eigenvalue $+1$ or -1. Similarly, we see that W_N acts on the space $\mathcal{M}_k(\Gamma(N))$ and we can decompose it in the direct sum of two eigensubspaces:

$$\mathcal{M}_k(\Gamma(N)) = \mathcal{M}_k(\Gamma(N))_+ \oplus \mathcal{M}_k(\Gamma(N))_-.$$

Corollary 12.2. *Let $f \in \mathcal{M}_k(\Gamma_0(N))_\epsilon$, where $\epsilon = \pm 1$. Then*

$$R(s;f) = (-1)^k\epsilon R(2k-s;f).$$

Corollary 12.3. *Let $f \in \mathcal{M}_k(\Gamma(N))_\epsilon$, where $\epsilon = \pm 1$. Then*

$$R(s;f) = (-1)^k N^{2k-2s}\epsilon R(2k-s;f).$$

12.3 If $f \in \mathcal{M}_k(\Gamma)$ is not a parabolic modular form we cannot, in general, attach the Dirichlet series to it. However, if we assume that f admits a Fourier expansion at ∞ with coefficients satifying $|a_n| \leq n^c$ we can still do it and obtain a holomorphic function $Z_f(s)$ defined for Re $s > c$. The next theorem generalizes the previous theorem to this case.

Theorem 12.2. *Let $f \in \mathcal{M}_k(\Gamma)$ and $g = W_N(f) \in \mathcal{M}_k(\Gamma')$ where $\Gamma' = F_N^{-1} \cdot \Gamma \cdot F_N$ is a subgroup of finite index in* $\mathrm{SL}(2, \mathbb{Z})$. *Let*

$$f = \sum_{n=0}^{\infty} a_n e^{2\pi i n/h}, \quad g = \sum_{n=0}^{\infty} b_n e^{2\pi i n/h'}$$

be the Fourier expansions at f and g at ∞. Assume that $|a_n|, |b_n| \leq O(n^c)$. Let $R(f; s) := N^{s/2}(2\pi)^{-s}\Gamma(s)Z_f(s)$. Then $Z_f(s)$ is holomorphic for Re $s > c + 1$ and $R(f; s) + a_0 s^{-1} + (-1)^k b_0 (2k - s)^{-1}$ admits a holomorphic extension to the whole complex plane. Moreover,

$$h^s R(f; s) = (-1)^k {h'}^{2k-s} R(f|_k F_N; 2k - s).$$

Remark 12.1. It is known that the Gamma-function $\Gamma(s)$ is meromorphic and has a simple pole at $s = 0$. Thus, in Theorem 12.2, $Z_f(s)$ admits a meromorphic extension to the complex plane with single pole at $2k$.

Example 12.2. Take $f(\tau) = E_{2k}(\tau)$. Then

$$E_{2k}(\tau) = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n,$$

where

$$\sigma_{2k-1}(n) = \sum_{d|n} d^{2k-1}.$$

It is easy to see that

$$n^{2k-1} \leq \sigma_{2k-1}(n) \leq A n^{2k-1}$$

for some positive constant A. Thus $Z_f(s)$ is defined and is convergent for Re $s > 2k$. Since

$$\sum_{n=1}^{\infty} \sigma_{2k-1}(n) n^{-s} = \sum_{m,l=1}^{\infty} l^{2k-1}(lm)^{-s} =$$

$$\sum_{m,l=1}^{\infty} m^{-s} l^{-s+2k-1} = \zeta(s)\zeta(s - 2k + 1),$$

we have

$$Z_{E_{2k}}(s) = \frac{2(2\pi i)^{2k}}{(2k-1)!} \zeta(s)\zeta(s - 2k + 1). \tag{12.7}$$

Recall that $E_{2k}(\tau) \in \mathcal{M}_k(\Gamma(1) = \mathcal{M}_k(\Gamma_0(1))$. Applying Theorem 12.2, we obtain

$$\zeta(s)\zeta(s - 2k + 1) = (2\pi)^{2k-2s} \frac{\Gamma(2k - s)}{\Gamma(s)} \zeta(2k - s)\zeta(1 - s).$$

Of course it follows also from the known functional equation for the Riemann zeta function

$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \pi^{\frac{s-1}{2}}\Gamma(\frac{1-s}{2})\zeta(1-s).$$

Example 12.3. Take $f(\tau) = \Theta(0,\tau)^{8t}$. We know that these functions are modular forms of weight $k = 2t$ for $\Gamma(2)$. We have

$$\Theta(0,\tau)^{8n} = \sum_{n=0}^{\infty} c_{8t}(n)e^{\pi in},$$

where

$$c_{8t}(n) = \#\{(r_1,\ldots,r_{8t}) \in \mathbb{Z}^{8t} : n = r_1^2 + \ldots + r_{8t}^2\}.$$

It is clear that we can bound $c_{8t}(n)$ by the number of integer points inside of the cube $[-\sqrt{n}, -\sqrt{n}]^{8t}$. This easily gives

$$c_{8t}(n) \le Cn^{4t} = Cn^{2k}.$$

Therefore, the $Z_f(s)$ is convergent for Re $s > 2k+1$. We have

$$Z_f(\tau) = \sum_{m=1}^{\infty} \frac{c_{8t}(n)}{n^s} = \sum_{(r_1,\ldots,r_{8t})\in\mathbb{Z}^{8t}\setminus\{0\}} \frac{1}{(r_1^2+\ldots+r_{8t}^2)^s} = \sum_{\lambda\in\Lambda\setminus\{0\}} \frac{1}{Q(\lambda)^s},$$

where $Q = x_1^2 + \ldots + x_{8t}^2$ and $\Lambda = \mathbb{Z}^{8t} \subset \mathbb{R}^{8t}$. More generally, for any positive definite quadratic form $Q : \mathbb{R}^n \to \mathbb{R}$ and a lattice Λ in $\mathbb{R}^n$ we can define the *Epstein zeta function*

$$Z_Q(s) = \sum_{\lambda\in\Lambda\setminus\{0\}} \frac{1}{Q(\lambda)^s}.$$

Although $f(\tau)$ is not a modular form for $\Gamma(1)$ it satisfies $f(-1/\tau) = f(\tau)\tau^{4t}$. Applying Corollary 2 to Theorem 1 with $N = 2$ we get

$$2^s 2^{s/2}(2\pi)^{-s}\Gamma(s)Z_f(s) = 2^{4t-s}2^{\frac{4t-s}{2}}(2\pi)^{-4t+s}\Gamma(4t-s)Z_f(4t-s)$$

which gives

$$Z_f(4t-s) = \frac{\pi^{4t-2s}}{2^{2t-s}}\frac{\Gamma(s)}{\Gamma(4t-s)}Z_f(s).$$

12.4 Now let us look at the Dirichlet series associated to cuspidal forms which are simultaneous eigenfunctions of Hecke operators.

Theorem 12.3. *Let f be a normalized cuspidal modular form of weight k with respect to $\Gamma(1)$ and $\sum c_n q^n$ be its Fourier expansion. Assume f is normalized in the sense that $c_1 = 1$. Assume that f is an eigenfunction for all the Hecke operators. Then the associated Dirichlet series $Z_f(s)$ admits the following infinite product expansion:*

$$Z_f(s) = \prod_{p\ \text{prime}} \frac{1}{(1 - c_p p^{-s} + p^{2k-1}p^{-2s})}.$$

Proof. We know from Corollary 11.3 that the function $n \to c_n$ is a multiplicative function. This implies that for any finite set S of prime numbers

$$\sum_{n\in\mathbb{N}(S)} \frac{c_n}{n^s} = \prod_{p\in S}(\sum_{m=0}^{\infty} c_{p^m} p^{-ms}) = \prod_{p\in S} \frac{1}{(1 - c_p p^{-s} + p^{2k-1}p^{-2s})},$$

where $\mathbb{N}(S)$ denotes the set of natural numbers whose prime decomposition involves only numbers from S. Here we use Corollary 11.3 which gives us that

$$(1 - c_p p^{-s} + p^{2k-1}p^{-2s})(\sum_{m=0}^{\infty} c_{p^m} p^{-ms}) = 1.$$

When S grows, the left-hand side tends to $Z_f(s)$. This implies that the infinite products converges to $Z_f(s)$. □

Example 12.4. Take $f = \Delta$ to obtain

$$Z_\Delta = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \prod_{p \text{ prime}} \frac{1}{(1 - \tau(p)p^{-s} + p^{11}p^{-2s})},$$

where $\tau(n)$ is the Ramanujan function. Applying Corollary 2 with $N = 1$, we get also the functional equation for $Z_\Delta(s)$:

$$Z_\Delta(12 - s) = (2\pi)^{12-2s} \frac{\Gamma(s)}{\Gamma(12 - s)} Z_\Delta(s).$$

Remark 12.2. Let

$$\Phi_{f,p} = 1 - c_p T + p^{2k-1}T^2 = (1 - \alpha_p T)(1 - \alpha'_p T).$$

We know that α_p and α'_p are algebraic integers. The *Petersson conjecture* suggested that $\alpha'_p = \bar{\alpha}_p$, or, equivalently,

$$|\alpha_p| = |\alpha'_p| = p^{k-\frac{1}{2}},$$

or

$$|c_p| \le 2p^{k-\frac{1}{2}},$$

or

$$|c_n| \le n^{k-\frac{1}{2}}\sigma_0(n) \quad \text{for all } n \ge 1.$$

This was proven by P. Deligne as a special case of his proof of Weil's conjectures about the zeta function of algebraic varieties. In particular, when $k = 6$ we get the *Ramanujan's Conjecture*:

$$|\tau(p)| \le 2p^{11/2}.$$

12.5 In this section we generalize some of the previous results to the case when $\Gamma(1)$ is replaced with $\Gamma_1(N)$. We will be rather sketchy and refer for the details to **[Seminar]**. We use the definition of the corresponding Hecke ring $H(\Gamma,\Delta)$ from Exercise 11.11. Let us denote it by $\mathbf{T}_N$. It is generated by the elements $T(p)$ for all prime p and elements $T(p,p)$ for all primes p not dividing N. Let $\mathbf{T}^{(N)}$ denote the subring of $\mathbf{T}_N$ generated by $T(p)$ and $T(p,p)$, where p does not divide N. One can extend the proof of Theorem 11.2 to show that $\mathbf{T}^{(N)}$ acts in the space $\mathcal{M}_k(\Gamma_1(N))^0$ by Hermitian operators (with respect to the Petersson inner product). This is not true for the ring $\mathbf{T}_N$. So a cuspidal form could be a simulateneous eigenfunction for all the Hecke operators coming from $\mathbf{T}^{(N)}$ but not an eigenfunction for some Hecke operator from $\mathbf{T}_N$.

It is easy to see that $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$ with the quotient group isomorphic to $(\mathbb{Z}/N\mathbb{Z})^*$. Thue latter group acts naturally on the algebra of modular forms with respect to $\Gamma_0(N)$, and for each $k\geq 0$ we have a direct sum decomposition into the eigensubspaces corresponding to Dirichlet characters $\chi:(\mathbb{Z}/N\mathbb{Z})^*\to\mathbb{C}^*$:

$$\mathcal{M}_k(\Gamma_1(N))=\oplus_\chi\mathcal{M}_k(\Gamma_1(N)_\chi, \tag{12.8}$$

Let

$$\mathcal{M}_k(\Gamma_0(N);\chi):=\{f\in\mathcal{M}_k(\Gamma_0(N)) : f|_kg=\chi'(g)f,\quad\forall g\in\Gamma_0(N)\},$$

where χ' is the composition of χ with the homomorphism $\Gamma_0(N)\to(\mathbb{Z}/N\mathbb{Z})^*$ which sends a matrix to the residue modulo N of its first coefficient. We will also need the notation

$$\mathcal{M}_k(\Gamma_0(N);\chi)^0=\mathcal{M}_k(\Gamma_0(N);\chi)\cap\mathcal{M}_k(\Gamma_0(N))^0.$$

We have

$$\mathcal{M}_k(\Gamma_1(N)_\chi=\mathcal{M}_k(\Gamma_0(N);\chi).$$

Clearly the subspace $\mathcal{M}_k(\Gamma_0(N)\subset\mathcal{M}_k(\Gamma_1(N)$ corresponds to the trivial character.

More explicitly, the action of $(\mathbb{Z}/N\mathbb{Z})^*$ on $\mathcal{M}_k(\Gamma_1(N))$ is defined as follows. For any $n\in(\mathbb{Z}/N\mathbb{Z})^*$, let α_n be any element of $\mathrm{SL}(2,\mathbb{Z})$ such that $\alpha_n=\left(\begin{smallmatrix} n & 0\\ 0 & n^{-1}\end{smallmatrix}\right)$ modulo N. Then the action of n on $\mathcal{M}_k(\Gamma_1(N)$ is given by the formula

$$<n>_k : f\to f|_k\alpha_n. \tag{12.9}$$

Notice that the Hecke operator $T(n,n)$ acts on $\mathcal{M}_k(\Gamma_1(N))$ as $n^{k-2}<n>$.

We have the following analogue of Theorem 11.2:

Theorem 12.4. *Let $T(n)\in\mathbf{T}^{(N)}$ with $(n,N)=1$. For any $f,g\in\mathcal{M}_k(\Gamma_0(N);\chi)^0$,*

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

where the inner product is the Petersson inner product. In other words, the adjoint of $T(n)$ is $T_n\circ<n \bmod N>$.

It is easy to see that the operators $T(m),(m,N)=1$ and $<n>$ form a set of commuting normal operators on $\mathcal{M}_k(\Gamma_1(N))$. This allows to decompose each $\mathcal{M}_k(\Gamma_0(N);\chi)$ into an orthogonal sum of $\mathbf{T}^{(N)}$-eigensubspaces.

The condition $(n,N)=1$ is important. The operators $T(n)$ for which n does not satisfy this condition are not normal operators. So, it becomes problematic to find a modular form which is a simultaneous eigenfunction for all the Hecke operators.

Another unfortunate thing is that the operator W_N does not commute with all the Hecke operators, so that we cannot combine Theorem 12.3 and Corollary 12.3 to obtain Dirichlet series $Z_f(s)$ with the infinite product as in Theorem 12.3 which satisfy the functional equation as in Corollary 12.3.

We have the following weaker assertion:

Proposition 12.1. *Let W_N be the operator on $\mathcal{M}_k(\Gamma_1(N))^0$ corresponding to the Fricke transformation F_N defined by $f \to f|_k \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. Let $T(n)_{k,\chi}$ denote the restriction of the Hecke operator $T(n), (n,N)=1$ to the subspace $\mathcal{M}_k(\Gamma_0(N);\chi)$. Then*

$$T(n)_{k,\chi} \circ W_N = \chi(n) W_N \circ T(n)_{k,\bar{\chi}},$$

where $\bar{\chi}$ denotes the complex conjugate character.

Proof. We refer for the proof to **[Shimura]**. □

However, one can still find common eigenvalues in $\mathcal{M}_k(\Gamma_1(N))^0$ for all the Hecke operators if we restrict these operators to a certain subspace. Let us explain this.

Let d, M be positive integers such that $dM|N$. There exists an injective linear map

$$\imath_{d,M,N} : \mathcal{M}_k(\Gamma_1(M))^0 \to \mathcal{M}_k(\Gamma_1(M))^0. \tag{12.10}$$

It is defined by sending $f(\tau)$ to $d^{\frac{k}{2}-1} f(d\tau)$. One checks that it is a homomorphism of $\mathbf{T}^{(N)}$-modules. Let $\mathcal{M}_k(\Gamma_1(M))^0_{old}$ be the subspace of $\mathcal{M}_k(\Gamma_1(M))^0$ spanned by the images of the maps $\imath_{d,M,N}$. Let $\mathcal{M}_k(\Gamma_1(M))^0_{new}$ be the orthogonal complement of $\mathcal{M}_k(\Gamma_1(M))^0_{old}$ with respect to the Petersson inner product. In fact, we have an orthogonal decompositions

$$\mathcal{M}_k(\Gamma_1(M))^0_{old} = \oplus_\chi \mathcal{M}_k(\Gamma_0(M);\chi)^0_{old},$$

where $\mathcal{M}_k(\Gamma_0(M);\chi)^0_{old} = \mathcal{M}_k(\Gamma_0(M);\chi)^0 \cap \mathcal{M}_k(\Gamma_0(M))^0_{old}$, as well as

$$\mathcal{M}_k(\Gamma_0(M);\chi)^0 = \mathcal{M}_k(\Gamma_0(M);\chi)^0_{old} \oplus \mathcal{M}_k(\Gamma_0(M);\chi)^0_{new}.$$

The next result, due to Atkin and Lehler, is called the Multiplicity One Theorem.

Theorem 12.5. *Let $f \in \mathcal{M}_k(\Gamma_1(N))^0_{new}$. Suppose that f is an eingefunction for all the Hecke operators from $\mathbf{T}^{(ND)}$, for some $D > 0$. If g is another such form with the same eiegenvalues, then g is a scalar multiple of f.*

Corollary 12.4. *Let $f \in \mathcal{M}_k(\Gamma_1(N))^0_{new}$. The following assertions are equivalent:*

(i) f is an eigenfunction for $\mathbf{T}^{(ND)}$ for some $D > 0$;

(ii) f is an eigenfunction for $\mathbf{T}^{(N)}$;

(iii) f is an eigenfunction for $\mathbf{T}_N$.

Proof. It follows from the theorem that each $\mathbf{T}^{(ND)}$-eigensubspace in $\mathcal{M}_k(\Gamma_1(N))^0_{new}$ is one-dimensional, and hence is $\mathbf{T}_N$-invariant because all the Hecke operators commute (Exercise 11.11 (vi)). This shows that (i) implies (iii). The rest of implications are obvious. □

Remark 12.3. Let $f = \sum a_n q^n$ be the Fourier expansion of a $f \in \mathcal{M}_k(\Gamma_1(N))^0_{new}$ satisfying one of the equivalent conditions of the previous corollary. One can show that $a_1 \neq 0$ so we can alaways normalize f to assume $a_1 = 1$. Such a modular form is called a *newform*.

So we can extend Theorem 11.2 to newforms. To see when newforms exist we observe that the maps $\imath_{d,M,N}$ send $\mathcal{M}_k(\Gamma_0(M);\chi)^0$ to $\mathcal{M}_k(\Gamma_0(N);\chi')^0$, where χ' is the composition of $\chi : (\mathbb{Z}/N\mathbb{Z}) \to \mathbb{C}^*$ with the natural surjection $(\mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/M\mathbb{Z})$. So, if χ is a primitive character of $(\mathbb{Z}/N\mathbb{Z})$, we have

$$\mathcal{M}_k(\Gamma_0(M);\chi)^0 = \mathcal{M}_k(\Gamma_0(M);\chi)^0_{new}.$$

We can apply Corollary 12.3 to get a functional equation for newforms. Notice that the space $\mathcal{M}_k(\Gamma_1(N))^0_{new}$ is invariant with respect to the operator W_N. This follows from the W_N-invariance of the space $\mathcal{M}_k(\Gamma_1(N))^0_{old}$. The latter is easy to check. We have, for any $f \in \mathcal{M}_k(\Gamma_1(M))^0$ such that $N = dM$,

$$W_{dM}(\imath_{d,M,N}(f(\tau)) = W_M(d^{\frac{k}{2}-1}f(d\tau)) =$$
$$(dM)^{-k}d^{\frac{k}{2}-1}(\tau)^{-2k}f(-1/M\tau) = d^{-k}\imath_{d,M,N}(W_M(f)). \quad (12.11)$$

This checks the claim.

It is also easy to see that

$$W_N(\mathcal{M}_k(\Gamma_0(N);\chi)^0_{new}) = \mathcal{M}_k(\Gamma_0(N);\bar{\chi})^0_{new}.$$

In particular, we can decompose $\mathcal{M}_k(\Gamma_0(N))^0_{new}$ into a direct sum of eigensubspaces of W_N:

$$\mathcal{M}_k(\Gamma_0(N))^0_{new} = \mathcal{M}_k(\Gamma_0(N))^0_{new,+} \oplus \mathcal{M}_k(\Gamma_1(N))^0_{new,-}.$$

An element of each space will satisfy the functional equation from Corollary 12.3 and also will admit the infinite product decomposition from Theorem 12.3.

Exercises

12.1 Show that the Mellin transform of the function $f(x) = \vartheta(0;ix) - 1$ is equal to $2\pi^{-s}\zeta(2s)\Gamma(s)$.

12.2 Show that the Dirichlet series $\sum_{n=1}^{\infty} a_n n^{-s}$ can be expressed as the Laplace transform $\int_0^{\infty} f(t)e^{-st}dt$ for an appropriate function $f(t)$.

12.3 Find the functional equation for Z_f where $f(\tau) = \Delta(11\tau)/\Delta(\tau)^{1/12}$ (see Exercise 10.6).

12.4 Show that $E_2(\tau) - pE_2(p\tau)$ belongs to $\mathcal{M}_1(\Gamma_0(p))$, where p is prime.

12.5 Prove Theorem 12.2.

12.6 Apply the proof of Theorem 1 to the function $f(\tau) = \vartheta_{00}(0;\tau)$ to obtain the functional equation for the Riemann zeta function.

12.7 Prove that for any $f = \sum a_n q^n \in \mathcal{M}_k(\Gamma(1))$ one has $|a_n| \leq O(n^{2k-1})$.

12.8 Show that the discriminant modular form $\Delta \in \mathrm{M}_6(\Gamma) \subset \mathrm{M}_6(\Gamma_0(N))$ is an eigenfunction for all Hecke operators from $\mathbf{T}'_N$ but not for all Hecke operators from $\mathbf{T}_N$ (unless $N = 1$).

12.9 Describe the decomposition of $\mathcal{M}_1(\Gamma_1(33))^0$ into the old and new subspaces by verifying assertions (i)-(iii) below.

(i) $\dim \mathcal{M}_1(\Gamma_1(33))^0 = 21, \dim \mathcal{M}_1(\Gamma_1(11))^0 = 1$, and $\mathcal{M}_1(\Gamma_1(3))^0 = 0$;

(ii) $\dim \mathcal{M}_1(\Gamma_1(33))^0_{old} = 2$;

(iii) $\dim \mathcal{M}_1(\Gamma_0(33); \chi)^0_{new} = 2$ for each nontrivial character χ.

(iv) Show that each $\mathcal{M}_1(\Gamma_0(33; \chi))^0_{new}$ is spanned by $\mathbf{T}_{33}$-eigenfunctions.

Lecture 13

The Shimura-Tanyama-Weil Conjecture

13.1 In the previous lecture we have attached a Dirichlet series to a cuspidal modular form with respect to the group $\Gamma_0(N)$. In this lecture we will attach a Dirichlet series to an elliptic curve over $\mathbb{Q}$. The conjecture from the title of the lecture tells that the latter Dirichlet series always coincides with the former one for an appropriate modular form.

Let E be an elliptic curve. We assume that it can be given by homogeneous equations with coefficients in $\mathbb{Q}$ and the set of points of $E(\mathbb{Q})$ with rational projective coordinates is not empty. We say in this case that E is an elliptic curve over $\mathbb{Q}$. One can show that the set $E(\mathbb{Q})$ is independent of the choice of a system of algebraic equations over $\mathbb{Q}$ defining E.

Lemma 13.1. *Let E be an elliptic curve over $\mathbb{Q}$. Then E is isomorphic to a plane cubic curve with equation*

$$Y^2Z - X^3 - c_2XZ^2 - c_3Z^3 = 0 \tag{13.1}$$

with integer coefficients c_2, c_3.

Proof. We use the Riemann-Roch Theorem from Lecture 8. Let $D = \sum n_P P$ be a divisor which is a linear combination of points from $E(\mathbb{Q})$. Let $L(D)_{\mathbb{Q}}$ denote the $\mathbb{Q}$-subspace of $L(D)$ which consists of rational functions on E with coefficients in $\mathbb{Q}$. Once can show that $\dim_{\mathbb{Q}} L(D)_{\mathbb{Q}} = \dim_{\mathbb{C}} L(D)$. Fix a point $Q \in E(\mathbb{Q})$ and apply the Riemann-Roch Theorem to obtain that $\dim_{\mathbb{Q}} L(nQ) = n$. Let x be a non-constant function in $L(2Q)$ and let $y \in L(3Q)$ which is not a linear combination of 1 and x. Since the functions $1, x, x^2, x^3, y, y^2, xy$ belong to the space $L(6Q)$ and the latter is of dimension 6 over $\mathbb{Q}$, we obtain a linear relation

$$a_0 + a_1x + a_2x^2 + a_3x^3 + b_0y + b_1xy + b_2y^2 = 0$$

with coefficients in $\mathbb{Q}$. Replacing x with $ax + b$ and y with $cy + dx + e$ for some appropriate coefficients $a, b, c, d, e \in \mathbb{Q}$ we may assume that the linear relation has the form

$$b_3 + b_2x + x^3 - y^2 = 0,$$

where $b_0, b_1 \in \mathbb{Q}$ (see Example 6.4). Multiplying x by α^{-2} and y by α^{-3} for an appropriate integer α, we can change b_2 to $b_2\alpha^4$ and b_3 to $b_3\alpha^6$. Choosing an appropriate α this makes we can assume that the coeffients $c_2 = b_2\alpha^4$ and $c_3 = b_3\alpha^6$ to be integers. Using the argument from the second half of the proof of Corollary 8.5 we obtain that the functions x, y define an isomorphism from $E \setminus \{Q\} \to C \setminus \{\infty\}$, where C is the plane cubic given by the equation (13.1), and ∞ is its point $(X, Y, Z) = (0, 1, 0)$. This can be extended to an isomorphism $E \cong C$. □

Observe that E can be given in many ways by an equation of the form (13.1). We can make it almost unique if we require some additional property. Let

$$\Delta = 4c_2^3 + 27c_3^2 \tag{13.2}$$

be the discriminant of the polynomial $t^3 + c_2 t + c_3$. We call it the *discriminant* of the equation (13.1). For every prime p let $\nu_p(\Delta)$ be the highest power of p which divides Δ. We say that the equation (13.1) is a *minimal Weierstrass equation* of E if for any other equation of the form (13.1) defining E with discriminat Δ' we have, for any prime p,

$$\nu_p(\Delta) \leq \nu_p(\Delta')$$

One can prove that a minimal Weierstrass equationt always exists and is unique (see **[Silverman]**).

Definition. Let E be an elliptic curve over $\mathbb{Q}$ and let (13.1) be its minimal Weierstrass equation with discriminant Δ. Let p be a prime number. We say

(a) E has *good reduction* (resp. *bad reduction*) modulo p if $p \not| \Delta$ (resp. $p|\Delta$),

(b) E has *multiplicative reduction* modulo p if $p|\Delta$ but $p \not| c_2c_3$,

(c) E has an *additive reduction* modulo p if $p|c_2$ and $p|c_3$.

Let us explain the terminology. Since the coefficients c_2 and c_3 are integers we can reduce them modulo p to obtain an algebraic curve over the finite field $\mathbb{F}_p$. This curve is a singular curve (i.e. the formal partial derivatives of the polynomial defining the equation has a common zero over the algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$) if and only if $p|\Delta$. If $p|c_2$ and $p|c_3$ the equation over $\mathbb{F}_p$ becomes $Y^2Z - X^3 = 0$. Its singular point is $(0, 1, 0)$, and its nonsingular solutions $(x, y, 1)$ over $\bar{\mathbb{F}}_p$ are of the form $(t^2, t^3), t \in \bar{\mathbb{F}}_p$. The addition law in $\bar{\mathbb{F}}_p$ defines the addition law on the set of nonsingular solutions equipping this set with the structure of an abelian group isomorphic to the additive group of $\bar{\mathbb{F}}_p$. Finally, if E has multiplicative reduction modulo p, then after reducing the coefficients c_2 and c_3 modulo p we obtain an algebraic curve over $\mathbb{F}_p$ which is isomorphic over $\bar{\mathbb{F}}_p$ to the curve

$$Y^2Z - X^2(X - \alpha Z) = 0 \tag{13.3}$$

with $\alpha \neq 0$. The point $(0, 0, 1)$ is its singular point. Any nonsingular solution over $\bar{\mathbb{F}}_p$ has the form $(t_0(t_1^2 + \alpha t_0^2), t_1(t_1^2 + \alpha t_0^2), t_0)$, where $(t_0, t_1) \in \mathbb{P}^1(\bar{\mathbb{F}}_p)$ and $t^2 + \alpha t_0^2 \neq 0$. The linear transformation $u_0 = t_0 + \sqrt{\alpha}, u_1 = t_0 - \sqrt{\alpha}$ allows one to identify the set of nonsingular solutions with the subset $\mathbb{P}^1(\bar{\mathbb{F}}_p) \setminus \{0, \infty\} = \bar{\mathbb{F}}_p^*$. So this set carries a natural structure of an abelian group isomorphic to the multiplicative group of the field $\bar{\mathbb{F}}_p$.

13.2 Now we are ready to define the *L-function* $L(E,s)$ of an elliptic curve over $\mathbb{Q}$. It is given as an infinite product

$$L(E,s) = \prod_{p \text{ prime}} L_p(E,s), \tag{13.4}$$

where

(a) if E has a good reduction modulo p

$$L_p(E,s) = \frac{1}{1 - a(p)p^{-s} + p^{1-2s}},$$

where

$$a(p) = p + 1 - \#E(\mathbb{F}_p),$$

and $E(\mathbb{F}_p) = \{(x,y,z) \in \mathbb{P}^2(\mathbb{F}_p) : y^2 z = x^3 + c_2 x z^2 + c_3 z^3\}$.

(b) if E has multiplicative reduction modulo p

$$L_p(E,s) = \frac{1}{1 - a(p)p^{-s}},$$

where $a(p) = 1$ if α in (13.3) belongs to $\mathbb{F}_p$ and $A(p) = -1$ otherwise.

(c) if E has additive reduction modulo p

$$L_p(s) = 1.$$

The next lemma shows that $L(E,s)$ is a Dirichlet series.

Lemma 13.2. *The infinite product $\prod_p (1 - c_p p^{-s})^{-1}$ with $|c_p| \le p^\alpha$ for some real α defines an absolutely convergent Dirichlet series for Re $s > c + 1$.*

Proof. Let c_n be a multiplicative complex-valued function on $\mathbb{N}$ with the value at a prime p equal to c_p. We have a formal identity

$$\sum_{n=1}^{\infty} \frac{c_n}{n^s} = \prod_p \frac{1}{1 - c_p p^{-s}}.$$

Since $|c_p| \le p^\alpha$, we have $|c_n| \le n^\alpha$ for all n. We know from Lecture 12 that this implies that the Dirichlet series is absolutely convergent for Re $s > c + 1$. $\square$

Corollary 13.1. *The infinite product $L(E,s)$ converges for Re $s > 2$ and is given there by an absolutely convergent Dirichlet series.*

Proof. Let a_p be the coefficient from the definition of $L(E,s)$. If p is a prime defining a bad reduction of E, then $|a_p| \le 1$. If p defines a good reduction, then $E(\mathbb{F}_p)$ consists of the infinity point and a points $(x,y,1)$, where $x, y \in \mathbb{F}_p$ and $y^2 = x^3 + c_2 x + c_3$. This gives $\#E(\mathbb{F}_p) \le 2p + 1$ and hence $|a_p| = |\#E(\mathbb{F}_p) - p - 1| \le p$. We can write the factor $L_p(E,s)$ for "good" primes in the form

$$L_p(E,s) = \frac{1}{(1 - r_p p^{-s})(1 - r'_p p^{-s})},$$

where

$$1 - a_pX + pX^2 = (1 - r_pX)(1 - r'_pX).$$

The roots r_p, r'_p are equal to $\frac{1}{2}(a_p \pm \sqrt{a_p^2 - 4p})$ and clearly satisfy $|r_p| \leq |a_p| \leq p$. Thus we can write down the infinite product $L(E,s)$ as the product $L_1(s)L_2(s)$, where each factor satisfies the assumption of the previous lemma with $c = 1$. The assertion follows from the lemma. □

In fact, we can do better and prove the convergence of the L-series for Re $s > \frac{3}{2}$. For this we invoke the following

Theorem 13.1. *(H.Hasse) In the above notation*

$$|p + 1 - \#E(\mathbb{F}_p)| < 2\sqrt{p}.$$

Proof. We refer to **[Knapp]** for an elementary proof of this theorem due to Yu. Manin. □

13.3 Now we are familiar with two Dirichlet functions both absolutely convergent for Re $s > 2$. One is the Dirichlet series $Z_f(s)$ associated to a cusp form f of weight 1 with respect to $\Gamma_0(N)$ and $L(E,s)$. The next conjecture relates these two functions:

Conjecture. *(Hasse-Weil) Let E be an elliptic curve over $\mathbb{Q}$. Define the* conductor *of E to be*

$$N = \prod_p p^{a_p},$$

where p runs in the set of primes for which E has a bad reduction, and $a_p = 1$ if the reduction is of multiplicative type, and $A_p = 2$ otherwise. There exists a unique $f \in \mathcal{M}_1(\Gamma_0(N))^0$ such that

$$Z_f(s) = L(E,s), Re\ s > 2.$$

Moreover, f is an eigenvector of all the Hecke operators and also an eigenvector for the operator W_N.

Notice that according to Remark 12.3, the form f must be a newform. Applying Corollary 12.2, we obtain the following:

Corollary 13.2. *Assume the above conjecture is true. Then $L(E,s)$ admits a holomorphic extension to the entire complex plane and satisfies the following functional equation:*

$$N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(E,s) = \pm N^{\frac{2-s}{2}}(2\pi)^{-s+2}\Gamma(2-s)L(E,2-s).$$

In fact, the previous conjecture was motivated by this assertion. It turns out that the latter corollary is almost equivalent to the Hasse-Weil conjecture. One observes first that $Z_f(s)$ satisfies the following additional property. Let

$$\chi : \mathbb{Z} \to \mathbb{C}$$

be a *Dirichlet character* modulo m. Recall that it means that $\chi(n) = 0$ if $(n,m) \neq 1$ and the induced function on $(\mathbb{Z}/m\mathbb{Z})^*$ is a homomorphism to $\mathbb{C}^*$. We say that χ is a *primitive character* if χ is not a Dirichlet character modulo any proper divisor of m. Let us modify the zeta function $Z_f(s) = \sum \frac{a_n}{n^s}$ associated to a modular form by setting

$$Z_f(s;\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)a_n}{n^s}.$$

There is an analog of Corollary 12.2:

Theorem 13.2. *Let $f \in \mathcal{M}_k(\Gamma_0(N))^0$ satisfying $W_N f = \epsilon f$. For any primitive Dirichlet character χ modulo m, where $(m,N) = 1$, set*

$$R_f(s;\chi) = (m^2N)^{s/2}(2\pi)^{-s}\Gamma(s)Z_f(s;\chi).$$

Then

$$R_f(s;\chi) = \epsilon(-1)^k m^{-1} G(\chi)^2 \chi(N) R_f(2k-s;\bar{\chi}).$$

Here $\bar{\chi}$ denotes the conjugate Dirichlet character defined by $\bar{\chi}(n) = \chi(\bar{n})$ and $G(m,\chi)$ is the Gauss sum *defined by*

$$G(\chi) = \sum_{s=0}^{m-1} e^{2\pi i s/m}\chi(s).$$

Proof. Let

$$\mathcal{M}_k(\Gamma_0(N),\chi) = \{f \in \mathcal{M}_k(\Gamma_0(N)) : f|_k \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \chi(\delta)f\}$$

Clearly, $\mathcal{M}_k(\Gamma_0(N),\chi) \subset \mathcal{M}_k(\Gamma_1(N))$, where

$$\Gamma_1(N) = \{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0(N) : \alpha \equiv \delta \equiv 1 \quad \text{modulo} \quad N\}$$

We can apply Theorem 12.1 to any cusp form $f \in \mathcal{M}_k(\Gamma_0(N),\chi)$. Now we use the following "shift trick":

$$f = \sum_{n=1}^{\infty} c_n q^n \in \mathcal{M}_k(\Gamma_0(N);\psi) \Longrightarrow f_\chi = \sum_{n=1}^{\infty} \chi(n)c_n q^n \in \mathcal{M}_k(\Gamma_0(M);\chi^2\psi),$$

where ψ is a primitive Dirichlet character modulo a divisor s of N, χ is a primitive character modulo some number m, and M is the least common multiple of N, m^2, and ms. The proof of this fact is a straightforward check using some known properties of the Gauss sums. Taking $\psi \equiv 1$, we obtain that

$$R_f(s;\chi) = R_g(s),$$

where $g \in \mathcal{M}(\Gamma(Nm^2);\chi^2)$. Now we apply Theorem 12.1 to $R_g(s)$, previously checking that

$$W_{Nm^2} f_\chi = \epsilon\chi(N)G(\chi)^2 m^{-1} f_{\bar{\chi}}. \tag{13.5}$$

□

Theorem 13.3. *(Weil's Converse Theorem) Let $L(s) = \sum_{n=1}^{\infty} c_n n^{-s}$ be a Dirichlet series with $|c_n| = O(n^a)$ for some $a > 0$. Let N, k be positive integers and $\epsilon = \pm 1$. Suppose*

(i) the function $R(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(s)$ extends to a holomorphic function on the entire complex plane, is bounded in every vertical strip, and satisfies the functional equation

$$R(s) = \epsilon(-1)^k R(2k - s);$$

(ii) for every integer m coprime with N, and every primitive Dirichlet character χ modulo m, set

$$L_\chi(s) = \sum_{n=1}^{\infty} c_n \chi(n) n^{-s}$$

and assume that the function

$$R_\chi(s) = (m^2 N)^{s/2}(2\pi)^{-s}\Gamma(s)L_\chi(s)$$

extends holomorphically to the entire complex plane, is bounded in every vertical strip, and satisfies

$$R_\chi(s) = \epsilon(-1)^k m^{-1} G(\chi)^2 \chi(N) R_\chi(2k - s);$$

(iii) the series $L(s)$ converges absolutely at $s = 2k - \delta$ for some $\delta > 0$.

Then there exists $f \in \mathcal{M}_k(\Gamma_0(N))^0$ such that

$$L(s) = Z_f(s).$$

We are skipping the proof referring to **[Ogg]** or **[Miyake]**.

13.4 Let us check the Hasse-Weil conjecture in the case when $E = X_0(N)$. Using the formula for the genus of a modular curve from Lecture 8, it is not difficult to see that N must belong to the set

$$\{11, 14, 15, 17, 19, 20, 21, 24, 32, 36, 49\}. \tag{13.6}$$

We shall use the theory of Hecke operators for $\Gamma = \Gamma_0(N)$. In Lecture 11 we considered only the case $\Gamma = \Gamma(1)$, so we have to rely on Exercises 11.7-11.9 instead. Let $\sigma_p = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$, where p is a prime number. According to Exercise 11.7, the matrix α_p defines a correspondence on $\mathcal{H}/\Gamma_0(N)$ which we denote by $T(p)$. We can use the same matrix to define a Hecke operator on the space of modular forms $\mathcal{M}_k(\Gamma_0(N))$ (see Exercise 11.9). The following is a simple description of the Hecke correspondences $T(p)$ in the case $(p, N) = 1$. We know that each point of $\mathcal{H}/\Gamma_0(N)$ can be interpreted as the isomorphism class of a pair (E, H), where E is an elliptic curve and H is its subgroup of order N. Equivalently, the pair (E, H) can be viewed as the pair of numbers $(j(E), j(E'))$, where $E' = E/H$. Let $S_0, S_1, \dots, S_p$ be the set of subgroups of order p in ${}_pE \cong (\mathbb{Z}/p\mathbb{Z})^2$. We have

$$T(p)(j(E), j(E')) = \{(j(E/S_i), j(E'/\bar{S}_i)), i = 0, \dots, p\}, \tag{13.7}$$

Assume p is prime of a good reduction for $X_0(N)$. Let $\bar{X}_0(p)$ denote the corresponding reduction. This is an elliptic curve (= a curve of genus 1) defined over the field $\mathbb{F}_p$.

The reduction of the affine part $\mathcal{H}/\Gamma_0(N)$ of $X_0(N)$ modulo p is an affine curve $V_0(N)_p$ over $\mathbb{F}_p$. Its points over a field K of characteristic p correspond to isomorphism classes of pairs (E, H) as above defined over K. There is one important difference between elliptic curves over a field of characteristic 0 and over a field of characteristic $p > 0$. In the former case the group of p-torsion points consists of p^2 elements. In the latter case, it consists of p elements or it is trivial (see Exercise 13.2). So, the degree of the correspondence $\bar{T}(p)$ obtained from $T(p)$ by reduction modulo p must be equal to one.

In characteristic $p > 0$ there are regular maps of algebraic varieties which are bijective on the set of point but nevertheless are not isomorphisms. An example of such a map is the *Frobenius map*. It is induced by the map of projective space defined by the formula:

$$F_p : (x_0, \dots, x_n) \to (x_0^p, \dots, x_n^p).$$

Let X be a projective algebraic subvariety in $\mathbb{P}^n$ defined by equations with coefficients in a field K of characteristic $p > 0$. Let $X^{(p)}$ be the variety whose equations are obtained from those of X when its coefficients are raised in p-th power. Then F_p restricts to a regular map $F_p : X \to X^{(p)}$ of algebraic varieties. In the special case when $K = \mathbb{F}_p$ we have $X = X^{(p)}$ so F is a map of X to itself. Although it is the identity on the set $X(\mathbb{F}_p)$ of points with coordinates in $\mathbb{F}_p$, it is not the identity on the set $X(\bar{\mathbb{F}}_p)$ of points with coordinates in the algebraic closure of $\mathbb{F}_p$. When $X = E$ is an elliptic curve over $\mathbb{F}_p$ the map F is a homomorphism of groups $E(\bar{\mathbb{F}}_p) \to E(\bar{\mathbb{F}}_p)$. One can show that the endomorphism $[p] : x \to x^p$ of the group $E(\bar{\mathbb{F}}_p)$ factores through F_p. Let $[p] = F_p' \circ F_p$. We have the following:

Theorem 13.4. *(Eichler-Shimura) Let p be a prime of good reduction for $X_0(N)$. Then we have the following equality in the ring* $\mathrm{Corr}(V_0(N)_p(\bar{F}_p))$:

$$\bar{T}(p) = F_p + F_p'.$$

Proof. We will only sketch it. Let us show that the two correspondences agree on a certain open subset of points of $V_0(N)$. Consider a point $P \in V_0(N)(\bar{\mathbb{F}}_p)$ and lift it to a point $P' \in X_0(N)(\bar{\mathbb{Q}})$, where $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$. The point P' can be represented as the isomorphism class of a pair (E, H), where E is an elliptic curve H is a cyclic subgroup of order N of $E(\bar{\mathbb{Q}})$. Equivalently, we can view this point as an isogeny $E \to E'$ with kernel H. The reduction modulo p defines a homomorphism ${}_pE(\bar{\mathbb{Q}}) \to {}_p\tilde{E}(\bar{\mathbb{F}}_p)$ whose kernel is a cyclic group A_0 of order p. Here we assume that $\tilde{E}$ is an *ordinary elliptic curve*, i.e. ${}_p\tilde{E}(\bar{\mathbb{F}}_p)$ is of order p. Let $A_0, \dots, A_p$ be the subgroups of order p of E. Then each $A_i, i \neq 0$ is mapped to the subgroup of order p in $\tilde{E}$. Let $\tilde{E}_i$ denote the reduction modulo p of the elliptic curve $E_i = E/A_i$. Let $\tilde{E}_i'$ be the similar notation for the curve E_i'. The multiplication map $x \to px$ of $\tilde{E}$ factors as

$$\tilde{E} \to \tilde{E}_i \to \tilde{E}.$$

When $i = 0$, the first map is purely inseparable of degree p, and the second map is separable of degree p. When $i \neq 0$ the first map is separable and the second one is inseparable, both are of degree p. We have, in both cases,

$$\tilde{E}^{(p)} \cong \tilde{E}_0, \quad \tilde{E}_i'^{(p)} \cong \tilde{E}_i', i > 0.$$

One can show that

$$(\tilde{E}^{(p)}, \tilde{E}'^{(p)}) = F_p(\tilde{E}, \tilde{E}').$$

Thus $F_p(\tilde{P}) = (\tilde{E}_0, \tilde{E}_0'$ and $F_p(\tilde{E}_i, \tilde{E}_i') = \tilde{P}, i > 0$. This implies that $\bar{T}(p) = F_p + F_p'$. □

Let E be an elliptic curve defined over a field K of characteristic $p > 0$. One can show that for any prime $l \neq p$ the group ${}_{l^n}E(\bar{K})$ of points of order dividing l^n defined over the algebraic closure $\bar{K}$ of K is is isomorphic to $(\mathbb{Z}/l^n\mathbb{Z})^2$. Of course we know this fact when $K = \mathbb{C}$. Since for any $m \geq n$ we have a canonical homomorphism ${}_{l^m}E(\bar{K}) \to {}_{l^n}E(\bar{K})$ defined by multiplication by l^{m-n}. Passing to the projective limit we obtain a rank 2 free modulle $T_l(E)$ over the ring of l-adic numbers $\mathbb{Z}_l$. It is called the *Tate module* of E.

Let α be an endomorphism α of E (= a map of algebraic varieties which induces a homomorphism of groups $E(K) \to E(K)$). It defines a homomorphism of groups ${}_{l^n}E(K) \to {}_{l^n}E(K)$. Passing to the projective limit we obtain an endomomorphism of the Tate module

$$\rho_l(\alpha) : T_l(E) \to T_l(E).$$

It is called the *l-adic representation* of α.

We shall apply this to the case when $K = \mathbb{F}_p$ and $\alpha = F_p$ is the Frobenius endomorphism.

Theorem 13.5. *Let $a_p = p + 1 - \#E(\mathbb{F}_p)$ and r_p, r_p' are the roots of the polynomial $p - a_pT + T^2$. Then r_p, r_p' are algebraic integers, and considered as elements of the algebraic closure of the field $\mathbb{Q}_l$ of l-adic numbers they coincide with the eigenvalues of the l-adic representation of F_p on $T_l(E)$.*

Proof. We refer to the proof to [**Silverman**]. □

Remark 13.1. One should compare this result with the well-known Lefschetz formula in topology. If one interprets $T_l(E)$ as the first cohomology H^1 group of E, then the Lefschetz formula says that for any map f the set of fixed points of f (i.e. points x such that $f(x) = x$) is equal to the sum $\sum(-1)^{\mathrm{Trace}}(f^*|H^i)$. In our situation f is equal to the Frobenius map, and its fixed points are obviously the points $x = (a_0, \dots, a_n)$ satisfying $a_i^p = a_i$, or equivalently $x \in E(\mathbb{F}_p)$. We have $\mathrm{Trace}(f^*|H^1)$ is equal to the sum of eigenvalues of F_p in $T_p(E)$. Also $H^0 = H^2 = \mathbb{Z}_l$ and $\mathrm{Trace}(f^*|H^0) = 1$, $\mathrm{Trace}(f^*|H^2) = p$, the degree of the Frobenius map.

Now everything is ready to verify the Hasse-Weil conjecture for elliptic modular curve $X_0(N)$. Consider the characteristic polynomial of $\rho_l(F_p)$. It is equal to

$$P(T) = T^2 - a_pT + \det(\rho_l(F_p)).$$

We know that $\det(\rho_l(F_p)) = r_pr_p'$ is an algebraic integer, and by Hasse's theorem $|r_p + r_p'| \leq p^{1/2}$. This easily implies that $r_pr_p' = p$. Thus

$$P(t) = T^2 - a_pT + p.$$

Since $F_p \circ F_p' = p$, we see that $\rho_l(F_p) + \rho_l(F_p')$ acts on $T_l(E)$ as the multiplication by a_p. This implies that $F_p + F_p'$ is equal to a_p as an element of $\mathrm{Corr}(V_0(N)_p)$. By Eichler-Shimura's Theorem, the Hecke correspondence $\bar{T}(p) = a_p$. From this we obtain that $T(p) = a_p$ as a correspondence on $X_{\mathcal{H}}/\Gamma_0(N)$. It follows from Corollary 8.4 that $\dim \mathcal{M}_1(\Gamma_0(N))^0$ is one-dimensional. Let f be a non-zero parabolic form from this space normalized in such a way that its Fourier expansion is of the form $q+\sum_{n=2}^{\infty} c_n q^n$. Clearly, f is an eigenfunction for all the Hecke operators $T(n)$. By Lemma 11.3, $T(p)f = c_n f$. Comparing with the above, we obtain $c_p = a_p$. Thus the infinite product expansion for $Z_f(s)$ coincides with the infinite product for $L(X_0(N), s)$, up to a finitely may factors corresponding to prime p of bad reduction for $X_0(N)$. Using Weil's Convese Theorem it is not hard to deduce from this that the Dirichlet series of f coincides with the L-series of $X_0(N)$.

13.4 Let E be an elliptic curve over Q and $G = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ be the Galois group of the algebraic closure of $\mathbb{Q}$. It acts naturally on the group of $E(\bar{\mathbb{Q}})$ of $\bar{\mathbb{Q}}$-points of E. This action defines a linear representation of G in the Tate module of E:

$$\rho_{E,l} : G \to GL(T_l(E) \otimes \mathbb{Q}_l) \cong GL(2, \mathbb{Q}_l).$$

Now for any prime number p the group G contains a distinguished element Frob_p, called the*Frobenius element*. It is defined as follows. Let $\sigma_p \in Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ be the pre-image of the Frobenius automorphism of the residue field $\mathbb{F}_p$. Choose an embedding $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$ and define Frob_p as the image of σ_p under the inclusion $Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. Assume E has a good reduction modulo p and $p \neq l$. Then, one proves that

$$\rho_{E,l}(\mathrm{Frob}_p) = \rho_{\bar{E},l}(F_p),$$

where $\bar{E}$ is the reduction of E modulo p. Thus we have

$$\det(1 - \rho_{E,l}(\mathrm{Frob}_p)T) = \det(1 - \rho_{\bar{E},l}(F_p)T).$$

In particular, if $L(s, E) = Z_f(s)$ for some modular form $f \in \mathcal{M}_1(\Gamma_0(N))^0$, then

$$\det(1 - \rho_{E,l}(\mathrm{Frob}_p)T) = p - a_p T + T^2,$$

where a_p are the Fourier coefficients of f. Here we assume that f is an eigenvector for all the Hecke operators and $a_1 = 1$. We shall refer to such modular forms as *normalized eigenforms.*

Now let $f \in \mathcal{M}_k(\Gamma_0(N), \chi)^0$ be any cuspidal modular form with a Dirichlet character which has the previous properties. Let K be an extension of $\mathbb{Q}$ generated by the Fourier coefficients of f. We know that K is a finite extension. For any finite place λ of K let K_λ be the completion of K at λ. Deligne constructed a representation

$$\rho_{f,l} : G \to GL(2, K_\lambda)$$

such that for each prime p we have

$$\rho_{f,l}((\mathrm{Frob}_p) = p - a_p T + T^2.$$

This representation is irreducible and is uniquely defined. Conjugating by a matrix from $GL(2, K_\lambda)$ we may assume that the matrices defining this representation have coefficients in the ring of integers $\mathcal{O}_\lambda$ of K_λ. Reducing them modulo the maximal ideal, we obtain a representation

$$\bar{\rho}_{f,l} : G \to GL(2, \mathbb{F}),$$

where $\mathbb{F}$ is a finite field.

Definition. Let $\mathbb{F}$ be a finite field. A representation $\rho : Gal(\mathbb{Q}/\mathbb{Q}) \to GL(2, \mathbb{F})$ is called a *modular representation* if it arises from a normalized eigenform $f \in \mathcal{M}_k(\Gamma_0(N), \chi)^0$ for some N, k, and χ.

Note the modular representation has the property that $\rho(c) = -1$, where c is the complex conjugation automorphism of $\bar{\mathbb{Q}}$. Representations $Gal(\mathbb{Q}/\mathbb{Q}) \to GL(2, \mathbb{F})$ with this property are called *odd.*

Conjecture. *(J.-P. Serre) Any odd irreducible representation $Gal(\mathbb{Q}/\mathbb{Q}) \to GL(2, \mathbb{F})$ is modular unless F is of characteristic $p \leq 3$ and ρ is induced by a character of $Gal(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{-1}))$ if $p = 2$ and by a character of $Gal(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$ if $p = 3$.*

In fact, Serre gives a conjectural recipe for finding an appropriate (N, k, χ). For example, it predicts (N, k, χ) for representations arising by reduction modulo p from the p-adic representations $\rho_{E,p}$ associated to an elliptic curve E over $\mathbb{Q}$ with whose reductions are all either good or of multiplicative type (we say then that E has *stable reductions*). Then N is equal to the product of all primes $l \neq p$ such that the discriminant Δ_E of E has order at l not divisible by p; $k = p + 1$ if $\nu_p(\Delta_E)$ is not divisible by p and equals 1 otherwise; $\chi \equiv 1$.

Theorem 13.6. *Serre's conjecture implies Fermat's Last Theorem.*

Proof. Let (a, b, c) be a non-trivial solution of $x^n + y^n = z^n$. It is known that without loss of generality we may assume that $n = p \geq 5$ is prime and p does not divide a and b. Also we may assume that $a \equiv -1 \pmod 4$ and that b is even. Consider the elliptic curve E given by the Weierstrass equation

$$y^2 = x(x - a^p)(x + b^p).$$

It can be verified that E has semi-stable reductions and

$$\Delta_E = -2^8(abc)^{2p}.$$

In particular $p|\nu_p(\Delta_E)$. Consider the representation $\rho_{E,p}$ and it reduction modulo p. It can be checked that this representation is irreducible and odd. If Serre's Conjecture is true, then $\rho_{E,p}$ is a modular representation and Serre's recipe gives $N = 2, k = 1, \chi \equiv 1$. However, $\mathcal{M}_1(\Gamma_0(2))^0 = \{0\}$. □

13.5 For the following we shall use the notion of the *Jacobian variety* of a compact Riemann surface X. It is defined as a complex torus $J(X) = \mathbb{C}^g/\Lambda$, where g is equal to the genus of X and Λ is the lattice in $\mathbb{C}^9$ spanned by the vectors

$$\Pi_i = (\int_{\gamma_1} \omega_i, \ldots, \int_{\gamma_{2g}} \omega_i), \quad i = 1 \ldots, g$$

for some basis $\omega_1, \ldots, \omega_g$ of the space of holomorphic differentials on X and a basis $\gamma_1, \ldots, \gamma_{2g}$ of homology 1-cycles on X. Fixing a point $p_0 \in X$ we obtain a natural holomorphic map $i_{p_0} : X \to J(X)$ defined by the formula:

$$p \to (\int_{p_0}^{p} \omega_1, \ldots, \int_{p_0}^{p} \omega_g) \quad \text{modulo } \Lambda.$$

It is an isomorphism when $g = 1$. This map extends to a map from the group of divisors $\mathrm{Div}(X)$ by the formula

$$\tilde{i}_{p_0}(\sum n_p p) = \sum n_p i_{p_0}(p),$$

where the addition in $J(X)$ is the addition in the factor group of the additive group of $\mathbb{C}^g$. By *Abel's theorem* this map defines an isomorphism from the group of diviors on X modulo linear equivalence onto the group $J(X)$.

Let Z be a finite holomorphic correspondence on X, i.e. Z is a subvariety of $X \times X$ defining a finite correspondence on the set of points of X. As we saw in Lecture 11, Z defines a homomorphism from $\mathrm{Div}(X)$ to itself. It is easy to check that it sends principal diviors to principal divisors, and hence defines an endomorphism of the Jacobian variety $J(X)$. We shall apply this to the case when X is a modular curve and a correspondence is a Hecke correspondence on it.

Although we defined the Jacobian variety as a complex torus, one can develope a purely algebraic theory for $J(X)$ valid for nonsingular projective curves X defined over an arbitrary field K. In this theory $J(X)$ is a projective algebraic variety whose set of points $J(X)(K')$ over any extension K' of K has a natural structure of an abelian group. Also, for any point p_0 in $X(K)$ there is a regular map $i_{p_0} : X \to J(X)$ defined over the field K. It induces an isomorphism from the group of K-divisors on X modulo linear equivalence onto the group of K-points of $J(X)$. There is an analogue of the Tate module $T_l(J(X))$ for $J(X)$ and of the l-adic representation of $\mathrm{Gal}(\bar{K}/K)$ in it.

13.6 We know that the Hasse-Weil conjecture is true for an elliptic curve of the form $X_0(N)$. Let E be an elliptic curve over $\mathbb{Q}$, assume that, for some N, there exists a nonconstant regular map defined over $\mathbb{Q}$ from $X_0(N)$ to E. We say that E is a *modular elliptic curve* or a *Weil elliptic curve.*

Theorem 13.7. *Let E be a Weil curve. Then it satisfies the Hasse-Weil conjecture. Conversely, if E is an elliptic curve over $\mathbb{Q}$ satisfying the Hasse-Weil conjecture, then E is a Weil elliptic curve.*

Proof. We shall only sketch a proof. Suppose E satisfies the Hasse-Weil conjecture. Then $L(E,s) = Z_f$ for some newform $f \in \mathcal{M}_1(\Gamma_0(M)))^0_{new}$. For any prime p not dividing N_E, the characteristic polynomial of Frob_p coincide with respect to the l-adic representations $\rho_{E,l}$ and $\rho_{f,l}$. Using the continuity of the l-adic reprsentation and the fact that the Frobenius elements form a dense subset in the Galois group G of $\mathbb{Q}$ (the Chebotarev theorem) we obtain that $\rho_{E,l} = \rho_{f,l}$. Now let us consider f as a holomorphic differential form on $X_0(M)$. Since f is an eigenfunction for the the Hecke ring $\mathbf{T}_M$, we have a character $\theta : \mathbf{T}_M \to \mathbb{Q}$ defined by the eigenvalues. Let T be the kernel of θ. The Hecke ring acts on $X_0(M)$ via correspondences, and hence acts on its Jacobian variety $J_0(M)$ via endomorphisms. Let $A = J_0(M)/TJ_0(M)$. This an abelian variety and its tangent space is naturally isomorphic to $\mathbb{C}f$. In particular, A is a elliptic curve. Applying the Eichler-Shimura theorem, we can show that the characteristic polynomial of Frob_p in the l-adic representation of A is expressed in terms of the Hecke operators:

$$\det(\rho_{A,l}(\mathrm{Frob}_p) - tI_2) = t^2 - \theta(T(p)t + p\theta(T(p,p)).$$

This allows us to verify that $L(E,s) = L(A,s)$. By a theorem of G. Faltings, the elliptic curves E and A are isogeneous over $\mathbb{Q}$, and in particular their conductors are equal. This will imply that $N_E = M$, and there exists a regular map over $\mathbb{Q}$ from $J_0(N)$ to E. Composing it with an embedding of $X_0(N)$ in $J_0(N)$ we obtain that E is modular.

Now assume that E is a Weil elliptic curve and let $X_0(N) \to E$ be a regular map over $\mathbb{Q}$. The space of holomorphic differential forms on E is one-dimensional over

$\mathbb{C}$. By constructing a certain "Neron model" of E over $\mathbb{Z}$ one produces a certain 1-form, whose pre-image on $X_0(N)$ is a holomorphic differential form such that, after identifying it with a cusp form f of weight 1, its Fourier coefficients at infinity are rational numbers. Again by the Eichler-Shimura theorem one can check that f is an $\mathbf{T}^{(N)}$-eigenform with eigenvalues λ_p of $T(p)$ satisfying $\lambda_p = p + 1 - \#E(\mathbb{F}_p)$ for all prime p not dividing N. Projecing it to the subspace of $\mathcal{M}_1(\Gamma_0(N))^0_{new}$ we find a newform f. Applying some results of Deligne-Langlands-Carayol one can show that $L(E,s) = Z_f(s)$. □

We now see that the Hasse-Weil conjecture is equivalent to the following:

Conjecture. *(Shimura-Taniyama-Weil) an elliptic curve over $\mathbb{Q}$ is a Weil elliptic curve.*

We have seen already that Serre's Conjecture implies Fermat's Last Theorem. It was shown by K. Ribet and B. Mazur, that the fact that the elliptic curve used for the proof of Ferma is modular implies the Ferma Theorem. Let us sketch the proof of the following:

Theorem 13.8. *The Shimura-Taniyama-Weil conjecture implies Fermat's Last Theorem.*

Proof. We apply the STW-conjecture to the elliptic curve E from the proof of Theorem 13.6. It is easy to compute its conductor N_E: it is equal to the product of primes divisors of $\frac{abc}{16}$. Consider, as in the proof of Theorem 13.6, the representation $\bar{\rho}_{E,p} : G \to GL_2(\mathbb{F}_p)$. If E is a Weil elliptic curve, the representation $\bar{\rho}_p$ is an irreducible modular representation of level N and weight 1 with trivial character χ. Let l be a prime divisor of N_E. We know that $p|\nu_l(\Delta_E)$ if $l \neq 2$. This implies that the representation $\bar{\rho}_{E,p}$ is finite at l. When $l \neq p$ this means that the restriction of $\bar{\rho}_{E,p}$ to $\mathrm{Gal}(\bar{\mathbb{Q}}_l/\mathbb{Q}_l)$ is unramified (i.e. factors through a representation of the Galois group of a finite unramified extension of $\mathbb{Q}$). When $p = l$, the definition is a little more technical, and we omit it. Now we apply a theorem of Mazur-Ribet which implies that $\bar{\rho}_{E,p}$ is modular of level N/l. Here we use the assumptions that $l|N$ but $p^2, l^2 \not| N_E$ and $l \not\equiv 1 \mod p$. After applying this theorem several times, we find that $\bar{\rho}_{E,p}$ is modular of level 2. Now we end as in the proof of Theorem 13.6 by finding contradiction with absence of parabolic modular form of level 1 for the group $\Gamma_0(2)$. □

Theorem 13.9. *(A. Wiles) An elliptic curve over $\mathbb{Q}$ with semi-stable reductions for each prime number is a Weil curve.*

Corollary 13.3. *Fermat's Last Theorem is true.*

Proof. Observe that the elliptic curve E used in the proof of theorem 13.8 has semi-stable reductions at each prime p. □

Exercises

13.1 Let E be an elliptic curve over a field K. Define the group law on the set of $E(K)$ of points of E with coordinates in K as follows. View a point P as a divisor of degree 1. Assume that $E(K) \neq \emptyset$. Fix a point $0 \in E(K)$. For any two points P, Q the space $L(P + Q - 0)$ is of dimension 1 over K (the Riemann-Roch Theorem). Thus there exists a unique postive divisor of degree 1 linearly equivalent to $P + Q - 0$. This divisor is denoted by $P \oplus Q$ and is called the sum of the points P and Q.

(i) Show that the the binary law of composition on $E(K)$ defined by $P \oplus Q$ is a commutative group.

(ii) Show that, when $K = \mathbb{C}$, the group law agrees with the group law on the complex torus $E(\mathbb{C})$.

13.2 Let E be an elliptic curve over an algebraically closed field K with the group law defined in the previous exercise. Let $f_0, \ldots, f_{n-1}$ be a basis of the space $L(nO)$. Show that

(i) the map $\phi : E \setminus \{O\} \to \mathbb{P}^{n-1}, \quad P \to (f_0(P), \ldots, f_{p-1}(P)$, has the image an algebraic curve C of degree n.

(ii) Let $\bar{C}$ be the closure of C in the projective space. Show that for any n-torsion point P there exists a hyperplane in $\mathbb{P}^{n-1}$ which intersects $\bar{C}$ at one point equal to $\phi(P)$.

(iii) Let $n = 3$. Fix a line L in $\mathbb{P}^2$ which is not a tangent to $\bar{C}$ and consider the map from $\bar{C}$ to L which assigns to a point $x \in \mathbb{C}$ the intersection point of the tangent of $\bar{C}$ at x with L. Use the Hurwitz formula to show that $\bar{C}$ has exactly nine 3-torsion points if K is of characteristic 0.

(iv) Assuming that $n = 3$ and E has at least 3 torsion points of order 3, show that the equation of $\bar{C}$ can be chosen in the Hesse form $x^3 + y^3 + z^3 + \lambda xyz = 0$.

(v) Show that in the case K is of characteristic 3, there are at most 3 points of order 3 on E.

13.3 Let χ be a Dirichlet character modulo m. Define the Dirichlet series $L_m(s;\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$. Show that

(i) $L_m(s;\chi)$ is absolutely convergent for $res > 0$ and admits an infinite product expansion

$$L_m(s;\chi) = \prod_{p \not| m} (1 - \chi(p) p^{-s})^{-1}.$$

(ii) Show that $L_m(s;\chi)$ admits a holomorphic extension to the entire complex plane which satisfies the functional equation

$$L_m(1-s;\bar{\chi}) = L_m(s,\chi)(m/2\pi)^s \Gamma(s)(e^{\pi i s/2} + \chi(-1)e^{-\pi i s/2} G(\chi)^{-1},$$

where $G(\chi)$ is the Gauss sum of χ.

Index