MODULAR GROUPS

JOSHUA GEORGE

ABSTRACT. In this paper I have depicted the properties of Modular Groups and Modular forms and discussed a particular application of modular forms - Eisenstein series and introduce Elliptic curves.

CONTENTS

1. INTRODUCTION

In class we discussed about the Special linear groups $\mathrm{SL}_2(\mathbb{R})$ which is the set of all matrices with real entries such that the determinant is 1 with the group operations of matrix multiplication and inversion. This group is a *normal* subgroup of the General linear group $\mathrm{GL}_2(\mathbb{R})$ (set of 2×2 invertible matrices (1.1)).

Consider

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{R}, ad-bc = 1 \right\}.$$

And we define a group action on $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ via fractional linear transformations as follows

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathbb{H} \to \mathbb{H} \quad z \mapsto \gamma z = \gamma(z) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}, \quad z \in \mathbb{H}$$

Let $\Gamma := \mathrm{SL}_2(\mathbb{Z}) \leqslant \mathrm{SL}_2(\mathbb{R})$ (1.2) and $\mathrm{SL}_2(\mathbb{Z}) \circlearrowright \mathbb{H}$ as above (Here Γ is called the **Full Modular Group**). An action is faithful if the kernel of the action is trivial [**1**, **p. 39**] or equivalently for any $g \in G$ and $x \in X (G \circlearrowright X)$ there is no group elements except the identity

Date: December 7, 2021.

such that $gx = x$. In order to make this action faithful on $\mathbb{H}$ we define the **Modular Group** $\Gamma(1) := \Gamma/\{\pm I\}$ and this group acts faithfully on $\mathbb{H}$ (2.4).

1.1: $\mathrm{SL}_2(\mathbb{R}) \trianglelefteq \mathrm{GL}_2(\mathbb{R})$.
Proof: From [**1**, **p. 29**] a group is normal iff it is the kernel of some homomorphism. Let $\mathbb{R}^\times$ be the mult. group of non zero reals. Define the map:

$$\varphi : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^\times, \quad X \mapsto \det(X)$$

for each $X \in \mathrm{GL}_2(\mathbb{R})$. This map is well defined as for $X \in \mathrm{GL}_2(\mathbb{R}), \det(X) \neq 0$. Since $\det(XY) = \det(X).\det(Y)$ by properties of determinant this map is a homomorphism. Now the kernel of the homomorphism is

$$\operatorname{Ker}\varphi = \{X \in \mathrm{GL}_2(\mathbb{R}) | \det(X) = 1\} = \mathrm{SL}_2(\mathbb{R}) \text{ by def.}$$

Therefore $\mathrm{SL}_2(\mathbb{R}) \trianglelefteq \mathrm{GL}_2(\mathbb{R})$. ■

1.2: $\Gamma \leqslant \mathrm{SL}_2(\mathbb{R})$.
Proof: Γ is non empty as it contains I. Also $\forall X \in \Gamma$, $X^{-1} \in \Gamma$ as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

and $\frac{1}{ad-bc} = 1$. Therefore if we take $X, Y \in \Gamma$, $X.Y^{-1} \in \Gamma$ by matrix multiplication. ■

1.3: $\Gamma \times \mathbb{H} \to \mathbb{H}$ is a well defined group action.
Proof: First note that if $\mathrm{Im}(z) > 0$ then $\mathrm{Im}(\gamma z) > 0$ and that $\mathbb{H}$ is mapped to $\mathbb{H}$

$$\text{Well, } \gamma(z) = \frac{az+b}{cz+d} = \frac{(az+b)(d+c\bar{z})}{|cz+d|^2}$$
$$= \frac{bd + ac|z|^2 + Re(z)(ad+bc) + i(ad-bc)\,\mathrm{Im}(z)}{|cz+d|^2}$$
$$= \frac{bd + ac|z|^2 + \mathrm{Re}(z)(ad+bc) + i\,\mathrm{Im}(z)}{|cz+d|^2}$$

Hence, $\mathrm{Im}(\gamma z) = \frac{\mathrm{Im}(z)}{|cz+d|^2}$ and the action is well defined.

Now let $z \in \mathbb{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma$

Then ,

(i) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot z = z$

(ii) $\gamma(\gamma' z) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \dfrac{a'z+b'}{c'z+d'} = \dfrac{a\dfrac{a'z+b'}{c'z+d'} + b}{c\dfrac{a'z+b'}{c'z+d'} + d} = \dfrac{(aa'+bc')z + ab' + bd'}{(ca'+dc')z + cb' + dd'}$

$= \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix} z = (\gamma\gamma')z$ ■

2. Modular Groups

Formal Definition [**2**]: The modular group $\Gamma(1)$ is the group of linear fractional transformations of the upper half of the complex plane, which have the form

$$z \mapsto \frac{az+b}{cz+d}$$

where $a,b,c,d \in \mathbb{Z}$ and $ad-bc=1$.

2.1: $\{\pm I\} = Z(\Gamma))$ where $Z(\Gamma) := \{X \in \Gamma \,|\, \forall Y \in \Gamma, XY = YX\}$.
$(\subseteq)$ is trivial.
$(\supseteq)$ Fix $X = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in Z(\Gamma)$ and choose $Y = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Doing $YX = XY$ gives us the following equations, $bg = fc, c(e-h) = (a-d)g, (a-d)f = b(e-h)$.
Selection 1: Choose Y $\ni c = 0$ and $b \neq 0$ .The above equations become
$bg = 0, 0 = (a-d)g, (a-d)f = b(e-h)$ Since $b \neq 0 \implies g = 0$.
Selection 2: Choose Y $\ni b = 0$ and $c \neq 0$. Then
$0 = fc, c(e-h) = (a-d)g, (a-d)f = 0) \implies f = 0$.
Selection 3: Choose Y $\ni b \neq 0$. From the above deductions $f = 0 = g$,
$0 = 0, c(e-h) = 0, 0 = b(e-h) \implies e = h$ This means $X = \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} \in Z(\Gamma)$ and since $\det(X) = 1 \implies e \pm 1$. ■

Now we know $Z(\Gamma) \trianglelefteq \Gamma$ from [**1**]. Therefore since $Z(\Gamma) = \{\pm I\}$ and $Z(\Gamma)$ we conclude that $\Gamma(1)$ is a group [**1, p. 29**] as $\Gamma(1) := \Gamma/\{\pm I\}$ (def).

Generators of the full modular group Γ.

2.2: Γ and $\Gamma(1)$ are generated by S and T where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Proof: [**4**, **p.6**] Observe that $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, n \in \mathbb{Z}$.

$$T^n \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}$$

and $S^2 = -I$. Thus $S \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \cdots (\alpha)$

Now consider $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma)$

Case (1): Suppose $c = 0$

Then $ad = 1 \Rightarrow a = d = \pm 1 \implies g = \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix} = \begin{cases} T^{b'} & \text{if } a = d = 1 \\ \text{or} & \\ S^2 T' & \text{if } a = d = -1 \end{cases}$

Case (2): Suppose $c \neq 0$. WLOG, we can suppose $|a| \geqslant |c|$. (in terms of α-as the transformation S on say g flips the rows so if either one is bigger we can apply this transformation) By the division algorithm we can write $a = cq + r \quad 0 \leqslant r < |c|$

$$T^{-q}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a-cq & b-qd \\ c & d \end{pmatrix}$$

Well $a-cq < c$ as $r < |c|$ 1. Applying S we switch these entries (and the signs) and we applying the division theorem (ie repeating the above procedure) until we get the lower left entry equal to 0, but this means it has reached case 1 and we are done. ■

2.3: Every Automorphism of $\mathbb{H}$ is of the form $\gamma(z) = \frac{az+b}{cz+d}$ where $a,b,c,d \in \mathbb{Z}$ and $ad-bc = 1$.[**5**]

2.4: The group of Automorphisms of $\mathbb{H}$ is isomorphic to $\Gamma(1)$, $\mathrm{Aut}(\mathbb{H}) \cong \Gamma(1)$.
Proof: Consider the map,

$$\varphi : \Gamma \to \mathrm{Aut}(\mathbb{H}), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \gamma(z) = \frac{az+b}{cz+d}$$

This is a homomorphism as consider
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \gamma(z) = \dfrac{az+b}{cz+d}$, $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \longmapsto \gamma'(z) = \dfrac{a'z+b'}{c'z+d'}$ then the matrix product maps to the corresponding composition. That is, the product is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

while the corresponding composition is the image of the product,

$$(\gamma \circ \gamma')(z) = \frac{(aa'+bc')z+(ab'+bd')}{(ca'+dc')z+cb'+dd'}$$

Therefore this is a homomorphism.Its also surjective. The kernel of this map is $\{\pm I\}$. Now by the *First isomorphism theorem*, we get

$$\Gamma/\{\pm I\} \cong \mathrm{Aut}(\mathbb{H}) \Rightarrow \Gamma(1) \cong \mathrm{Aut}\mathbb{H})$$

(A really clean proof of this is also in [**6**, **p.3-5**]) ■

3. Fundamental Domain

Definition: Fundamental domain for the upper halfplane $\mathbb{H}$ under the action of Γ is a set $\mathbb{F}$ containing the representative of each orbit ($\mathscr{O}$) of $\mathbb{H}$ under Γ or equivalently the fundamental domain for Γ is a connected domain $\overline{\mathbb{F}}$ such that:

- $\forall z \in \mathbb{H}\ \exists\ \gamma \in \Gamma \ni \gamma(z) \in \mathbb{F}$
- if $z_1, z_2 \in \mathbb{F} \ni \gamma(z_1) = z_2$ for some $\gamma \in \Gamma$ then $z_1 = z_2$ and $\gamma = \pm I$.

Recall: Suppose $\Gamma \circlearrowleft \mathbb{H}$ then

$$\mathscr{O}_x = \{g.x \,|g \in \Gamma\} \iff \{y \in \mathbb{H} \,|g.x = y \text{ for some } g \in \Gamma\} \iff \{y \in \mathbb{H} \,|x \sim y\}$$

3.1: Fix $z \in \mathbb{H}$. The set $(m,n) \in \mathbb{Z}^2 \backslash (m,n) \neq (0,0)$ such that $|mz+n| \leqslant 1$ is finite and non empty.

Proof: Let $z = x + iy$, then
$|mz+n| \leqslant 1 \iff (mx+n)^2 + (my)^2 \leqslant 1 \implies (my)^2 \leqslant 1 \implies |m| < \frac{1}{\sqrt{y}}$, m is bounded. Also $|mz+n| \leqslant \implies -1 \leqslant mz+n \leqslant \implies -1-mx \leqslant n \leqslant 1-mx, n$ is bounded. Also, substituting $(m,n) = (0,1)$ shows its non empty. ■

3.2: Fundamental Domain.

(i) $\forall z \in \mathbb{H} \; \exists \; \gamma \in \Gamma \ni \gamma(z) \in \mathbb{F}$

(ii) Consider $z_1 \neq z_2$,

$$z_2 \in \mathscr{O}_\Gamma(z_1) = \{\tau | \gamma.z_1 = \tau, \gamma \in \Gamma\} \implies \begin{cases} \mathrm{Re}(z_1) = \pm\frac{1}{2}, z_2 = z_1 \mp 1 \\ |z_1| = 1, z_2 = \frac{-1}{z} \end{cases}$$

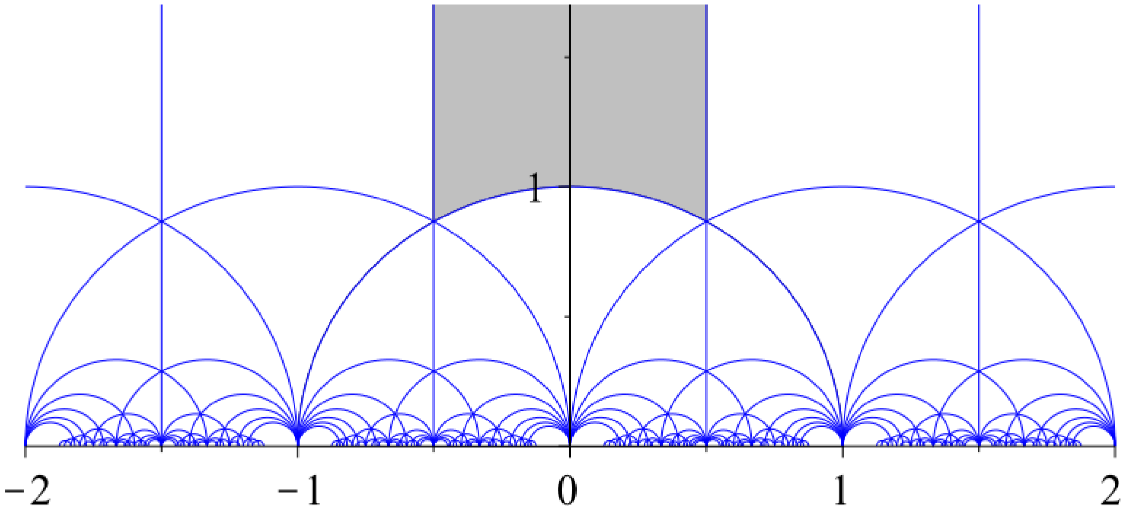
Recall: $T(z) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ which can be represented as $Tz = z+1, T^{-1}z = z-1$ and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ which is $Sz = \frac{-1}{z}$.

(iii) Let $z \in \mathbb{F}$ and $\mathrm{Stab}_\Gamma(z) = \{\gamma \mid \gamma \in \Gamma, \gamma z = z\}$ the stabilizer of $z \in \Gamma$. One has $\mathrm{Stab}_\Gamma(z) = \{\pm I\}$ except in the following cases:

- $z = i$
- $z = \rho = e^{2\pi i/3}$
- $z = -\bar{\rho} = e^{\pi i/3}$

The Fundamental Domain for Γ is the region

$$\mathbb{F} := \{z \in \mathbb{H} : |z| \geqslant 1, |\mathrm{Re}(z)| \leqslant \frac{1}{2}\}$$



(The grey area is the fundamental domain)

Proof: [**4**, **p.7-9**] [**7**, **p.3-5**]
Let $\gamma = \begin{pmatrix} k & l \\ m & n \end{pmatrix} \in \Gamma$.

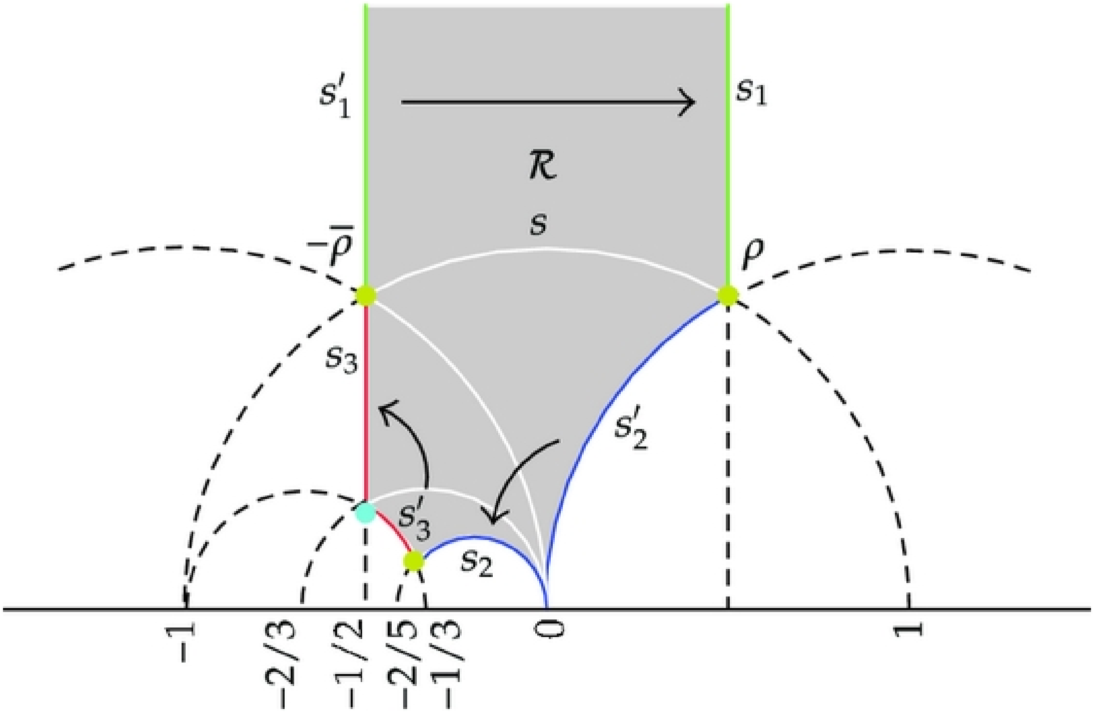
(i) Then,

$$\operatorname{Im}(\gamma z) = \frac{\operatorname{Im}(z)}{|mz+n|^2}, \quad (1.3)$$

As $(m,n) \neq (0,0)$,we see that $|mz+n|$ attains a minimum as γ varies over Γ (using lemma) .Now choose $|mz+n|$ to be minimal, therefore $\operatorname{Im}(\gamma z)$ is maximal for $\gamma \in \Gamma$
By translation we can ensure $|x| \leqslant \frac{1}{2}$, (this is so as we are always in the upper half plane so as we are trying to find the fundamental domain we can always ensure by translation (Orbit definition) that the real part is between -1/2 and 1/2) (Here translation means we can find $n \in \mathbb{Z} \ni \gamma(z) + n$ has real part $\leqslant 1/2$).
Now we claim $|\gamma z| \geqslant 1$. Suppose not, ie $|\gamma z| < 1$. Consider $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ where S acts on γz to yield $S(\gamma z) = \frac{-1}{\gamma z}$, Also $\operatorname{Im}(\frac{-1}{\gamma z}) = \frac{\operatorname{Im}(\gamma z)}{|\gamma z|^2}$ Therefore,

$$\operatorname{Im}(S\gamma z) = \frac{\operatorname{Im}(\gamma z)}{|\gamma z|^2} > \operatorname{Im}(\gamma z) \quad (\text{ as } \gamma z < 1)$$

Contradiction! (as $\operatorname{Im}(\gamma z)$ was assumed to be maximal).



(ii) (iii) Since $|z| \geqslant 1$ and $|\operatorname{Re}(z)| \leqslant \frac{1}{2}$, we get $\operatorname{Im}(z) \geqslant \frac{\sqrt{3}}{2}$ as their sum-squared $\geqslant 1$. We have to prove no two points in the interior of $\mathbb{F}$ share the same orbit.Assume $z_1, z_2 \in \mathbb{F}$ and WLOG that $\operatorname{Im}(z_2) \geqslant \operatorname{Im}(z_1)$ and there exists an $\gamma \in \Gamma \ni z_2 = \gamma(z_1)$. It follows that $\operatorname{Im}(z_2) = \operatorname{Im}(\gamma.z_1) = \operatorname{Im}(z_1)\,|mz_1+n|^{-2} \geqslant \operatorname{Im}(z_1)$. Hence $|mz_1+n|^2 \leqslant 1$ (as we need

$\frac{\mathrm{Im}(z_1)}{|mz_1+n|^2} \geqslant \mathrm{Im}(z_1))$. We know $\mathrm{Im}\,(z_1) \geqslant \frac{\sqrt{3}}{2}$, now,
$|mz_1+n|^2 = (m\mathrm{Re}(z_1)+n)^2 + (m\mathrm{Im}(z_1))^2 = m^2\mathrm{Re}(z_1)^2 + 2mn\mathrm{Re}(z_1) + n^2 + m^2\mathrm{Im}(z_1)^2 \geqslant m^2 + 2mn\mathrm{Re}(z_1) + n^2 \cdots (\alpha)$.
Suppose $|m| \geqslant 2$, (α) becomes,
$m^2 + 2mn\mathrm{Re}(z_1) + n^2 \cdots (\alpha) \geqslant 4 + 4n\mathrm{Re}(z_1) + n^2 \geqslant 4 + 2n + n^2$ (as max value of $\mathrm{Re}(z_1)$ is 1/2. Then $4+2n+n^2 = 4+n(2+n)$. The zeroes of $n(2+n)$ are when $n = 0, -2$ and its negative when $n = -1$. If $n = -1$ (this is the value for which the expression is smallest) then $4+2n+n^2 = 4-2+1 = 3 \lightning$. Therefore $|m| < 2 \implies m \in \{-1, 0, 1\}$. Now case by case consider,

Before I prove this note that:$(-\gamma)(z) = \dfrac{-kz-l}{-mz-n} = \dfrac{kz+l}{mz+n} = \gamma z$, this basically shows that the action γ is the same thing as the action $-\gamma$.
CASE 1: $m = 0, n = \pm 1, n \neq 1$ (by eq α). Since $kn - lm = 1$ we get that γ or $-\gamma$ must be equal to $T^j = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}$. But for $\gamma(z_1)$ to lie in $\mathbb{F}$ again only $\in \{-1, 0, 1\}$ are possible as T^j by definition takes $T^j z \mapsto z + j$. For $j = 0$, we have $z_1 = z_2$. For $j = \pm 1$ by the definition of T we see that z_2 and z_1 must lie on the boundary lines $\mathrm{Re}(z) = \pm\frac{1}{2}$ of F and hence not in the interior of F.

CASE 2: $m = 1$, by eq (α) $|n| \leqslant 1$. Suppose $n = 0, m = 1$, then $|z_1| = 1$(unit circle) as $|z_1| \geqslant 1$ and $|m_1 z + n| \leqslant 1$. Now $|z_1| = 1 = kn - lm = -l$. Therefore
$z_2 = \gamma(z_1) = \begin{pmatrix} k & -1 \\ 1 & 0 \end{pmatrix} = \dfrac{kz_1 - 1}{z_1} = k - \dfrac{1}{z_1}$. But $|\dfrac{-1}{z_1}| = \dfrac{1}{|z_1|} = 1$. This means $-1/|z_1|$ also belongs in the complex unit circle. The values of k which make this possible are: (We cant consider the points on the unit circle below the complex plane as we are considering the points on the upper half plane and consider the diagram)

- $k = 0$: then $\gamma z_1 = \dfrac{1}{z_1}$ multiplying both sides by z_1 we get $z_1^2 = -1 \implies z_1 = \pm i$, but since we are in $\mathbb{H}, z_1 = i$, but $\dfrac{1}{z_1} = i$. This gives us $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{Stab}_\Gamma(i)$.
- $k = 1$: suppose $\dfrac{-1}{z_1} = \rho \implies z_1 = -\overline{\rho}$, but $k - \dfrac{1}{z_1} = 1 - \dfrac{1}{z_1} = -\overline{\rho}$. Therefore we started with $-\overline{\rho}$ and its image is the same. Therefore $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{Stab}_\Gamma(-\overline{\rho})$
- $k = -1$: the exact same reasoning as above but here $z_1 = \rho$. Therefore $\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{Stab}_\Gamma(\rho)$.

In all the three above cases we get $z_2 = z_1$. Now suppose $n = 1$, then by (α) this is possible iff $\mathrm{Re}(z) = -1/2$. We get $1 \geqslant |mz_1 + n| = |z_1 + 1|$. The only point with the property is ρ (as $|\rho + 1| \leqslant 1$ is within the unit circle). Therefore let $z_1 = \rho$. We know $kn - lm = 1 = k - l$.
$z_2 = \gamma z_1 = \begin{pmatrix} k & l \\ 1 & 1 \end{pmatrix} \rho = \begin{pmatrix} k & k-1 \\ 1 & 1 \end{pmatrix} \rho = \dfrac{k\rho + k - 1}{\rho + 1} = \dfrac{k(\rho+1)}{\rho+1} - \dfrac{1}{\rho+1}$, but

$\rho+1=-\overline{\rho}$, we get $k-\frac{1}{-\overline{\rho}}=k+\rho$. The only values of k where this point is in $\mathbb{F}$ are the points when:

- $k=0$: we get $0+\rho$ we get the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \in \mathrm{Stab}_{\Gamma}(\rho)$ which fixes the point ρ.
- $k=1$: we get $1+\rho=-\overline{\rho}$

Now suppose $d=-1$: We take $z_1=-\overline{\rho}$ and eventually get two cases $k=-1, k=0$. We get the matrix $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in \mathrm{Stab}_{\Gamma}(-\overline{\rho})$

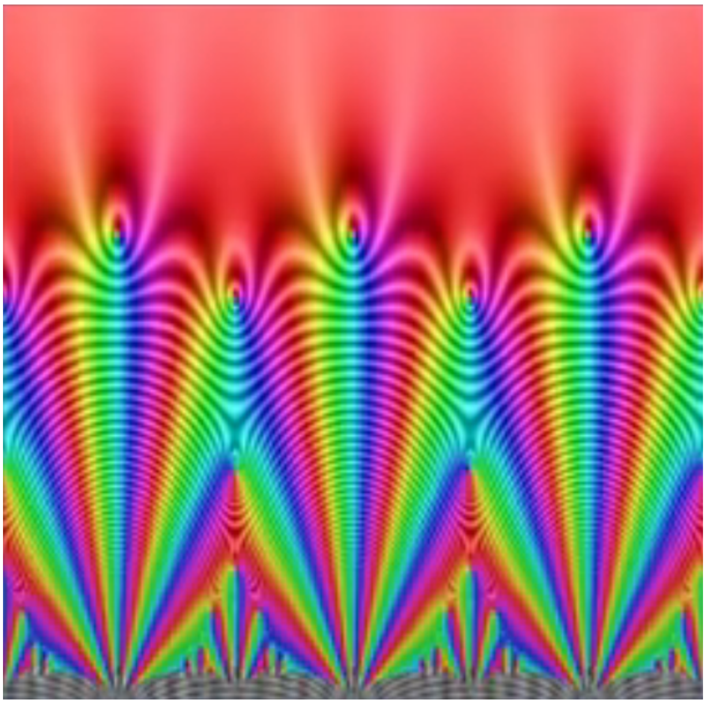
CASE 3: $m=-1$: Recall the action of γ is the same as $-\gamma$. Therefore, the proof follow from the case $m=1$. ■

4. Modular Forms

Definition: Holomorphic functions are complex differentiable functions.
Definition: A function $f:\mathbb{C}\to\mathbb{C}$ is said to be complex differentiable at $z\in\mathbb{C}$ if

$$\lim_{\substack{h\in\mathbb{C}\\ h\to 0}} \frac{f(z+h)-f(z)}{h}$$

exists. Again, if the limit exists, its value is called $f'(z)$. If f is complex differentiable at every $z\in U\subset\mathbb{C}$, then f is said to be holomorphic on U.



Modular form

Definition: [**4** , **p.1-2**] A modular form of weight k for

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}, ad-bc=1 \right\}$$

is a complex-valued function f on the upper half-plane $\mathbb{H}$ satisfying the following three conditions:

1. f is a holomorphic function on $\mathbb{H}$.
2. For any $z \in \mathbb{H}$ and any matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ as above, we have:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

3. As $\mathrm{Im}(z) \to \infty$, $f(z)$ is bounded.

Note:

- Consider $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$, well the modularity condition means $f(z+1) = (0z+1)^k f(z) = f(z)$.
- Consider $S = \begin{pmatrix} 0 & -1 \\ 1 & 10 \end{pmatrix} \in \Gamma$ the modularity condition means $f(\frac{-1}{z}) = (z)^k f(z)$.
- Consider $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \Gamma$ the modularity condition means $f(z) = (-1)^k f(z)$. If k is odd then the $f \equiv 0$.

4.1: If a function $f : \mathbb{H} \to \mathbf{C}$ satisfies the modularity condition with weight k for two matrices γ_1 and γ_2 in Γ then it satisfies the modularity condition with weight k for $\gamma_1\gamma_2$ and for the inverse γ_1^{-1}.

Proof. [**4**, **p.5**] Let $\gamma_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\gamma_2 = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. The modularity condition with weight k for these matrices says $f(\gamma_1 z) = (cz+d)^k f(z)$ and $f(\gamma_2 z) = (c'z+d')^k f(z)$ for all $z \in \mathbb{H}$. It follows that for all z,

$$\begin{aligned} f((\gamma_1\gamma_2)z) &= f(\gamma_1(\gamma_2 z)) \\ &= (c\gamma_2 z+d)^k f(\gamma_2 z) \\ &= (c\gamma_2 z+d)^k (c'z+d')^k f(z) \end{aligned}$$

Since $\gamma_2 z = (a'z+b')/(c'z+d')$, a calculation shows

$$(c\gamma_2 z+d)^k (c'z+d)^k = ((ca'+dc')z+(cb'+dd'))^k$$

so

$$f((\gamma_1\gamma_2)z) = ((ca'+dc')z+(cb'+dd'))^k f(z),$$

and the bottom matrix entries of

$$\gamma_1\gamma_2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} * & * \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

are exactly the " c " and " d " that appear when we write $f((\gamma_1\gamma_2)z)$ as $(cz+d)^k f(z)$. Thus f satisfies the modularity condition with weight k for $\gamma_1\gamma_2$.
We now want to prove that if $f(\gamma_1 z) = (cz+d)^k f(z)$ for all $z \in \mathbb{H}$ then the same condition holds with γ_1 replaced by γ_1^{-1}, which is $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ because γ_1 has determinant 1.
Replacing z with $\gamma_1^{-1}z$ in the modularity condition for the matrix γ_1, we get

$$f(z) = \left(c\left(\gamma_1^{-1}z\right)+d\right)^k f\left(\gamma_1^{-1}z\right)$$

for all z. Dividing both sides by $\left(c\left(\gamma_1^{-1}\right)+d\right)^k$,

$$f\left(\gamma_1^{-1}z\right) = \frac{1}{\left(c\gamma_1^{-1}z+d\right)^k} f(z)$$

for all z. Since $c\gamma_1^{-1}z+d = (ad-bc)/(-c_1z+a_1) = 1/(-cz+a)$,

$$f\left(\gamma_1^{-1}z\right) = (-cz+a)^k f(z)$$

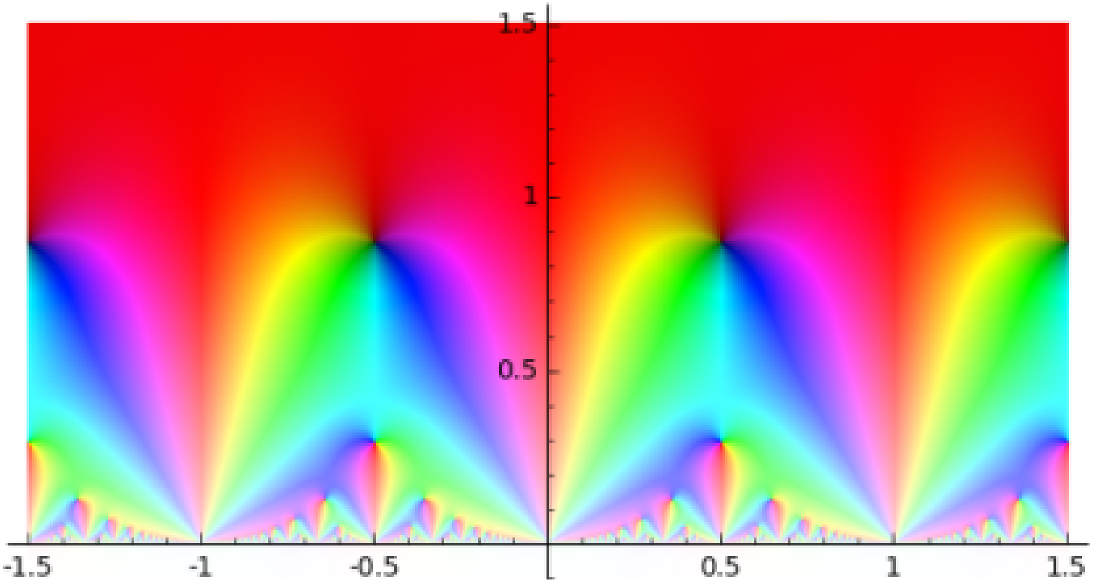
for all z, which is the modularity condition for γ_1^{-1} ■.

Note: (4.1) shows us that the set of all $\gamma \in \mathbb{Z}$ for which f satisfies the modularity condition with weight k is a subgroup of Γ.

4.2: [**4**, **p.5-6**] If the set $\{\gamma_1,\ldots,\gamma_m\}$ generates Γ and a function $f : \mathbb{H} \to \mathbf{C}$ satisfies the modularity condition with weight k for each γ_i then f satisfies the modularity condition with weight k for all of Γ.
Proof: From note, if the set $\{\gamma_1,\ldots,\gamma_m\}$ contains a set of generators of Γ then it is all of Γ.
■

Note: To check if a $f : \mathbb{H} \mapsto \mathbb{C}$ is a modular form we it suffices to check property (1), (3) from the definition of modular forms as well as the modularity condition $f(z+1) = f(z)$ and $f(\frac{-1}{z}) = z^k.f(z)$ as the group Γ is generated by T and S (ie if the function satisfies the conditions for T and S then its true for their products as the condition (2.2) is preserved under matrix multiplication and inversion).

5. Eisenstein Series



A modular form : Eisenstein series of weight 4

Definition: [**4** , **p.11**] For even $k \geqslant 4$, the weight k Eisenstein series is

$$G_k(z) := \sum_{\substack{(m,n)\in\mathbf{Z}^2\\(m,n)\neq(0,0)}} \frac{1}{(mz+n)^k}.$$

Definition:[**4** , **p.18**] The above can be also written as:

$$E_k(z) = \frac{1}{2} \sum_{\substack{(c,d)\in\mathbf{Z}^2\\\gcd(c,d)=1}} \frac{1}{(cz+d)^k}$$

5.1: The Eisenstein series $G_k(z)$ is absolutely convergent: for each $z \in \mathbb{H}$, the series $\sum_{(m,n)\neq(0,0)} 1/|mz+n|^k$ converges. [**4**, **p.11-12**]

5.2: For even $k \geqslant 4$, the Eisenstein series G_k is a modular form of weight k for Γ. [**4**, **p.12**]

5.3 [**4**, **p.18**] For even $k \geqslant 4$,

$$G_k(z) = 2\zeta(k).E_k(z)$$

Proof: Note $0 \neq a \in \mathbb{Z}, \gcd(a,0) = a$. For $(0,0) \neq (m,n) \in \mathbb{Z}^2$, with $\nu = \gcd(m,n)$,

$$\gcd\left(\frac{m}{\nu}, \frac{n}{\nu}\right) = 1 \quad \text{let } c = \frac{m}{\nu}, d = \frac{m}{\nu}$$

$$
\begin{aligned}
G_k(z) &= \sum_{(m,n)\in\mathbf{Z}^2} \frac{1}{(mz+n)^k} = \sum_{\nu\geqslant 1} \sum_{\substack{(c,d)\\ \gcd(c,d)=\nu}} \frac{1}{(c\nu z+d\nu)^k} \\
&= \sum_{\nu\geqslant 1} \frac{1}{\nu^k} \sum_{\substack{(c,d)\\ \gcd(c,d)=1}} \frac{1}{(cz+d)^k} = \zeta(k) \sum_{\substack{(c,d)\\ \gcd(c,d)=1}} \frac{1}{(cz+d)^k}
\end{aligned}
$$

These calculations are valid since the series $G_k(z)$ converges absolutely for all integers $k \geqslant 3$ It follows that

$$E_k(z) = \frac{1}{2} \sum_{\substack{(c,d)\in\mathbf{Z}^2\\ \gcd(c,d)=1}} \frac{1}{(cz+d)^k}$$

as the series defining G_k and E_k cancel to zero for odd k. ■

Definition: [**8** , **p.1**] For $z = x+iy \in \mathbb{H}, k = \sigma + it, \mathrm{Re}(k) > 1$ the non holomorphic eisenstein series is

$$G_k(z) = \frac{1}{2} \sum_{(0,0)\neq(m,n)\in\mathbb{Z}^2} \frac{\mathrm{Im}(z)^k}{|mz+n|^{2k}}$$

Definition:[**8** , **p.1**] The above series can also be written as

$$E_k(z) = \frac{1}{2} \sum_{(c,d)\in\mathbb{Z}^2, \gcd(c,d)=1} \frac{\mathrm{Im}(z)^k}{|cz+d|^{2k}}.$$

5.4: For all $z \in \mathbb{H}$ and $\mathrm{Re}\, k > 1$,

$$G_k(z) = \zeta(2k)E_k(z)$$

Proof: [**8** , **p.2**] Following a similar argument as the start of (5.2),

$$\gcd\left(\frac{m}{\nu}, \frac{n}{\nu}\right) = 1 \quad \text{let } c = \frac{m}{\nu}, d = \frac{m}{\nu}$$

Then

$$
\begin{aligned}
G_k(z) &= \frac{1}{2} \sum_{\nu\geqslant 1} \sum_{(m,n)\in\mathbb{Z}^2, \gcd(m,n)=\nu} \frac{y^k}{|mz+n|^{2k}} \\
&= \frac{1}{2} \sum_{\nu\geqslant 1} \sum_{(c,d)\in\mathbb{Z}^2, \gcd(c,d)=1} \frac{y^k}{|\nu cz+\nu d|^{2k}} \\
&= \frac{1}{2} \sum_{(c,d)\in\mathbb{Z}^2, \gcd(c,d)=1} \frac{y^k}{|cz+d|^{2k}} \sum_{\nu\geqslant 0} \nu^{-2k} \\
&= \zeta(2k)E_k(z)
\end{aligned}
$$

■

6. Elliptic Curves

(This section will contain a brief introduction to elliptic curves)

What is an elliptic curve?

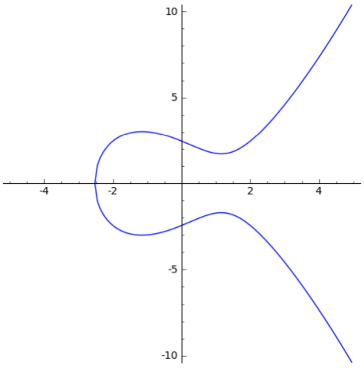


Figure 1. $y^2 = x^3 - 4x + 6$ over $\mathbb{R}$ **[9 , p.4]**

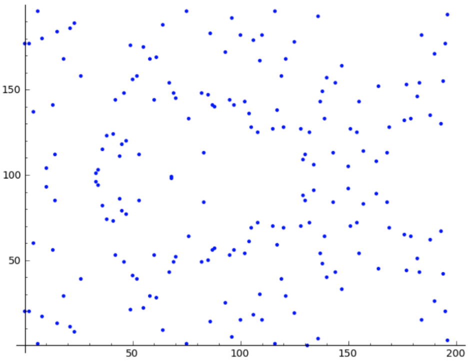


Figure 2. $y^2 = x^3 - 4x + 6$ over $\mathbb{F}_{197}$ **[9 , p.5]**

An Elliptic curve is an equation of the form

$$y^2 = x^3 + Ax + B, \quad \text{for some constants } A, B.$$

with discriminant

$$\Delta = 4A^3 + 27B^2 \text{ is nonzero.}$$

The main question mathematicians study for elliptic curves are how many rational numbers satisfy the equation $y^2 = x^3 + Ax + B$. Since there maybe infinitely many, we consider working over a finite field $\mathbb{F}_p = \{0, 1, \cdots p-1\}, p$ - prime. To make this a field we define operations $(+, \times)$ and are done $mod(p)$

Taniyama-Shimura Conjecture: The conjecture says that every rational elliptic curve over $\mathbb{Q}$ is a modular form .

7. Discussion

Throughout this paper I showed the following:

- Section 1, 2: I show the properties of the full modular group and modular group using concepts such as normal subgroups, group actions , automorphisms, generators and isomorphism theorem.
- Section 3: I discuss the definition of the fundamental domain which involves orbits and stablisers of the $\mathbb{H}$ under the action of Γ and how periodic functions under translations are invariant.
- Section 4, 5, 6: I introduce modular forms and the applications of the same - Eisensteins series and elliptic curves.

Note: The eisenstein series are automorphic as well ie : $\mathrm{E}_k(\gamma(z)) = \mathrm{E}_k(z)$, convergent and admits a fourier expansion as well!

ACKNOWLEDGEMENT

I would like to Thank God for giving me the wisdom to do this course and I would like to express my special gratitude to Professor Topaz who gave me the golden opportunity to do this project on the topic Modular Groups. It helped me in doing ample amount of research and I learnt many a things related to this topic.

I would also like to give special thanks to my parents and friends who supported me emotionally and physically during the course of this project.

REFERENCES

[1] Topaz, Adam. *Math 328: Introduction to Group Theory University of Alberta, Fall 2021* (2021).

[2] Modular Group. *Modular Group - From Wikipedia, the free encyclopedia*. Retrieved from `https://en.wikipedia.org/wiki/Modular_group` ([Online; accessed 3-December-2021])

[3] Edvardsson, Elisabet. *Modular forms for triangle groups*. (2017).

[4] Conrad, Keith. *MODULAR FORMS (DRAFT, CTNT 2016)*. (2016) `https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016/02/CTNTmodularforms.pdf`.

[5] Math3ma. *Automorphisms of the Upper Half Plane*. `https://www.math3ma.com/blog/automorphisms-of-the-upper-half-plane`([Online; accessed 5-December-2021])

[6] Jerry. *MATH 311: COMPLEX ANALYSIS — AUTOMORPHISM GROUPS LECTURE.*

[7] Hruza, Johannes and Trachsler, Manuel . *The modular group and the fundamental domain* (2019).

[8] Bell, Jordan . *Nonholomorphic Eisenstein series, the Kronecker limit formula, and the hyperbolic Laplacian*. (2014).

[9] Sutherland, Andrew . *18.783 Elliptic Curves*. (2017).