Modular Forms

Cormac Grindall, Hussein Hijazi, Carlos Tapp

1 Modular group

1.1 Definitions

Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \hat{\mathbb{C}}$ and define

$$gz := \frac{az + b}{cz + d}$$

then one can easily see that

$$\frac{az + b}{cz + d} = \frac{a(x + iy) + b}{c(x + iy) + d} = \frac{ax + b + iay}{cx + d + icy} \cdot \frac{cx + d - icy}{cx + d - icy} = \frac{iy(-axc - bc + acx + ad)}{|cz + d|^2} = \frac{iy}{|cz + d|^2}$$

so that $\mathrm{Im}(gz) = \dfrac{\mathrm{Im}(z)}{|cz + d|^2}$ which shows that $\mathbb{H}$ is stable under action of $\mathrm{SL}_2(\mathbb{Z})$.

Note further that $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} z = \dfrac{-z}{-1} = z$ acts trivially on $\mathbb{H}$, hence the group

$$\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$$

acts faithfully on $\mathbb{H}$. Let $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{SL}_2(\mathbb{R})$ be the discrete subgroup with coefficients in $\mathbb{Z}$.

Definition 1.1

The group $G = \mathrm{SL}_2(\mathbb{Z})/{\pm 1}$ is called the **modular group**, i.e. the image of $\mathrm{SL}_2(\mathbb{Z})$ in $\mathrm{PSL}_2(\mathbb{R})$

1.2 Fundamental domain of the modular group

Let $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ be elements in G. Then one has

$$Sz = -1/z, \quad Tz = z + 1, \quad S^2 = 1, \quad (ST)^3 = 1$$

Let D be the subset of $\mathbb{H}$ formed of all points of z $\mathbb{H}$ formed by all points z such that $|z| \geq 1$ and $|\mathrm{Re}(z) \leq 1/2|$, then we have the figure below representing the orbit of D under the subset

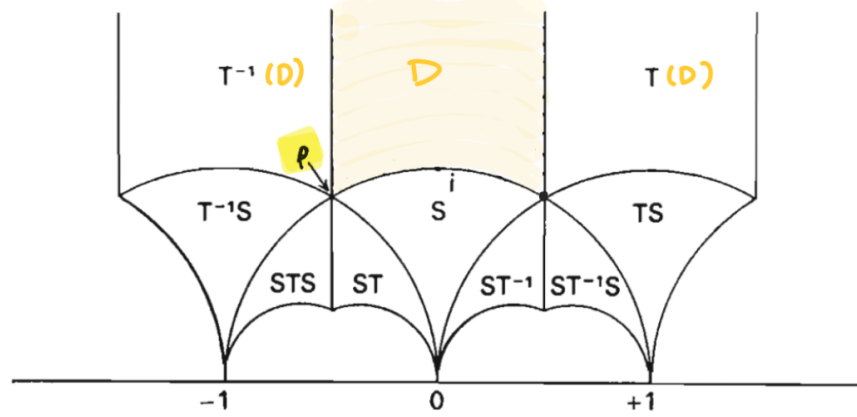$$\left\{1, T, TS, ST^{-1}S, S, ST, STS, T^{-1}S, T^{-1}\right\}$$

of the group G.

Figure 1

Theorem 1.2

(i) For every $z \in \mathbb{H}$, there exists $g \in G$ such that $gz \in D$.

(ii) Suppose that two distinct points z, z' of D are congruent modulo G. Then, $\operatorname{Re}(z) = \pm 1/2$ and $z = z' \pm 1$, or $|z| = 1$ and $z' = -1/z$

(iii) Let $z \in D$ and let $I(z) = \{g \mid g \in G, gz = z\}$ the stabilizer of z in G. One has $I(z) = \{1\}$ except in the following cases:

    (a) $z = i$ in which case $I(z)$ is the group of order 2 generated by S;

    (b) $z = \rho = e^{2\pi i/3}$, in which case $I(z)$ is the group of order 3 generated by ST ;

    (c) $z = -\hat{\rho} = e^{\pi i/3}$, in which case $I(z)$ is the group of order 3 generated by TS

Proof.
(i) Let $G' \subset G$ be the subgroup generated by S and T and let $z \in \mathbb{H}$. We seek to prove that there exsits $g' \in G'$ such that $g'z \in D$ which will prove assertion (1). If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an element of G' then as before $\operatorname{Im}(gz) = \frac{\operatorname{Im}(z)}{|cz+d|^2}$. Since c and d are integers, the number of pairs (c, d) such that $|cz + d|$ is less than a given constant is finite, thus there is a choice $g \in G'$ such that $\operatorname{Im}(gz)$ is maximized.
Chose $n \in \mathbb{Z}$ such that $-1/2 < | < \operatorname{Re}(T^n gz)|1/2$ (show that this necessarily exists). The element $z' = T^n gz$ belongs to D as $|z| \geq 1$ because otherwise the element $\operatorname{Im}(-1/z') > \operatorname{Im}(z')$ which is impossible. Set $g' = T^n g$ which is the element we are looking for and note that $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ ■

Now let $z \in D$ and $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ such that $gz \in D$. We may assume $\operatorname{Im}(gz) \geq \operatorname{Im}(z)$ i.e $|cz + d|^2 \leq 1$ by replacing the pair (z, g) by (gz, g^{-1}) if needed. Since c is an integer, the only cases to check which satisfy this inequality are $c = -1, 0, 1$.

2

If $c = 0$ then $d = \pm 1$ for which $g = \begin{pmatrix} 1 & \pm b \\ 0 & 1 \end{pmatrix}$ so that g acts by translation, i.e $gz = z \pm b$. Since both $|\operatorname{Re}(z)|, |\operatorname{Re}(gz)| < 1/2$ then either $b = 0, g = 1$ or $b = \pm 1$ in which case $\operatorname{Re}(z) = \pm 1/2$ and $\operatorname{Re}(gz) = -\operatorname{Re}(z)$.

If $c = 1$ then $|cz + d| \leq 1$ implies $|z + d| \leq 1$. Hence $d = 0$ except when $z = \rho, \widetilde{-\rho}$, in which cases $d = 0, 1$ or $d = 0, -1$ If $d = 0$, $|z| \leq 1$ so $|z| = 1$ since we are in D. But $ad - bc = 1$ implies $b = -1$. Hence $gz = a - 1/z \in D$so as above, $a = 0$ or $\operatorname{Re}(-1/z) = \pm 1/2$. Then $-1/z \in D$, $|-1/z| = 1$ thus $-1/z = \rho$ or $-\widetilde{\rho}$ and $z = \rho$ or $-\widetilde{\rho}$. In these cases, $a = 0, -1$ for $z = \rho$ and $a = 0, 1$ for $z \setminus \widetilde{\rho}$.

If $d = 1$, $z = \rho$ gives $a = b = 1$ so $g\rho = \frac{a-1}{1+\rho} = a + \rho$ thus $a = 0, 1$

If $d = -1, z = -\widetilde{\rho}$ then $g(-\widetilde{\rho}) = (a + (-\widetilde{\rho}))$ similarly and $a = 0, -1$. This proves (ii). ∎

For (iii), suppose $g \in G$, $z \in D$ and $gz = z$. In particular, $gz \in D$ so we can use what we did for (ii). There are two possibilities:

If $c = 0$, then g is given by $\begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix}$ but $gz = z$ means $b = 0$ so $g = 1_G$.

If $c = \pm 1$, then there are three further situations: when $d = 0$, g is given by $\begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$. We know $gz \in D$ if and only if $a = 0$ and $|z| = 1$ or $z = \rho$ and $a = 0, -1$ or $z = -\widetilde{\rho}$ and $a = 0, 1$. But out of these possibilities we only have $gz = z$ $z = i \mapsto a = 0$ or $z = \rho \mapsto a = -1$ or $z = -\widetilde{\rho} \mapsto a = -1$.

When $d = 1$, then $z = \rho$ and $a = 0$ (to have $gz = z$).

When $d = -1$ then $z = -\widetilde{\rho}$ and $a = 0$.

Then assertions (1) and (2) imply

Corollary 1.3

The canonical map $D \to \mathbb{H}/G$ is surjective and its restriction to the interior of D is injective.

Theorem 1.4

The group G is generated by S and T.

Proof. Let G' be the subgroup generated by S, T once more and $g \in G$. Choose a point $z_0 \in \mathring{D}$ and let $z = gz_0$. Since by Theorem 1.2, there exists $g' \in G'$ such that $g'z \in D$, the points z_0 and $g'z = g'gz_0$ of D are congruent modulo G and one of them is in $\mathring{D}$.

3

By assertions (2) and (3), the two points coincide and $g'g = 1$, hence $g \in G'$ as desired. ∎

2 Modular Functions

2.1 Defintions

Definition 2.1

We say a function f is **weakly modular of weight** $2k$ if is meromorphic on the half plane $\mathbb{H}$ and verifies the relation
$$f(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right), \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ k \in \mathbb{Z}$$

We denote g as the image of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in G. Then
$$\frac{\mathrm{d}(gz)}{\mathrm{d}z} = \frac{\mathrm{d}}{\mathrm{d}z}\left(\frac{az + b}{cz + d}\right) = \frac{(cz + d)(a) - (az + b)(c)}{(cz + d)^2} = \frac{ad - bc}{(cz + d)^2} = \frac{1}{(cz + d)^2}$$
Then by Definition 2.1
$$f(z) = (cz + d)^{-2k} f(gz) \implies \frac{f(gz)}{f(z)} = \left(\frac{\mathrm{d}(gz)}{\mathrm{d}z}\right)^{-k} \iff f(gz)\mathrm{d}(gz)^k = f(z)\mathrm{d}z^k$$
This is to be read as the *differential form of weight* k, $f(z)\mathrm{d}z^k$ is invariant under G.

Theorem 1.4 shows G is generated by S and T, so we only need to check the invariance on these generators.

Proposition 2.2

Let f be meromorphic on $\mathbb{H}$. The function f is a weakly modular function of weight $2k$ if and only if it satisfies the two relations:
$$f(z + 1) = f(z) \quad (f(Tz) = f(z))$$
$$f\left(\frac{-1}{z}\right) = z^{2k} f(z) \quad (f(Sz) = z^{2k} f(z))$$

Proof. $\implies$
Suppose f is weakly modular, then taking $g = T \in \mathrm{SL}_2(\mathbb{Z})$, we see
$$f(z) = 1^{-2k} f\left(\frac{z + 1}{1}\right) = f(z + 1)$$

and taking $g = S$ instead

$$f(z) = z^{-2k} f\left(\frac{-1}{z}\right) \implies f\left(\frac{-1}{z}\right) = z^{2k} f(z)$$

$\impliedby$

Suppose the two relations are satisfied, then since S and T generate G, for any $g \in G$, we can find $f(gz)$ by applying the respective relations implied by S and T. We need only show that the correct factor of $(cz + d)^{-2k}$ arises. Let

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

Note that since $S^2 = -1 \equiv 1 \pmod{G}$, then start with base cases $V = T$ and $V = S$ and using induction on

$$V = T^{n_1} S T^{n_2} S T^{n_3} S \dots$$

its trivial to see the correct factor fall out. ∎

By the first relation, we can show that f may be expressed as a function of $q = e^{2\pi i z}$.

Proof. Indeed, since $f(z) = f(z + 1)$, then f is 1-periodic. We can then define an equivalence relation on $\mathbb{H}$ by

$$z \sim w \iff z - w \in \mathbb{Z}.$$

So that the new domain of interest is the image of $\mathbb{H}$ in $\mathbb{C}/\mathbb{Z}$. Let

$$q : \mathbb{C}/\mathbb{Z} \to \mathbb{C}$$
$$z \mapsto e^{2\pi i z}$$

This map is well-defined because if $[z] = [z']$ (i.e. $z = z' + k$ for some $k \in \mathbb{Z}$) then

$$q(z) = e^{2\pi i z} = e^{2\pi i z} e^{2\pi i k} = e^{2\pi i (z+k)} = q(z')$$

and furthermore this map is injective because

$$e^{2\pi i z} = e^{2\pi i w} \iff e^{2\pi i (z - w)} = 1 \iff z - w \in \mathbb{Z} \iff z \sim w.$$

which implies that q has a left inverse, $p : \mathbb{C} \to \mathbb{C}/\mathbb{Z}$ so that $p \circ q = \mathrm{Id}_{\mathbb{C}/\mathbb{Z}}$.

f, being 1-periodic, can be considered as a function from $\mathbb{C}/\mathbb{Z} \to \mathbb{C}$, whence

$$f = f \circ \mathrm{Id}_{\mathbb{C}/\mathbb{Z}} = f \circ (p \circ q) = (f \circ p) \circ q : \mathbb{C}/\mathbb{Z} \to C$$

So we see that f can be written as a function of q and hence denote

$$\widetilde{f}(q(z)) = (f \circ p)(q(z)), z \in \mathbb{C}$$

and essentially $\widetilde{f}(z) = f\left(\frac{\log q}{2\pi i}\right) = \widetilde{f}(q)$ ∎

Since f is meromorphic on $\mathbb{H}$, then $\widetilde{f}$ is meromorphic on $D := \{q(z) \mid |q| < 1, q(z) \neq 0\}$

If $\widetilde{f}$ extends to a meromorphic (resp. holomorphic) function at the origin, we say, BY ABUSE OF LANGUAGE, that f is meromorphic (resp. holomorphic) at infinity, i.e. $\widetilde{f}$ admits a

Laurent expansion around a neighborhood of 0

$$\widetilde{f}(q) = \sum_{-\infty}^{\infty} a_n q^n$$

where $a_n = 0$ for n small enough (resp. for $n < 0$).

> **Definition 2.3**
>
> A weakly modular function is called **modular** if it is meromorphic at infinity. We set $f(i\infty) = \widetilde{f}(0)$ and call it the **value at infinity**

> **Definition 2.4**
>
> A modular function which is holomorphic everywhere (including infinity) is called a **modular form**; if such a function is zero at infinity, it is called a **cusp form** ("Spitzenform" in German — "forme parabolique" in French)

Then a modular form of weight $2k$ admits power series expansions

$$f(z) = \sum_{0}^{\infty} a_n q^n = \sum_{0}^{\infty} a_n e^{2\pi i n z}$$

which converges when $|q| < 1$ (i.e. for $\text{Im}(z) > 0$) which is obviously 1-periodic and VERIFY

$$f\left(\frac{-1}{z}\right) = z^{2n} f(z)$$

and is a cusp form when

$$f(i\infty) = 0 \implies \widetilde{f} = 0 \implies a_0 = 0$$

Claim: If f and f' are of weight $2k$ and $2k'$, respectively, the product ff' is a modular form of weight $2k + 2k'$

> **Proof.** Obviously as
> $$f(z)f'(z) = (cz+d)^{-2k} f(gz)(cz+d)^{-2m} f'(gz) = (cz+d)^{-2(k+m)}(f \cdot f')(gz)$$
> ∎

2.2 Lattice functions and modular functions

> **Definition 2.5**
>
> Let V be a real vector space of finite dimension. Then a subgroup Γ is called a **lattice** if it satisfies one of the following equivalent conditions:
> (a) Γ is discrete and V/Γ is compact;
> (b) Γ is discrete and generates the $\mathbb{R}$-vector space V;

(c) There exists an $\mathbb{R}$-basis $(e_1, \ldots, e_n)$ of V which is a $\mathbb{Z}$-basis of Γ (i.e. $\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$)

Denote the set of lattices of $\mathbb{Z}$ by $\mathscr{R}$ (here $\mathbb{C}$ is considered as a dimension two real vector space). Let M be the set of pairs $(\omega_1, \omega_2) \in \mathbb{C}^* \times \mathbb{C}^*$ such that $\text{Im}(\omega_1/\omega_2) > 0$,i.e

$$M := \{(\omega_1, \omega_2) \in \mathbb{C}^* \times \mathbb{C}^* : \text{Im}(\omega_1/\omega_2) > 0\}$$

To such a pair we associate the lattice

$$\Gamma(\omega_1, \omega_2) = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

with basis given by (ω_1, ω_2).

Claim: The map $\Gamma : M \to \mathscr{R}$ is surjective

Proof. Indeed, if Γ is a lattice (using definition (c)) then there exist ω_1, ω_2, a basis of $\mathbb{C}$ (a basis of $\mathbb{R}^2$), such that

$$\Gamma = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

Since they form a basis, neither are 0 so that $(\omega_1, \omega_2) \in \mathbb{C}^* \times \mathbb{C}^*$. That is, (ω_1, ω_2) generate Γ as a $\mathbb{Z}$-module

Either ω_1/ω_2 already lies in the upper half-plane or if it doesn't, we can reorder the basis and then ω_2/ω_1 will. $\blacksquare$

Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ and let $(\omega_1, \omega_2) \in M$. Set $\omega_1' := a\omega_1 + b\omega_2, \omega_2' := c\omega_1 + d\omega_2$ so that

$$g \cdot (\omega_1, \omega_2) := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = (a\omega_1 + b\omega_2, c\omega_1 + d\omega_2) = (\omega_1', \omega_2')$$

Then we see that

$$\Gamma(\omega_1', \omega_2') = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2' = \mathbb{Z}(a\omega_1 + b\omega_2) \oplus \mathbb{Z}(c\omega_1 + d\omega_2)$$

so that $\{\omega_1', \omega_2'\}$ is also a basis of $\Gamma(\omega_1, \omega_2)$. Then set $z = \omega_1/\omega_2$ and $z' = \omega_1'/\omega_2'$ and hence

$$z' = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\left(\frac{\omega_1}{\omega_2}\right) + b}{c\left(\frac{\omega_1}{\omega_2}\right) + d} = \frac{az + b}{cz + d} = gz$$

which shows $\text{Im}(z') > 0$ (since $\mathbb{H}$ is stable under the action of $\text{SL}_2(\mathbb{Z})$ and thus $(\omega_1', \omega_2') \in M$

Proposition 2.6

For two elements of M to define the same lattice, it is necessary and sufficient that they are congruent modulo $\text{SL}_2(\mathbb{Z})$

Proof. Above we have shown one direction, where if they are congruent modulo $\mathrm{SL}_2(\mathbb{Z})$, i.e

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

then they define the same lattice.

In the other direction, suppose (ω_1, ω_2) and ω_1', ω_2' define the same lattice. Then there are integers $a, b, c, d, e, f, g, h \in \mathbb{Z}$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} \qquad \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

but then this implies

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Then, since the entries are integers, taking determinants on both sides we see that the determinant of each matrix is ± 1. But since $\mathrm{Im}(\omega_1/\omega_2) > 0$ and $\mathrm{Im}(\omega_1'/\omega_2') > 0$, the determinants can not be negative otherwise these ratios would have opposite imaginary parts. Therefore, they differ exactly by matrices in $\mathrm{SL}_2(\mathbb{Z})$. ∎

Therefore, we have a bijection

$$\mathscr{R} \longleftrightarrow {}^M\big/_{\mathrm{SL}_2(\mathbb{Z})}$$

Now let $\mathbb{C}^*$ act on $\mathscr{R}$ (resp. on M) By

$$\Gamma \mapsto \lambda\Gamma \quad (\text{resp. } (\omega_1, \omega_2) \mapsto (\lambda\omega_1, \lambda\omega_2)), \quad \lambda \in \mathbb{C}^*$$

> **Proposition 2.7**
>
> The map $(\omega_1, \omega_2) \mapsto \omega_1/\omega_2$ gives, by passing to the quotient, a bijection of ${}^{\mathscr{R}}\big/_{\mathbb{C}^*}$ onto ${}^{\mathbb{H}}\big/_G$. Thus, an element of ${}^{\mathbb{H}}\big/_G$ can be identified with a lattice of $\mathbb{C}$ defined up to homothety (i.e. $\Gamma' = \lambda\Gamma$ for some $\lambda \in \mathbb{C}^*$)

Proof. By the action of $\mathbb{C}^*$ on $\mathscr{R}$, we have the well defined bijection

$$\Psi : {}^M\big/_{\mathbb{C}^*} \longleftrightarrow \mathbb{H}$$
$$(\omega_1, \omega_2) \mapsto \omega_1/\omega_2$$
$$(z, 1) \mapsfrom z$$

Now let $g \in \mathrm{SL}_2(\mathbb{Z})$, then we have

$$\Psi(g \cdot (\omega_1, \omega_2)) = g \cdot \Psi(\omega_1, \omega_2)$$

$$\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\left(\frac{\omega_1}{\omega_2}\right) + b}{c\left(\frac{\omega_1}{\omega_2}\right) + d}$$

Thus

$$\frac{M/_{\mathbb{C}^*}}{\mathrm{SL}_2(\mathbb{Z})} \underset{\text{nat bij}}{\Longleftrightarrow} \mathbb{H}/_G$$

But

$$\frac{M/_{\mathbb{C}^*}}{\mathrm{SL}_2(\mathbb{Z})} \cong \frac{\mathcal{R}}{\mathbb{C}^*}$$
$$\lambda(\omega_1, \omega_2) \mapsto \lambda\Gamma(\omega_1, \omega_2)$$

∎

Remark: Every lattice Γ can be associated to the elliptic curve $\mathbb{C}/_\Gamma$. Then two lattices define isomorphic elliptic curves if and only if they are homothetic. Thus the bijection in the previous proposition can be thought of as isomorphism classes of elliptic curves.

Let $F : \mathcal{R} \to \mathbb{C}$ and $k \in \mathbb{Z}$. We say that F is of *weight* $2k$ if for all $\Gamma \in \mathcal{R}$ and $\lambda \in \mathbb{C}^*$, the following holds

$$F(\lambda\Gamma) = \lambda^{-2k}F(\Lambda)$$

If $(\omega_1, \omega_2) \in M$, then denote $F(\omega_1, \omega_2)$ to be the value $F(\Gamma(\omega_1, \omega_2))$. Then the previous relation becomes

$$F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-2k}F(\omega_1, \omega_2)$$

Claim: $F(\omega_1, \omega_2)$ is invariant by the action of $\mathrm{SL}_2(\mathbb{Z})$ on M

Proof. Proposition 2.6 shows that the action of $\mathrm{SL}_2(\mathbb{Z})$ preserves the lattice structure, hence the image of a lattice Γ under F is also preserved by this action

$$F(\Gamma) = F(g\Gamma), \quad g \in \mathrm{SL}_2(\mathbb{Z})$$

∎

Claim: The product $\omega_2^{2k}F(\omega_1, \omega_2)$ only depends on $z = \omega_1/\omega_2$

Proof. Suppose $\omega_1/\omega_2 = \omega_1'/\omega_2'$. Then

$$\omega_2^{2k}F(\omega_1, \omega_2) = \omega_2^{2k}F\left(\omega_2\left(\frac{\omega_1}{\omega_2}\right), \omega_2\left(\frac{\omega_2}{\omega_2}\right)\right) = F(\omega_1/\omega_2, 1)$$
$$= F(\omega_1'/\omega_2', 1)$$
$$= (\omega_2')^{2k}F(\omega_1', \omega_2')$$

So, $\omega_2^{2k}F(\omega_1, \omega_2)$ is a function of ω_1/ω_2, an element of $\mathbb{H}$.

∎

Thus, as a result, there exists a function $f : \mathbb{H} \to \mathbb{C}$ such that

$$F(\omega_1, \omega_2) = \omega_2^{-2k}f(\omega_1/\omega_2)$$

9

Since F is invariant by $\mathrm{SL}_2(\mathbb{Z})$, we see that f satisfies

$$\omega_2^{-2k} f(\omega_1/\omega_2) = (c\omega_1 + d\omega_2)^{-2k} f\left(\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2}\right)$$

Let $z \in \mathbb{H}$ and take $(\omega_1, \omega_2) = (z, 1)$, then f satisfies the modular relation

$$f(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right), \quad \forall z \in \mathbb{H}$$

It also holds that we can associate any function f which satisfies this relation to a function $F : \mathscr{R} \to \mathbb{C}$ of weight $2k$. Indeed, define

$$F : M \to \mathbb{C}$$

$$(\omega_1, \omega_2) \mapsto \omega_2^{-2k} f(\omega_1/\omega_2)$$

Then this satisfies the invariance under $\mathrm{SL}_2(\mathbb{Z})$ and the relation $F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-2k} F(\omega_1, \omega_2)$. So let

$$F : \mathscr{R} \to \mathbb{C}$$

$$\Gamma_0 \mapsto F(\Gamma_0) := F((\omega_1, \omega_2))$$

with (ω_1, ω_2) any element in M such that $\Gamma((\omega_1, \omega_2)) = \Gamma_0$ With these realizations, we have proved the correspondence

$$\{\text{modular functions of weight } 2k \longleftrightarrow \text{lattice functions of weight } 2k\}$$

2.3 Examples of modular functions; Eisenstein series

> **Lemma 2.8**
>
> Let Γ be a lattice in $\mathbb{C}$. The series
>
> $$\sum_{\gamma \in \Gamma \setminus \{0\}} \frac{1}{|\gamma|^\sigma}$$
>
> converges for $\sigma > 2$

Proof. Let δ be the minimum distance between points in Γ and consider the annulus

$$A := \{z \in \mathbb{C} \mid r < |z| < r + \delta/2\}$$

Any two lattice points in this annulus are separated by an arc along the inner radius of length at least $\delta/2$. Then it follows that A contains at most $4\pi r/\delta$ lattice points and the number of lattice points in an annulus $\{n \le |\gamma| \le n+1\}$ is bounded above by cn, where

$$c \le \frac{2}{\delta} \cdot \frac{4\pi r}{\delta} = \frac{8\pi}{\delta^2}$$

Then we have

$$\sum_{\substack{\gamma \in \Gamma \setminus \{0\} \\ |\gamma| \geq 1}} \frac{1}{|\gamma|^{\sigma}} \leq \sum_{n=1}^{\infty} \frac{cn}{n^k} = c \sum_{n=1}^{\infty} \frac{1}{n^{k-1}} < \infty$$

since $\sigma > 2$. Thus we see

$$\sum_{\gamma \in \Gamma \setminus \{0\}} \frac{1}{|\gamma|^{\sigma}} = \sum_{\substack{\gamma \in \Gamma \setminus \{0\} \\ 0 < |\gamma| < 1}} \frac{1}{|\gamma|^{\sigma}} + \sum_{\substack{\gamma \in \Gamma \setminus \{0\} \\ |\gamma| \geq 1}} \frac{1}{|\gamma|^{\sigma}} < \infty$$

since the first summation is also clearly bounded. ∎

Definition 2.9

For $k > 1$ and $\Gamma \in \mathscr{R}$, the **Eisenstein series of index** k is defined as

$$G_k(\Gamma) := \sum_{\gamma \in \Gamma \setminus \{0\}} \frac{1}{\gamma^{2k}}$$

which converges absolutely by the previous lemma

By the bijection in the previous section, we can also view G_k as

$$G_k(\omega_1, \omega_2) = \sum_{(m,n) \in (\mathbb{Z} \times \mathbb{Z}) \setminus \{0\}} \frac{1}{(m\omega_1 + n\omega_2)^{2k}}$$

Then, this is a lattice function, and from the previous discussion we know

$$G_k(\omega_1, \omega_2) = \sum_{(m,n) \in (\mathbb{Z} \times \mathbb{Z}) \setminus \{0\}} \frac{1}{(m\omega_1 + n\omega_2)^{2k}} = \omega_2^{-2k} f(\omega_1/\omega_2)$$

$$\implies G_k(z) = \sum_{(m,n) \in (\mathbb{Z} \times \mathbb{Z}) \setminus \{0\}} \frac{1}{(mz + n)^{2k}}$$

which is also absolutely convergent and $z = \omega_1/\omega_2$. The function on $\mathbb{H}$ corresponding to G_k is, by slight abuse of notation, also denoted G_k (this is okay because of the procedure from the previous section).

Proposition 2.10

Let $k > 1$ be an integer. The Eisenstein series $G_k(z)$ is a modular form of weight $2k$. We have $G_k(i\infty) = 2\zeta(2k)$ where ζ denotes the Riemann zeta function. Actually, one can show

$$G_k(z) = 2\zeta(2k) + \frac{2^{k+1}\pi^{2k}(-1)^k}{(2k-1)!} \sum_{1}^{\infty} \sigma_{2k-1}(n) e^{2\pi i n z}$$

where $\sigma_k(n) = \sum_{d|n} d^k$.

Proof. We have already shown $G_k(z)$ is a weakly modular function of weight $2k$, that is
$$G_k(z) = (cz + d)^{-2k} G_k \left(\frac{az + b}{cz + d} \right), \quad \forall z \in \mathbb{H}, g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$
It remains to show that it is holomorphic everywhere (including infinity).
Recall a theorem of Weierstrass in complex analysis

> **Theorem 2.11**
>
> Suppose $\{f_n\}$ is a sequence of functions holomorphic on an open set Ω and that $\{f_n\}$ converges to a function f uniformly on every compact subset of Ω. Then f is holomorphic on Ω.

We have that the truncated series defined by $G_k(z)$ is uniformly and absolutely convergent and each term of the series is holomorphic on $\mathbb{H}$, so necessarily by the theorem $G_k(z)$ is holomorphic on all of $\mathbb{H}$.

Finally, we check holomorphicity at $i\infty$. Since we know $G_k(z)$ is weakly modular, we need only look at its behavior on the fundamental domain D. In view of the uniform convergence in D, we check $G_k(i\infty)$ in a term by term limit. For $z \neq 0$, we have

$$\lim_{\mathrm{Im}\, z \to \infty} G_k(z) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \left(\lim_{\mathrm{Im}\, z \to \infty} \frac{1}{(mz+n)^{2k}} \right)$$

When $m \neq 0$, the summation vanishes. So assume $m = 0$, then it becomes

$$\sum_{n \neq 0} \frac{1}{n^{2k}} = 2 \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = 2\zeta(2k)$$

■

The Eisenstein series of lowest weights are when $k = 2, 3$ which make G_2 and G_3 modular forms of weight 4 and 6 respectively. The theory of elliptic curves suggests the convenience of defining the multiples

$$g_2 = 60 G_2, \quad g_3 = 140 G_3$$

Then we have

$$g_2(i\infty) = 120 \zeta(4) = \frac{4}{3} \pi^4, \quad g_3(i\infty) = \frac{8}{27} \pi^6$$

Then set $\Delta = g_2^3 - 27 g_3^2$.

Claim: Δ is a cusp form of weight 12.

> **Proof.** Clearly g_2^3 is a modular form of weight $4 \cdot 3 = 12$ and g_3^2 is a modular form of weight $6 \cdot 2 = 12$, therefore Δ is one as well. We need only check the value of Δ at $i\infty$.
> $$\Delta(i\infty) = g_2^3(i\infty) - 27 g_3^2(i\infty) = \left(\frac{4}{3} \right)^3 \pi^{12} - 27 \left(\frac{8}{27} \right)^2 \pi^{12} = 0$$

Recall the Weierstrass function associated to Γ

$$\wp_\Gamma(u) = \frac{1}{u^2} + \sum_{\gamma \in \Gamma \setminus \{0\}} \left(\frac{1}{(u-\gamma)^2} - \frac{1}{\gamma^2} \right)$$

In the Laurent expansion of $\wp_\Gamma$, we see

$$\wp_\Gamma(u) = \frac{1}{u^2} + \sum_{k=2}^{\infty} (2k-1)G_k(\Gamma)u^{2k-2}$$

and setting $x = \wp_\Gamma(u), y = \wp_\Gamma'(u)$, we have

$$y^2 = 4x^3 - g_2 x - g_3$$

Up to a constant, Δ as defined above is the discriminant of the polynomial expression on the RHS. One can show that the cubic equation in $\mathbb{CP}^2$ is isomorphic to the elliptic curve $\mathbb{C}/\Gamma$.

3 The space of modular forms

3.1 The zeros and poles of a modular function

> **Definition 3.1**
>
> If $f \not\equiv 0$ is meromorphic function on $\mathbb{H}$ and $p \in \mathbb{H}$, the integer n such that $\frac{f}{(z-p)^n}$ is holomorphic and non-zero at p, denoted by $v_p(f)$, is called the **order** or **valency** of f at p

<u>**Claim:**</u> $v_p(f(z)) = v_{g(p)}(f(z))$

Proof. The goal is to use the argument principle around small balls around p and $g(p)$. Starting with the modular relation

$$f(z) = (cz + d)^{-2k} f(g(z)), \quad \forall g \in \text{SL}_2(\mathbb{Z})$$

Let $h(z) = (cz + d)^{2k}$ and note it is holomorphic everywhere on $\mathbb{H}$. Then taking derivatives we get

$$f'(z) = h(z)f'(gz)g'(z) + h'(z)f(g(z))$$

which gives

$$\begin{aligned} \frac{\mathrm{d}f}{f} = \frac{f'(z)\mathrm{d}z}{f(z)} &= \frac{h(z)f'(g(z))g'(z) + h'(z)f(g(z))}{h(z)f(g(z))} \\ &= \frac{f'(g(z))g'(z)\mathrm{d}z}{f(g(z))} + \frac{h'(z)\mathrm{d}z}{h(z)} \\ &= \frac{\mathrm{d}f(g(z))}{f(g(z))} + \frac{h'(z)\mathrm{d}z}{h(z)} \end{aligned}$$

13

By the argument principle and choice of sufficiently small balls $c_\epsilon(p)$ and $c_\epsilon g(p)$, we have

$$v_p(f) = \frac{1}{2\pi i} \int_{c_\epsilon(p)} \frac{df(z)}{f(z)} \quad v_p(f) = \frac{1}{2\pi i} \int_{c_\epsilon(g(p))} \frac{df(g(z))}{f(g(z))}$$

Substituting our derivation, it is immediate

$$v_p(f) = \frac{1}{2\pi i} \int_{c_\epsilon(p)} \frac{df(z)}{f(z)} = \frac{1}{2\pi i} \int_{c_\epsilon(p)} \left(\frac{df(g(z))}{f(g(z))} + \frac{h'(z)dz}{h(z)} \right) = v_{g(p)} f(z)$$

since the second integral vanishes as $h'(z)/h(z)$ is holomorphic. ∎

Thus, $v_p(f)$ only depends on the image of p in $\mathbb{H}/G$. Furthermore, $v_{i\infty}(f)$ is defined as the order of $q = 0$ in the extension $\widetilde{f}(q)$ defined previously. Denote the order of the stabilizer of the point p by e_p. Then

$$e_p = \begin{cases} 2 & \text{if } p \equiv i \pmod{G} \\ 3 & \text{if } p \equiv \rho \pmod{G} \\ 1 & \text{otherwise} \end{cases}$$

Theorem 3.2

Let f be a modular function of weight $2k$ not identically zero. One has

$$v_{i\infty}(f) + \sum_{p \in \mathbb{H}/G} \frac{1}{e^p} v_p(f) = \frac{k}{6}$$

or equivalently

$$v_{i\infty}(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{p \in (\mathbb{H}/G) \setminus \{i, \rho\}} v_p(f) = \frac{k}{6}$$

Since $\widetilde{f}$ as defined before is meromorphic, there exists $r > 0$ such that $\widetilde{f}$ has no zeroes or poles in the punctured open disk $0 < |q| < r$. This is equivalent to saying f has no zeroes or poles when $\operatorname{Im} z > \frac{1}{2\pi} \log(1/r)$. Then the portion of the fundamental domain D defined by the inequality $\operatorname{Im} z \leq \frac{1}{2\pi} \log(1/r)$ is compact. As f is meromorphic in $\mathbb{H}$, it only has a finite number of zeros and poles on this compact set and hence the summation defined above makes sense.
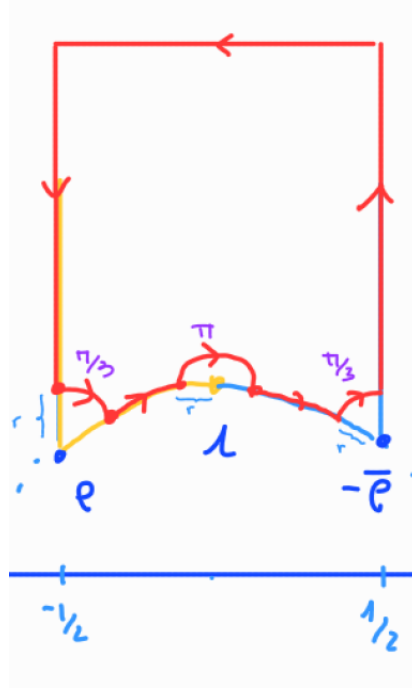
Proof.

Figure 2: The contour $\mathcal{C}_r$

Suppose f has no poles on the boundary of D except possibly at $\rho, -\widetilde{\rho}, i$. Then there exists a contour such that its interior contains a representative of each zero or pole of f not congrunet to i or ρ. (Note that $\rho = -1/\widetilde{\rho}$), so they are congruent by the S matrix).

Let $\mathcal{C}_r$ denote this contour with the path given by the Figure 1. Then by the argument principle, we know

$$\frac{1}{2\pi i} \int_{\mathcal{C}_r} \frac{\mathrm{d}f}{f} = \sum_{p \in (\mathbb{H}/G) \setminus i, \rho} v_p(f)$$

On the other hand, we can calculate the integral directly along the contour path. There are eight sections of the contour labeled $C_1, \ldots, C_8$ as in the figure.

15

For C_1, we have

$$\int_{C_1} \frac{\mathrm{d}f}{f} = \frac{\widetilde{f}(e^{2\pi i z}) 2\pi i z e^{2\pi i z}}{\widetilde{f}(e^{2\pi i z})} \mathrm{d}z = \int_{C_1} \frac{\widetilde{f}'(q(z)) q'(z)}{\widetilde{f}(q(z))}$$

$$= \int_{q(C_1)} \frac{\widetilde{f}'(q)}{\widetilde{f} q} \mathrm{d}q = -2\pi i v_0(\widetilde{f})$$

$$= -2\pi i v_{i\infty}(f) \implies \frac{1}{2\pi i} \int_{C_1} \frac{\mathrm{d}f}{f} \mathrm{d}z = -v_{i\infty}(f)$$

Since $f(z) = f(z+1)$ we have $f'(z) = f'(z+1)$ so clearly

$$\int_{C_2} \frac{\mathrm{d}f}{f} = -\int_{C_8} \frac{\mathrm{d}f}{f}$$

as C_2, C_8 have opposite orientation.

If we denote $C_{p,r,\alpha}$ an arc of a circle of radius r, angle α centered at $p \in \mathbb{C}$ with clockwise (negative) orientation, then if f has a zero or pole at p, we have

$$\lim_{r \to 0} \frac{1}{2\pi i} \int_{C_{p,r,\alpha}} \frac{\mathrm{d}f}{f} = -\frac{\alpha}{2\pi} v_p(f)$$

This implies

$$\lim_{r \to 0} \frac{1}{2\pi i} \int_{C_5} \frac{\mathrm{d}f}{f} = -\frac{1}{2} v_i(f)$$

$$\lim_{r \to 0} \frac{1}{2\pi i} \int_{C_3} \frac{\mathrm{d}f}{f} = -\frac{1}{6} v_\rho(f)$$

$$\lim_{r \to 0} \frac{1}{2\pi i} \int_{C_7} \frac{\mathrm{d}f}{f} = -\frac{1}{6} v_{\widetilde{\rho}}(f) = -\frac{1}{6} v_\rho(f)$$

Finally, for C_4, C_6, recall that $Sz = -1/z$ and note that it maps C_4 to $-C_6$ and also $f(z) = z^{-2k} f(Sz)$, so that

$$f'(z) = -2k z^{-2k-1} f(-1/z) + z^{-2k} f'(-1/z)(-1/z^2)$$

giving

$$\int_{C_4} \frac{\mathrm{d}f}{f} = \int_{C_4} \frac{-2k}{z} \mathrm{d}z + \int_{C_4} \frac{f'(S(z)) S'(z)}{f(S(z))} \mathrm{d}z = \frac{2\pi i k}{6} - \int_{C_6} \frac{f'(u)}{f(u)} \mathrm{d}u$$

and hence

$$\int_{C_4} \frac{\mathrm{d}f}{f} + \int_{C_6} \frac{\mathrm{d}f}{f} = 2\pi i k / 6$$

In total, we collect the equivalent integrations to get

$$\sum_{p \in (\mathbb{H}/G) \setminus i, \rho} v_p(f) = -v_{i\infty}(f) - \frac{1}{2} v_i(f) - \frac{1}{3} v_\rho(f) + \frac{k}{6}$$

and rearranging gives the desired relation.

In the case where f has zeroes or poles on the half-line

$$\{z \mid \mathrm{Re}(z) = -1/2, \mathrm{Im}\, z > \sqrt{3}/2\}$$

then $v_{T\lambda}(f) = v_\lambda(f)$ so we also have the contour in Figure 2 and with a bit more calculation we arrive to the same result.
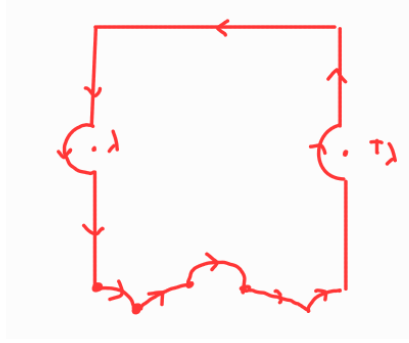

Figure 3

Any situation with more poles on the boundary of D can be dealt similarly. ∎

3.2 The algebra of modular forms

If $k \in \mathbb{Z}$, we denote M_k the $\mathbb{C}$-vector space of modular forms of weight $2k$ (resp. M_k^0 for cusp forms of weight $2k$). By definition of being cusp ($f(i\infty) = 0$), it is clear M_k^0 is the kernel of the linear map

$$M_k \to \mathbb{C}$$
$$f \mapsto f(i\infty)$$

Then M_k/M_k^0 has dimension at most 1. Moreover, for $k \geq 2$, the Eisenstein series $G_k(z)$ is an element of M_k such that $G_k(i\infty) \neq 0$ by Proposition 2.10. Hence, we have the isomorphism

$$M_k = M_k^0 \oplus \mathbb{C}G_k, \quad k \geq 2$$

Theorem 3.3

Recalling $g_2 = 60G_2$, $g_3 = 140G_3$ and $\Delta = g_2^3 - 27g_3^2 \in M_6^0$, then
(1) We have $M_k = 0$ for $k < 0$ and $k = 1$
(2) For $k = 0, 2, 3, 4, 5$, M_k is a vector space of dimension 1 with basis
$$\{1, G_2, G_3, G_4, G_5\}$$
and $M_k^0 = 0$
(3) Multiplication by Δ defines an isomorphism of M_{k-6} onto M_k^0

Proof.
(i) Suppose $k < 0$, then by Theorem 3.2 the sum of the orders would need to be a negative rational number. But as $f \in M_k$ is holomorphic, it only has zeros and no poles, hence the orders are positive. Therefore, when $k < 0$, M_k is empty.

Suppose $k = 1$, then once more the valency relation would result in the equation
$$n + \frac{n'}{2} + \frac{n''}{3} + n''' = \frac{1}{6}, \quad n, n', n'', n''' \in \mathbb{Z}$$
This equation has no solutions because each term is at least greater than $1/6$ itself when any of the chosen integers is non-trivial.

(iii) First, we make some observations

Claim: $v_\rho(G_2) = 1$, $v_p(G_2) = 0$ when $p \not\equiv \rho \pmod{G}$

Proof. Applying the valency relation to G_2, we get
$$\frac{2}{6} = n + \frac{n'}{2} + \frac{n''}{3} + n'''$$
The only solution to this is $n = n' = n''' = 0, n'' = 1$ ∎

Claim: $v_i(G_3) = 1$, $v_p(G_3) = 0$ when $p \not\equiv i \pmod{G}$

Proof. Applying the valency relation to G_3, we get
$$\frac{3}{6} = n + \frac{n'}{2} + \frac{n''}{3} + n'''$$
The only solution to this is $n = n'' = n''' = 0, n' = 1$ ∎

Claim: Δ does not vanish on $\mathbb{H}$ and has a simple zero at $i\infty$.

Proof. Notice that at i
$$\Delta(i) = g_2^3(i) \overset{0}{-} 27g_3^2(i) \neq 0$$
and hence Δ is not identically 0. Note that Δ has weight 12, and it is a cusp form as we have shown previously thus $v_{i\infty}(\Delta) \geq 1$. Then the valency relation becomes
$$v_{i\infty}(\Delta) + \frac{n'}{2} + \frac{n''}{3} + n''' = 1$$
and hence $v_{i\infty}(\Delta) = 1$ and $v_p(\Delta) = 0$ for $p \neq i\infty$. ∎

Now, if f has weight $2k$ then it $1/f$ has weight $-2k$. Let $f \in M_k^0$ and set $g = \frac{f}{\Delta}$ which has weight $2k - 12 = 2(k - 6)$. Moreover,
$$v_p(g) = v_p(f) - v_p(\Delta) = \begin{cases} v_p(f) & p \neq i\infty \\ v_p(f) - 1 & p = i\infty \end{cases}$$
Thus $v_p(g) \geq 0$ for all p and g is holomorphic everywhere. Hence, we have $g \in M_{k-6}$ and he process of either multiplying or dividing by Δ gives the isomorphism
$$M_{k-6} \cong M_k^0$$
(ii) For $k = 0, 2, 3, 4, 5$ one has $k - 6 < 0$. Thus $M_{k-6} = 0$ by part (i) and by (iii) $M_k^0 = 0$. Now since $\dim M_k/M_k^0 \leq 1$ then $\dim M_k \leq 1$. But $1, G_2, G_3, G_4, G_5$ are non zero in M_0, M_2, M_3, M_4, M_5 respectively we have $\dim M_k = 1$ when $k = 0, 2, 3, 4, 5$. ∎

Corollary 3.4

Noting that $[x]$ is the largest integer n such that $n \leq x$, we have
$$\dim M_k = \begin{cases} \left[\frac{k}{6}\right] & \text{if } k \equiv 1 \pmod 6, k \geq 0 \\ \left[\frac{k}{6}\right] + 1 & \text{if } k \not\equiv 1 \pmod 6, k \geq 0 \end{cases}$$

Proof.
Statements (i) and (ii) from Theorem 3.3 prove $0 \leq k < 6$ cases. Now recall that for $2 \geq k \geq 6$ we hvae the isomorphism $M_k = M_k^0 \oplus \mathbb{C} \cdot G_k$. Then it is seen
$$\dim M_k = 1 + \dim M_k^0 = 1 + \dim M_{k-6} \underset{\text{induc}}{=} \begin{cases} 1 + \left[\frac{k}{6} - 1\right] = \left[\frac{k}{6}\right] & \text{if } k \equiv 1 \pmod 6 \\ 1 + \left[\frac{k-6}{6} + 1\right] = 1 + \left[\frac{k}{6}\right] & \text{if } k \not\equiv 1 \pmod 6 \end{cases}$$
∎

Corollary 3.5

The space M_k has for basis the family of monomials $G_2^\alpha G_3^\beta$ with $\alpha, \beta \in \mathbb{Z}_{\geq 0}$ and $2\alpha + 3\beta = k$

Proof. First denote $A := \{G_2^\alpha G_3^\beta \mid \beta, \alpha \in \mathbb{Z}_{\{} \geq 0\}, 2\alpha + 3\beta = k\}$. By induction on k, we show that there are exactly $\dim M_k$ monomials in A by showing a generating set of appropriate dimension. For $k < 6$, this has already been shown by Theorem 3.3. Now for $k \geq 6$, a pair $\widetilde{\alpha}, \widetilde{\beta} \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ such that $2\widetilde{\alpha} + 3\widetilde{\beta} = k - 6$ gives for $(\widetilde{\alpha}, \widetilde{\beta} + 2) = (\alpha, \beta)$
$$2\alpha + 3\beta = 2\widetilde{\alpha} + 3\widetilde{\beta} + 2 \cdot 3 = k$$
and we get $\dim M_{k-6}$ many monomials $G_2^\alpha G_3^\beta$ in A. All the elements in A come from such pairs except if we can write $k = 2\alpha$ or $k = 2\alpha + 3$. Exactly one of these situations always happens so we get that
$$|A| = \dim M_{k-6} + 1 = \dim(M_k - 1) + 1 = \dim M_k$$
and thus the result follows
∎

Actually the table of bases looks like this

k	M_k	M_{k+1}	M_{k+2}	M_{k+3}	M_{k+4}	M_{k+5}
0	1	0	G_2	G_3	G_4	G_5
6	$\Delta M_0, G_6$	$\Delta M_1, G_7$	$\Delta M_2, G_8$	$\Delta M_3, G_9$	$\Delta M_4, G_{10}$	$\Delta M_5, G_{11}$
12	$\Delta M_6, G_{12}$	$\Delta M_7, G_{13}$	$\Delta M_8, G_{14}$	$\Delta M_9, G_{15}$	$\Delta M_{10}, G_{16}$	$\Delta M_{11}, G_{17}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

<u>**Remark:**</u> Let $M = \bigoplus_0^\infty M_k$ be the graded algebra defined by the direct sum of M_k and $\varepsilon : \mathbb{C}[X, Y] \to M$ be the homomorphism which maps $X \mapsto G_2$ and $Y \mapsto G_3$. The previ-

ous corollary says this is an isomorphism, hence M is identified with a polynomial algebra $\mathbb{C}[G_2, G_3]$.

3.3   The modular invariant

We set the so called j-invariant

$$j = \frac{1728g_2^3}{\Delta}$$

Proposition 3.6

(1) The function j is a modular function of weight 0
(2) It is holomorphic in $\mathbb{H}$ and has a simple pole at infinity
(3) It defines by passage to quotient a bijection $\mathbb{H}/G$ onto $\mathbb{C}$

Proof.
(i) g_2^3 and Δ are modular functions of weight 12, so their division results in a modular form of weight 0.
(ii) $\Delta \neq 0$ on $\mathbb{H}$ and has a simple zero at $i\infty$ by Theorem 3.3 and g_2 is holomorphic everywhere as it is a modular form.
(iii) The map is bijective if and only if for all $\lambda \in \mathbb{C}$ the modular form

$$f_\lambda = 1728g_2^3 - \lambda\Delta$$

has a unique zero modulo G. To see this, not f_λ is a modular form of weight 12 thus

$$v_{i\infty}(f_\lambda) + \frac{1}{2}v_i(f_\lambda) + \frac{1}{3}v_\rho(f_\lambda) + n = 1$$

The only situations where this holds correspond to the choices

$$(v_{i\infty}(f_\lambda), v_i(f_\lambda), v_\rho(f_\lambda)) = \{(1,0,0), (0,2,0), (0,0,3), (0,0,0)\}$$

and $n = 1$. This shows f_λ has a unique zero in $\mathbb{H}/G$ ∎

Proposition 3.7

Let f be a meromorphic function on $\mathbb{H}$. The following properties are equivalent:
(1) f is a modular function of weight 0
(2) f is a quotient of two modular forms of the same weight;
(3) f is a rational function of j.

Proof.
The implications $(i) \implies (ii) \implies (iii)$ are clear and so we show $(iii) \implies (i)$.
We may assume f is holomorphic on $\mathbb{H}$ because if not multiply f by a suitable polynomial in j. This new function would be holomorphic in $\mathbb{H}$ and by the following proof, a rational function of j, so f is too.
Since Δ is zero at $i\infty$, there exists $n \in \mathbb{N}$ such that $g = \Delta^n f$ is holomorphic at $i\infty$. By

construction, g is a modular form of weight 12 and then because of Proposition 3.6(ii) it is a $\mathbb{C}$-linear combination of $G_2^\alpha G_3^\beta$ where $2\alpha + 3\beta = 6n$. We may then assume that g is exactly $G_2^\alpha G_3\beta$, i.e.

$$f = \frac{G_2^\alpha G_3^\beta}{\Delta}$$

. If not, apply the following reduction: recall $6n = 2; \alpha + 3\beta$, thus the values $p = \alpha/3$ and $\beta/2$ are integers as

$$\alpha = \frac{6n - 3\beta}{2}$$

is divisible by 3 (similarly for q). Therefore, since $n = (2\alpha + 3\beta)/6 = \alpha/3 + \beta/2 = p + q$, one has

$$\frac{G_2^\alpha G_3^\beta}{\Delta^n} = \frac{G_2^{3p} G_3^{2q}}{\Delta^{p+q}}$$

So it remains to see that G_2^3/Δ and G_3^2/Δ are rational functions in j; this is obvious

$$G_2^3 = \frac{g_2^3}{60^3} \implies \frac{G_2^3}{\Delta} = \frac{1}{60^3} \cdot \frac{j}{1728}$$

$$G_3^2 = \frac{g_3^2}{140^2} = \frac{\Delta - g_2^3}{(-27)140^2} = \frac{\Delta - \frac{j\Delta}{1728}}{(-27)140^2} \implies \frac{G_3^2}{\Delta} = \frac{1728 - j}{(-27)(1728)(140)^2}$$

■

Remark: $\mathbb{H}/G$ can be compactified and j gives an isomorphism from its compactification onto the Riemann sphere $\mathbb{CP}^1 \cong S^2 = \mathbb{C} \cup \{\infty\}$

The coefficient $1728 = 2^6 3^3$ has been introduced so that j has residue 1 at infinity. More precisely, the series expansions is

$$j(z) = \frac{1}{q} + 744 + \sum_1^\infty c(n)q^n, \quad z \in \mathbb{H}, q = e^{2\pi i z}$$

Then one has

$$c(1) = 2^2 3^3 1823 = 196884, c(2) = 2^{11} \cdot 5 \cdot 2099 = 21493760$$

The $c(n)$ are integers and enjoy the remarkable divisibility properties when $a \geq 1$, the following

$$n \equiv 0 \ (\text{mod } 2^a) \implies c(n) \equiv 0 \ (\text{mod } 2^{3a+8})$$
$$n \equiv 0 \ (\text{mod } 3^a) \implies c(n) \equiv 0 \ (\text{mod } 3^{2a+3})$$
$$n \equiv 0 \ (\text{mod } 5^a) \implies c(n) \equiv 0 \ (\text{mod } 5^{a+1})$$
$$n \equiv 0 \ (\text{mod } 7^a) \implies c(n) \equiv 0 \ (\text{mod } 7^a)$$
$$n \equiv 0 \ (\text{mod } 11^a) \implies c(n) \equiv 0 \ (\text{mod } 11^a)$$

Now if we consider the monster group and we look at the list of degrees of irreducible $\mathbb{C}$-representations we get

$$1, 196883, 21296876, 842609376$$

The crazy part is that

$$196884 = 1 + 196883$$
$$21493760 = 1 + 196883 + 21296876$$
$$864299970 = 2 \cdot 1 + 2 \cdot 196883 + 21296876 + 842609376$$