Principal congruence subgroup

and

Modular curve $X_{\Gamma(2)}$

Congruence subgroup $\Gamma(2)$

$$\Gamma(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2 \right\}$$

$$\overline{\Gamma(2)} := \Gamma(2)/\{\pm 1\} \subset PSL_2(\mathbb{Z})$$

Lemma: $\Gamma(2)$ is a normal subgroup of Γ_1 and

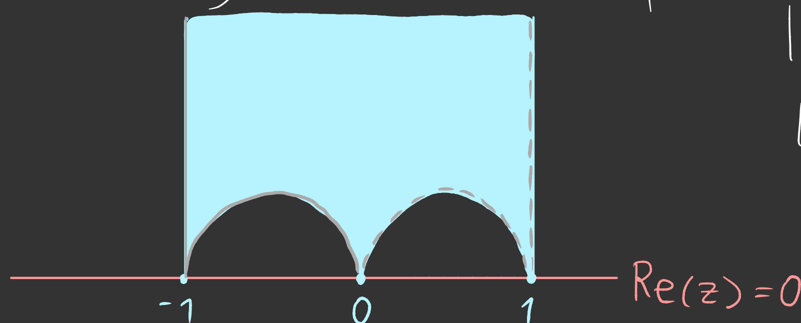
$[\Gamma_1 : \Gamma(2)] = 6.$

Theorem:

a) $\overline{\Gamma}(2)$ is freely generated by 2 elements:

$$A := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

b) $$\mathcal{F}_{\Gamma(2)} := \left\{ z \in \mathfrak{h} \;\middle|\; \begin{array}{l} \operatorname{Re}(z) \in [-1, 1) \\ |z + \tfrac{1}{2}| \geq \tfrac{1}{2} \\ |z - \tfrac{1}{2}| > \tfrac{1}{2} \end{array} \right\}$$



$\mathcal{F}_{\Gamma(2)}$ is a fundamental domain of the action of $\Gamma(2)$ on $\mathfrak{h}$.

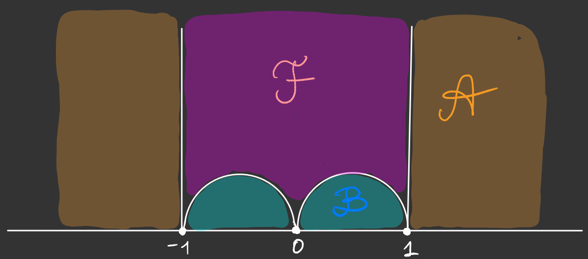
Proof:

Step 1: Show that there are no relations between A & B

Let $F(\alpha,\beta)$ be the free group with generators α & β

We will show that the map $\pi: F(\alpha,\beta) \to \overline{\Gamma(2)}$

given by $\pi: \alpha \mapsto \bar{A}$, $\beta \mapsto \bar{B}$ is injective.



Consider the following partition of $\mathfrak{h}$

$$\mathfrak{h} = \mathcal{F} \sqcup \mathcal{B} \sqcup \mathcal{A}$$

Claim 1:

- If $z \in \mathcal{F} \cup \mathcal{B}$ then $A^k z \in \mathcal{A}$ for all $k \in \mathbb{Z} \setminus \{0\}$

- If $z \in \mathcal{F} \cup \mathcal{A}$ then $B^k z \in \mathcal{B}$ for all $k \in \mathbb{Z} \setminus \{0\}$

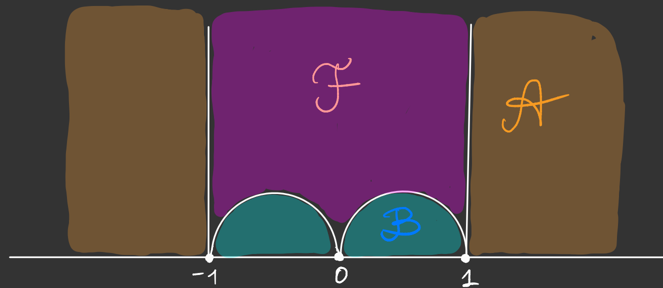
$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

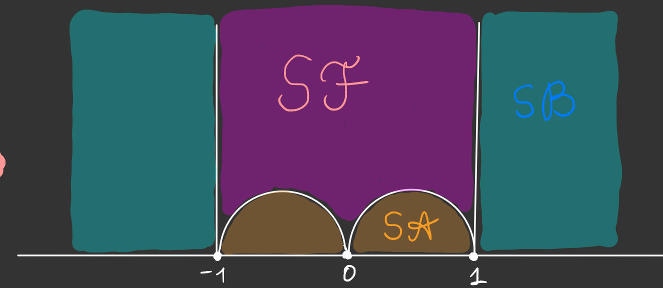
$$B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

$$SAS = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}$$

$$= - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} = -B^{-1}$$





Let m be an element of $F(\alpha,\beta)$

$m = \alpha^{k_1}\cdot\beta^{\ell_1}\cdot\alpha^{k_2}\cdot\beta^{\ell_2}\cdots\alpha^{k_s}\cdot\beta^{\ell_s}$ ← reduced word

$(k_1 \in \mathbb{Z},\ \ell_1, k_2, \ell_2, \ldots, k_s \in \mathbb{Z}\setminus\{0\},\ \ell_s \in \mathbb{Z})$

Claim 2: Set $M := \pi(m)$. Let $z \in \mathcal{F}$.

If $k_1 \neq 0$ then $Mz \in \mathcal{A}$

If $k_1 = 0$ and $\ell_2 \neq 0$ then $Mz \in \mathcal{B}$

We prove this claim by induction on s.

This claim implies the injectivity of π.

Claim 2: Let $M = A^{k_1} B^{\ell_1} A^{k_2} B^{\ell_2} \cdots A^{k_s} B^{\ell_s}$ and $z \in \mathcal{F}$

If $k_1 \neq 0$ then $Mz \in \mathcal{A}$

If $k_1 = 0$ and $\ell_1 \neq 0$ then $Mz \in \mathcal{B}$

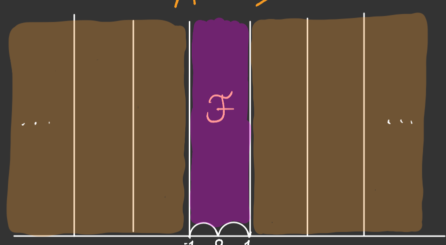
We prove this claim by induction on $\ell(M)$, where

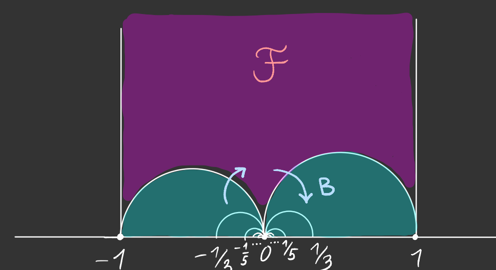
$$\ell(M) := \begin{cases} 2s & \text{if } k_1, \ell_s \neq 0 \\ 2s-1 & \text{if } k_1 = 0 \text{ and } \ell_s \neq 0 \\ 2s-1 & \text{if } k_1 \neq 0 \text{ and } \ell_s = 0 \\ 2s-2 & \text{if } k_1, \ell_s = 0 \end{cases}$$

Base of induction: $\ell(M) = 1$. Then $M = A^{k_1}$ or $M = B^{\ell_1}$

$A \longrightarrow$

$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$





$B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$

$$\frac{1}{2n-1} \xrightarrow{B} \frac{\frac{1}{2n-1}}{2 \cdot \frac{1}{2n-1} + 1} = \frac{1}{2 + 2n-1} = \frac{1}{2n+1}$$

Step of induction: Claim 1

We have proven that the map

$$\pi : F(\alpha, \beta) \to \overline{\Gamma}(2) \quad \text{is injective}$$

Step 2:

What about surjectivity of π?

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$.

We need to show: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm A^{k_1} B^{l_1} \cdots A^{k_s} B^{l_s}$

for some $k_1, l_1, \dots, k_s, l_s \in \mathbb{Z}$.

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \left(\begin{array}{c|c} a+2c & b+2d \\ \hline c & d \end{array}\right)$$

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \left(\begin{array}{c|c} a & b \\ \hline c+2a & d+2b \end{array}\right)$$

Consider the following **algorithm:**

Input: $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$

1. If $|\overset{\text{odd}}{a}| \underset{\neq}{\geq} |\overset{\text{even}}{c}|$ and $c \neq 0$

   There exists an integer k such that

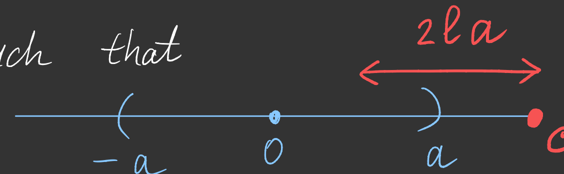
   

   $$|a + 2kc| < |c|$$

   $$M \longrightarrow \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^k M \,;$$

2. If $|a| < |c|$

   There exists an integer ℓ such that

   $$|c + 2a\ell| < |a|$$

   $$M \longrightarrow \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^\ell \cdot M \,;$$

3. If $c = 0$ then $M = \pm \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^k$ for some $k \in \mathbb{Z}$

   $M \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; finish algorithm

Claim: The algorithm terminates for all $M \in \Gamma(2)$ after a finite number of steps.

Indeed, $|a| + |c|$ decreases after each step.

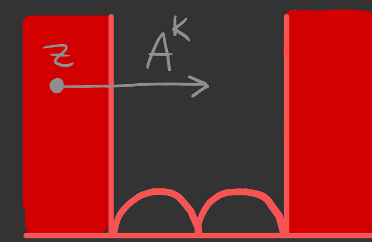
This proves that $\pi : F(\alpha, \beta) \to \overline{\Gamma(2)}$ is surjective
This finishes the proof of part a).

Proof of part b)

Claim 2 implies that for all $z \in \mathfrak{h}$ at most one $\Gamma(2)$-translate of z is contained in $\mathcal{F}$.

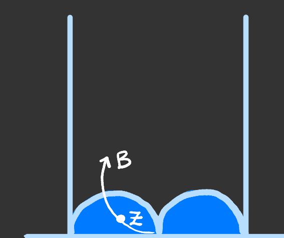
It remains to show that for all $z \in \mathfrak{h}$ there exists $M \in \Gamma(2)$ such that $Mz \in \mathcal{F}$.

Consider the following **algorithm:**



Input $z \in \mathfrak{h}$

1. If $z \in \mathcal{A}$
   then there exists $k \in \mathbb{Z}$ such that $A^k z \in \mathcal{F} \cup \mathcal{B}$
   $z \longrightarrow A^k z$
2. If $z \in \mathcal{B}$
   then there exists $\ell \in \mathbb{Z}$ such that $B^\ell z \in \mathcal{F} \cup \mathcal{A}$
   $z \longrightarrow B^\ell z$



3. If $z \in \mathcal{F}$ return z

Claim: Let $z_0, z_1, \dots, z_n, \dots$ be the sequence of values of variable z in the algorithm above. Then

- $\operatorname{Im}(z_{n+1}) \geq \operatorname{Im}(z_n)$ $\qquad \operatorname{Im}(A^k z) = \operatorname{Im}(z)$
- $\operatorname{Im}\left(-\frac{1}{z_{n+1}}\right) \geq \operatorname{Im}\left(-\frac{1}{z_n}\right)$ $\qquad \operatorname{Im}\left(-\frac{1}{B^k z}\right) = \operatorname{Im}\left(-\frac{1}{z}\right)$

At each step one of this inequalities is strict.

Exercise: Let $z \in \mathfrak{h}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$.

Then $\operatorname{Im}\left(\frac{az+b}{cz+d}\right) = \frac{\operatorname{Im}(z)}{|cz+d|^2}$.

Claim: Algorithm terminates after a finite number of steps.

Suppose that $z_n = \frac{a_n z + b_n}{c_n z + d_n}$.

- $\operatorname{Im}\left(\frac{a_n z + b_n}{c_n z + d_n}\right) \geq \operatorname{Im}(z) \Rightarrow |c_n z + d_n|^2 \leq 1 \Rightarrow$ finite number of (c_n, d_n)
- $\operatorname{Im}\left(\frac{-c_n z - d_n}{a_n z + b_n}\right) \geq \operatorname{Im}(z) \Rightarrow |a_n z + b_n|^2 \leq 1 \Rightarrow$ finite number of (a_n, b_n)

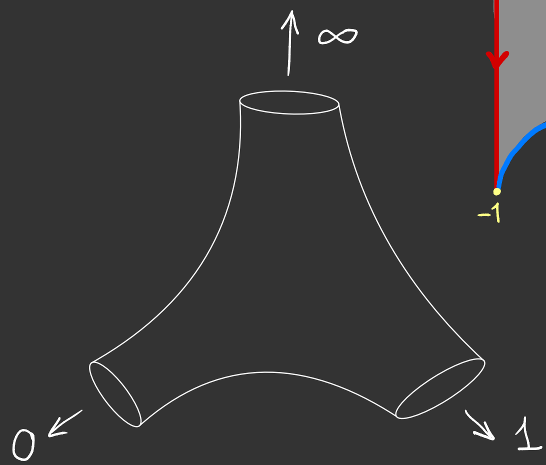
This finishes the proof of the theorem. $\blacksquare$

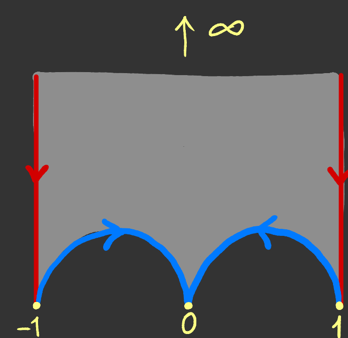
Modular curve $X_{\Gamma(2)}$

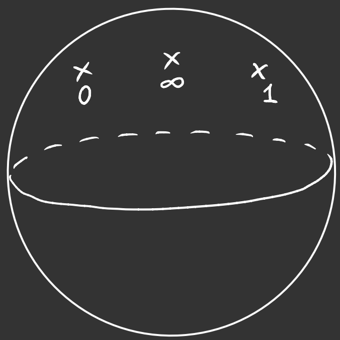
Definition: $Y_{\Gamma(2)} := \overline{\Gamma}(2) \backslash \mathfrak{h}$

topological space
metric space
complex manifold

Riemann surface (complex variety of dimension 1)







Definition: Let $\Gamma \subset PSL_2(\mathbb{Z})$ be a congruence subgroup.
A point $z \in \mathfrak{h}$ is an **elliptic point of Γ** if the stabilizer $\mathrm{Stab}(\Gamma, z) := \{\gamma \in \Gamma \mid \gamma z = z\}$ is non-trivial.

Lemma: $\Gamma(2)$ has no elliptic points.

Proof: Suppose that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$ and $z \in \mathfrak{h}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = z \qquad \neq \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\frac{az+b}{cz+d} = z \qquad cz^2 + (d-a)z - b = 0$$

has complex roots

$$(d-a)^2 - 4bc = a^2 + d^2 - 2ad - 4bc = (a+d)^2 - 4 < 0$$

This condition implies that $|a+d| < 2$

a and d are odd $\Rightarrow$ $a+d$ is even

Therefore $a+d=0$.

Thus $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 2b' \\ 2c' & -a \end{pmatrix}$. for some $c', d' \in \mathbb{Z}$.

Since $ad-bc=1$ we have $-a^2-4b'c'=1$ $(\blacktriangle)$

Since a is odd, then $-a^2 \equiv 1 \bmod 4$

This contradicts $(\blacktriangle)$ and finishes the proof $\blacksquare$

Definition: A **cusp** of a congruence subgroup Γ is a Γ-equivalence class of $\mathbb{Q} \cup \{\infty\}$.

Lemma: $\Gamma(2)$ has 3 cusps: $1, 0, \infty$

some thoughts about the proof:

$$\mathbb{Q} \cup \{\infty\} \simeq \mathbb{P}_1(\mathbb{Q}) = \{[m:n] \mid (m,n) \in \mathbb{Z}^2 \setminus \{0\}\}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} [m:n] = [am+bn : cm+dn]$$

$$\pi: \mathbb{P}_1(\mathbb{Q}) \longrightarrow \mathbb{P}_1(\mathbb{Z}/2\mathbb{Z})$$

$(m,n)=1$,
$[m:n] \to [m \bmod 2, n \bmod 2]$

$\pi(Mv) = \pi(v)$ for all $M \in \Gamma(2)$ and $v \in \mathbb{P}_1(\mathbb{Q})$

$$\mathbb{P}_1(\mathbb{Z}/2\mathbb{Z}) = \{\underset{0}{[0:1]}, \underset{\infty}{[1:0]}, \underset{1}{[1:1]}\}$$

Modular lambda function

$$\theta_{00}(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z}$$

$$\theta_{01}(z) = \sum_{n\in\mathbb{Z}} (-1)^n e^{\pi i n^2 z}$$

$$\theta_{10}(z) = \sum_{n\in\mathbb{Z}} e^{\pi i (n+\frac{1}{2})^2 z}$$

Definition:

The function $\lambda(z) := \dfrac{\theta_{10}^4(z)}{\theta_{00}^4(z)}$

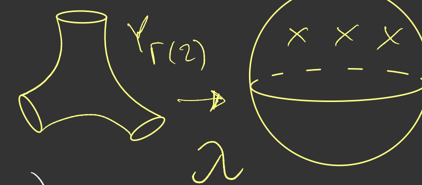
is called **the modular lambda function**

Theorem:

a) For all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$ and $z \in \mathfrak{h}$ we have

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

b) λ is a holomorphic bijection between $\Gamma(2) \setminus \mathfrak{h}$ and $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$.



Proof: By exercise 5

$$\theta_{00}^4\left(\frac{az+b}{cz+d}\right) = (cz+d)^2\, \theta_{00}^4(z)$$

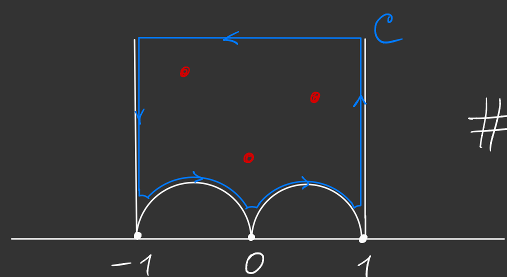
$$\theta_{10}^4\left(\frac{az+b}{cz+d}\right) = (cz+d)^2\, \theta_{10}^4(z)$$

This implies part a).

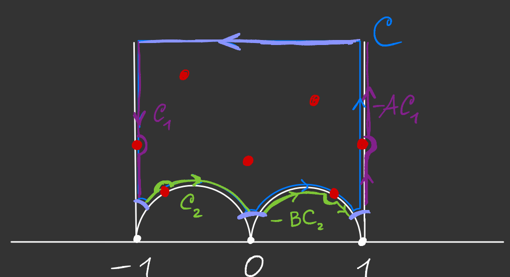
Let $c \in \mathbb{C} \setminus \{0, 1\}$

Set $f(z) := \lambda(z) - c$

We will compute the number of zeroes of f in a fundamental domain of $\Gamma(2) \setminus \mathfrak{h}$.



$$\#\text{ zeroes inside } C = \frac{1}{2\pi i} \int_C \frac{f'(z)}{f(z)} dz$$



$$f(Mz) = f(z) \quad \text{for all } M \in \Gamma(2)$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}) \qquad z = \frac{a\tau + b}{c\tau + d} \Rightarrow dz = (c\tau + d)^{-2} d\tau$$

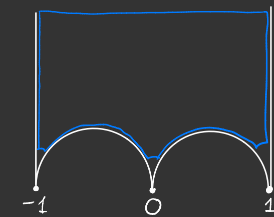
$$f\left(\frac{\tau}{2\tau+1}\right) = f(\tau)$$

$$(2\tau+1)^{-2} f'\left(\frac{\tau}{2\tau+1}\right) = f'(\tau)$$

If f transforms like a modular function then f' transforms like a weight 2 modular form

$$\int_{C_2} \frac{f'(\tau)}{f(\tau)} d\tau - \int_{BC_2} \frac{f'(\tau)}{f(\tau)} d\tau = \underbrace{\int_{C_2} \left(\frac{f'(\tau)}{f(\tau)} d\tau - \frac{f'\left(\frac{\tau}{2\tau+1}\right)}{f\left(\frac{\tau}{2\tau+1}\right)} (2\tau+1)^{-2} d\tau \right)}_{=0}$$

$$f(\tau) = \sum_{n=n_0}^{\infty} c_f(n)\, e^{\pi i n \tau}, \qquad c_f(n_0) \neq 0, \quad n_0 \in \mathbb{Z}$$



$$\int_{-1+iT}^{1+iT} \frac{f'(\tau)}{f(\tau)}\, d\tau \xrightarrow[\text{as } T \to \infty]{=}$$

$$\int_{-1+iT}^{1+iT} \frac{\pi i n_0\, e^{\pi i n_0 \tau}}{e^{\pi i n_0 \tau}}\, d\tau = 2\pi i n_0 = 2\pi i \,\mathrm{ord}_\infty(f)$$

for $c \notin \{0, 1\}$

$$\lim_{z \to \infty} \lambda(z) = 0 \qquad \mathrm{ord}_\infty(\lambda - c) = 0$$

$$\lim_{z \to 0} \lambda(z) = 1 \qquad \mathrm{ord}_0(\lambda - c) = 0$$

$$\lim_{z \to 1} \lambda(z) = \infty \qquad \mathrm{ord}_1(\lambda - c) = -1$$

$\Rightarrow$ $\lambda - c$ has exactly one zero in a fundamental domain.

$\blacksquare$

Definition: λ-function is a <u>Hauptmodul</u> for $\Gamma(2)$

Definition: A congruence subgroup $\Gamma \subset SL_2(\mathbb{Z})$ is a **congruence subgroup of genus 0** if $\Gamma \backslash \mathfrak{H}$ is homeomorphic to $\mathbb{P}^1(\mathbb{C}) \setminus \left\{ \begin{array}{l} \text{finite} \\ \text{number} \\ \text{of points} \end{array} \right\}$

iso as Riemann surfaces

A holomorphic function $f: \Gamma \backslash \mathfrak{H} \to \mathbb{P}^1(\mathbb{C}) \setminus \left\{ \begin{array}{l} \text{finite} \\ \text{number} \\ \text{of points} \end{array} \right\}$

f is $1:1$

then f is a **Hauptmodul for Γ**

Remark: λ-function is a weakly holomorphic modular form of weight 0 for $\Gamma(2)$.

$$\lambda \in M_0^!(\Gamma(2)).$$

$$\dim M_0^!(\Gamma(2)) = \infty.$$