Mysterious factorisations and Knopp's cocycle

Mike Daas

5th of July, 2022

Universiteit Leiden

Setting up

Recall the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\widehat{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$:

$$\text{if} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{then} \quad \gamma \cdot x = \frac{ax+b}{cx+d}.$$

On $\mathbb{R}(z)$ we have the *weight* 2 action:

$$f(z)|_2\gamma = (cz+d)^{-2} f(\gamma \cdot z).$$

Setting up

Recall the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\widehat{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$:

$$\text{if} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{then} \quad \gamma \cdot x = \frac{ax+b}{cx+d}.$$

On $\mathbb{R}(z)$ we have the *weight* 2 action:

$$f(z)|_2\gamma = (cz+d)^{-2} f(\gamma \cdot z).$$

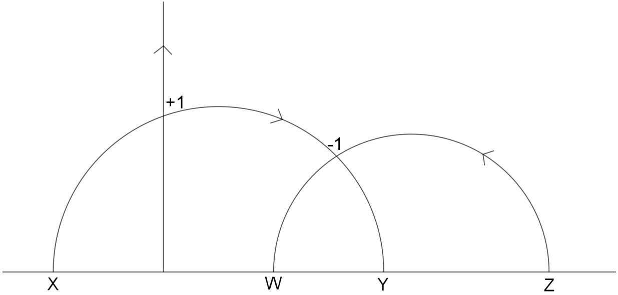
Let $\tau \in \mathbb{R}$ be of degree 2 over $\mathbb{Q}$. Its Galois conjugate is denoted τ'.

Lemma

The stabiliser of $\tau \in \mathbb{R}$ is infinite cyclic: $\Gamma_\tau = \langle \gamma_\tau \rangle \subset \mathrm{PSL}_2(\mathbb{Z})$.

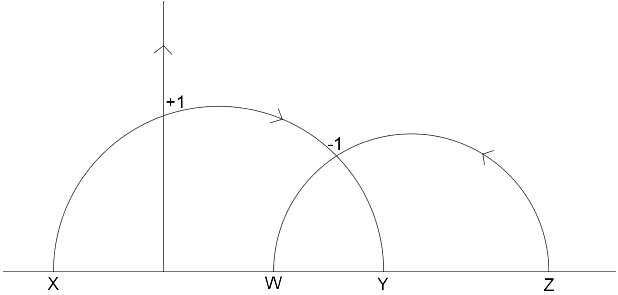
Intersecting geodesics

Any pair $(x, y) \subset \widehat{\mathbb{R}}^2$ defines a unique geodesic in $\mathcal{H}$ by drawing a half circle:



Intersecting geodesics

Any pair $(x, y) \subset \widehat{\mathbb{R}}^2$ defines a unique geodesic in $\mathcal{H}$ by drawing a half circle:



Two geodesics can intersect either positively or negatively, depending on their orientations. We denote this intersection by

$$(x \to y) \cap (z \to w) \in \{-1, 0, 1\}.$$

Knopp's cocycle

Definition

The *Knopp cocycle* f_τ associated to τ is defined by

$$f_\tau(\gamma) = \sum_{\delta \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_\tau} \frac{(\delta\tau' \to \delta\tau) \cap (\gamma\infty \to \infty)}{z - \delta\tau}.$$

Knopp's cocycle

Definition

The *Knopp cocycle* f_τ associated to τ is defined by

$$f_\tau(\gamma) = \sum_{\delta \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_\tau} \frac{(\delta\tau' \to \delta\tau) \cap (\gamma\infty \to \infty)}{z - \delta\tau}.$$

- So $\delta\tau' \to \delta\tau$ contributes to the sum if and only if $\gamma\infty \in \mathbb{Q}$ is in between $\delta\tau$ and $\delta\tau'$. If $\delta\tau > \gamma\infty$ it contributes 1, otherwise -1.

Knopp's cocycle

Definition

The *Knopp cocycle* f_τ associated to τ is defined by

$$f_\tau(\gamma) = \sum_{\delta \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_\tau} \frac{(\delta\tau' \to \delta\tau) \cap (\gamma\infty \to \infty)}{z - \delta\tau}.$$

- So $\delta\tau' \to \delta\tau$ contributes to the sum if and only if $\gamma\infty \in \mathbb{Q}$ is in between $\delta\tau$ and $\delta\tau'$. If $\delta\tau > \gamma\infty$ it contributes 1, otherwise -1.
- Every element in $\mathrm{SL}_2(\mathbb{Z}) \cdot \tau$ has the same discriminant as τ. So, the set $\mathrm{SL}_2(\mathbb{Z})/\Gamma_\tau$ bijects with the set of real quadratic irrationalities σ satisfying $\mathrm{disc}(\sigma) = \mathrm{disc}(\tau) = D$.

Knopp's cycle

Definition

The *Knopp cocycle* f_τ associated to τ is defined by

$$f_\tau(\gamma) = \sum_{\delta \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_\tau} \frac{(\delta\tau' \to \delta\tau) \cap (\gamma\infty \to \infty)}{z - \delta\tau}.$$

- So $\delta\tau' \to \delta\tau$ contributes to the sum if and only if $\gamma\infty \in \mathbb{Q}$ is in between $\delta\tau$ and $\delta\tau'$. If $\delta\tau > \gamma\infty$ it contributes 1, otherwise -1.
- Every element in $\mathrm{SL}_2(\mathbb{Z}) \cdot \tau$ has the same discriminant as τ. So, the set $\mathrm{SL}_2(\mathbb{Z})/\Gamma_\tau$ bijects with the set of real quadratic irrationalities σ satisfying $\mathrm{disc}(\sigma) = \mathrm{disc}(\tau) = D$.
- This actually is a cocycle:

$$f_\tau(\gamma_1\gamma_2) = f_\tau(\gamma_1) + f_\tau(\gamma_2)|_2\gamma_1^{-1}.$$

Knopp's cocycle

Definition

The *Knopp cocycle* f_τ associated to τ is defined by

$$f_\tau(\gamma) = \sum_{\delta \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_\tau} \frac{(\delta\tau' \to \delta\tau) \cap (\gamma\infty \to \infty)}{z - \delta\tau}.$$

- So $\delta\tau' \to \delta\tau$ contributes to the sum if and only if $\gamma\infty \in \mathbb{Q}$ is in between $\delta\tau$ and $\delta\tau'$. If $\delta\tau > \gamma\infty$ it contributes 1, otherwise -1.
- Every element in $\mathrm{SL}_2(\mathbb{Z}) \cdot \tau$ has the same discriminant as τ. So, the set $\mathrm{SL}_2(\mathbb{Z})/\Gamma_\tau$ bijects with the set of real quadratic irrationalities σ satisfying $\mathrm{disc}(\sigma) = \mathrm{disc}(\tau) = D$.
- This actually is a cocycle:

$$f_\tau(\gamma_1\gamma_2) = f_\tau(\gamma_1) + f_\tau(\gamma_2)|_2\gamma_1^{-1}.$$

Remark

This sum is finite. Consider e.g. $\gamma\infty = 0$. We look for zeroes of $px^2 + qx + r = 0$ with $q^2 - 4pr = D$ and $\sigma' < 0 < \sigma$. The latter means that $pr < 0$. However, this bounds $q^2 = D + 4pr < D$, yielding only finitely many possibilities.

The multiplicative Knopp cocycle

Recall the dlog map on polynomials: if $P(z) = \prod (z - \alpha_i)^{n_i}$, then

$$\operatorname{dlog}(P)(z) = \frac{P'(z)}{P(z)} = \sum \frac{n_i}{z - \alpha_i}.$$

We want to lift our cocycle along dlog.

The multiplicative Knopp cocycle

Recall the dlog map on polynomials: if $P(z) = \prod (z - \alpha_i)^{n_i}$, then

$$\mathrm{dlog}(P)(z) = \frac{P'(z)}{P(z)} = \sum \frac{n_i}{z - \alpha_i}.$$

We want to lift our cocycle along dlog.

Proposition

For some appropriate choices of $x_\gamma \in \mathbb{Q}(\tau)$, we have a cocycle defined by

$$F_\tau(\gamma) = x_\gamma \prod_{\delta \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_\tau} (z - \delta\tau)^{(\delta\tau \cap \delta\tau') \cap (\gamma\infty \to \infty)}.$$

The multiplicative Knopp cocycle

Recall the dlog map on polynomials: if $P(z) = \prod (z - \alpha_i)^{n_i}$, then

$$\operatorname{dlog}(P)(z) = \frac{P'(z)}{P(z)} = \sum \frac{n_i}{z - \alpha_i}.$$

We want to lift our cocycle along dlog.

Proposition

For some appropriate choices of $x_\gamma \in \mathbb{Q}(\tau)$, we have a cocycle defined by

$$F_\tau(\gamma) = x_\gamma \prod_{\delta \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_\tau} (z - \delta\tau)^{(\delta\tau \cap \delta\tau') \cap (\gamma\infty \to \infty)}.$$

Definition

For τ_1, τ_2 both real quadratic irrationalities, we define

$$F_{\tau_1}[\tau_2] := F_{\tau_1}(\gamma_{\tau_2})(\tau_2).$$

This is independent on the choice of τ_2 in its $\mathrm{SL}_2(\mathbb{Z})$-orbit. However, choosing $\gamma_{\tau_2}^{-1}$ instead will invert the outcome.

Context

Why is this cocycle interesting?
Recent work by H. Darmon and J. Vonk uses a similar construction but then for the group $\mathrm{SL}_2(\mathbb{Z}[1/p])$ on the p-adic upper half plane.

Context

Why is this cocycle interesting?
Recent work by H. Darmon and J. Vonk uses a similar construction but then for the group $\mathrm{SL}_2(\mathbb{Z}[1/p])$ on the p-adic upper half plane.
Their goal is to do explicit class field theory for real quadratic fields (RM theory) just like classical CM theory:

$$H_K = K(j(\tau)) \quad \text{where} \quad \tau \in \mathcal{O}_K.$$

Context

Why is this cocycle interesting?
Recent work by H. Darmon and J. Vonk uses a similar construction but then for the group $\mathrm{SL}_2(\mathbb{Z}[1/p])$ on the p-adic upper half plane.
Their goal is to do explicit class field theory for real quadratic fields (RM theory) just like classical CM theory:

$$H_K = K(j(\tau)) \quad \text{where} \quad \tau \in \mathcal{O}_K.$$

Better yet, produce formulas (à la Gross-Zagier) for the differences

$$j(\tau_1) - j(\tau_2).$$

Context

Why is this cocycle interesting?
Recent work by H. Darmon and J. Vonk uses a similar construction but then for the group $\mathrm{SL}_2(\mathbb{Z}[1/p])$ on the p-adic upper half plane.
Their goal is to do explicit class field theory for real quadratic fields (RM theory) just like classical CM theory:

$$H_K = K(j(\tau)) \quad \text{where} \quad \tau \in \mathcal{O}_K.$$

Better yet, produce formulas (à la Gross-Zagier) for the differences

$$j(\tau_1) - j(\tau_2).$$

This Knopp cocycle is the $\mathbb{R}$-baby case. Still interesting to study!

Example

Set $\tau_1 = \frac{1+\sqrt{5}}{2}$ and $\tau_2 = \sqrt{3}$. Then

$$\gamma_{\tau_2} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \quad \text{so} \quad \gamma_{\tau_2}\infty = 2.$$

Example

Set $\tau_1 = \frac{1+\sqrt{5}}{2}$ and $\tau_2 = \sqrt{3}$. Then

$$\gamma_{\tau_2} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \quad \text{so} \quad \gamma_{\tau_2}\infty = 2.$$

In the $\mathrm{SL}_2(\mathbb{Z})$-orbit of τ_1 we have only

$$\frac{3-\sqrt{5}}{2} < 2 < \frac{3+\sqrt{5}}{2} \quad \text{and} \quad \frac{5-\sqrt{5}}{2} < 2 < \frac{5+\sqrt{5}}{2}.$$

Example

Set $\tau_1 = \frac{1+\sqrt{5}}{2}$ and $\tau_2 = \sqrt{3}$. Then

$$\gamma_{\tau_2} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \quad \text{so} \quad \gamma_{\tau_2}\infty = 2.$$

In the $\mathrm{SL}_2(\mathbb{Z})$-orbit of τ_1 we have only

$$\frac{3-\sqrt{5}}{2} < 2 < \frac{3+\sqrt{5}}{2} \quad \text{and} \quad \frac{5-\sqrt{5}}{2} < 2 < \frac{5+\sqrt{5}}{2}.$$

As a result,

$$F_{\tau_1}(\gamma_{\tau_2}) = \frac{\left(z - \frac{3+\sqrt{5}}{2}\right)\left(z - \frac{5+\sqrt{5}}{2}\right)}{\left(z - \frac{3-\sqrt{5}}{2}\right)\left(z - \frac{5-\sqrt{5}}{2}\right)}.$$

Example

Set $\tau_1 = \frac{1+\sqrt{5}}{2}$ and $\tau_2 = \sqrt{3}$. Then

$$\gamma_{\tau_2} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \quad \text{so} \quad \gamma_{\tau_2}\infty = 2.$$

In the $\mathrm{SL}_2(\mathbb{Z})$-orbit of τ_1 we have only

$$\frac{3-\sqrt{5}}{2} < 2 < \frac{3+\sqrt{5}}{2} \quad \text{and} \quad \frac{5-\sqrt{5}}{2} < 2 < \frac{5+\sqrt{5}}{2}.$$

As a result,

$$F_{\tau_1}(\gamma_{\tau_2}) = \frac{\left(z - \frac{3+\sqrt{5}}{2}\right)\left(z - \frac{5+\sqrt{5}}{2}\right)}{\left(z - \frac{3-\sqrt{5}}{2}\right)\left(z - \frac{5-\sqrt{5}}{2}\right)}.$$

Hence

$$F_{\tau_1}[\tau_2] = \frac{\left(-5 + 2\sqrt{3} - \sqrt{5}\right)\left(-3 + 2\sqrt{3} - \sqrt{5}\right)}{\left(-5 + 2\sqrt{3} + \sqrt{5}\right)\left(-3 + 2\sqrt{3} + \sqrt{5}\right)}$$

Example

Set $\tau_1 = \frac{1+\sqrt{5}}{2}$ and $\tau_2 = \sqrt{3}$. Then

$$\gamma_{\tau_2} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \quad \text{so} \quad \gamma_{\tau_2}\infty = 2.$$

In the $\mathrm{SL}_2(\mathbb{Z})$-orbit of τ_1 we have only

$$\frac{3-\sqrt{5}}{2} < 2 < \frac{3+\sqrt{5}}{2} \quad \text{and} \quad \frac{5-\sqrt{5}}{2} < 2 < \frac{5+\sqrt{5}}{2}.$$

As a result,

$$F_{\tau_1}(\gamma_{\tau_2}) = \frac{\left(z - \frac{3+\sqrt{5}}{2}\right)\left(z - \frac{5+\sqrt{5}}{2}\right)}{\left(z - \frac{3-\sqrt{5}}{2}\right)\left(z - \frac{5-\sqrt{5}}{2}\right)}.$$

Hence

$$F_{\tau_1}[\tau_2] = \frac{\left(-5+2\sqrt{3}-\sqrt{5}\right)\left(-3+2\sqrt{3}-\sqrt{5}\right)}{\left(-5+2\sqrt{3}+\sqrt{5}\right)\left(-3+2\sqrt{3}+\sqrt{5}\right)} = \frac{21-8\sqrt{5}}{11}.$$

Mysterious factorisations I

$$F_{\tau_1}[\tau_2] = \frac{\left(-5+2\sqrt{3}-\sqrt{5}\right)\left(-3+2\sqrt{3}-\sqrt{5}\right)}{\left(-5+2\sqrt{3}+\sqrt{5}\right)\left(-3+2\sqrt{3}+\sqrt{5}\right)} = \frac{21-8\sqrt{5}}{11}.$$

There is no obvious reason for the $\sqrt{3}$ to disappear.

Mysterious factorisations I

$$F_{\tau_1}[\tau_2] = \frac{\left(-5+2\sqrt{3}-\sqrt{5}\right)\left(-3+2\sqrt{3}-\sqrt{5}\right)}{\left(-5+2\sqrt{3}+\sqrt{5}\right)\left(-3+2\sqrt{3}+\sqrt{5}\right)} = \frac{21-8\sqrt{5}}{11}.$$

There is no obvious reason for the $\sqrt{3}$ to disappear. In this case:

$$\left(-5+2\sqrt{3}-\sqrt{5}\right)\left(-3+2\sqrt{3}-\sqrt{5}\right) = -4(\sqrt{3}-2)(\sqrt{5}+4)$$
$$\left(-5+2\sqrt{3}+\sqrt{5}\right)\left(-3+2\sqrt{3}+\sqrt{5}\right) = 4(\sqrt{3}-2)(\sqrt{5}-4).$$

Mysterious factorisations I

$$F_{\tau_1}[\tau_2] = \frac{\left(-5+2\sqrt{3}-\sqrt{5}\right)\left(-3+2\sqrt{3}-\sqrt{5}\right)}{\left(-5+2\sqrt{3}+\sqrt{5}\right)\left(-3+2\sqrt{3}+\sqrt{5}\right)} = \frac{21-8\sqrt{5}}{11}.$$

There is no obvious reason for the $\sqrt{3}$ to disappear. In this case:

$$\begin{aligned}\left(-5+2\sqrt{3}-\sqrt{5}\right)\left(-3+2\sqrt{3}-\sqrt{5}\right) &= -4(\sqrt{3}-2)(\sqrt{5}+4)\\ \left(-5+2\sqrt{3}+\sqrt{5}\right)\left(-3+2\sqrt{3}+\sqrt{5}\right) &= \;\;4(\sqrt{3}-2)(\sqrt{5}-4).\end{aligned}$$

Coincidence? Let's try $\tau_1 = \sqrt{2}$ and $\tau_2 = \sqrt{3}$. Then $F_{\tau_1}[\tau_2]$ equals

$$\frac{\left(4+\sqrt{2}-2\sqrt{3}\right)\left(1+\sqrt{2}-\sqrt{3}\right)\left(2+\sqrt{2}-\sqrt{3}\right)\left(3+\sqrt{2}-\sqrt{3}\right)}{\left(-3+\sqrt{2}+\sqrt{3}\right)\left(-2+\sqrt{2}+\sqrt{3}\right)\left(-1+\sqrt{2}+\sqrt{3}\right)\left(-4+\sqrt{2}+2\sqrt{3}\right)}.$$

Mysterious factorisations II

So $F_{\tau_1}[\tau_2]$ equals

$$\frac{\left(4+\sqrt{2}-2\sqrt{3}\right)\left(1+\sqrt{2}-\sqrt{3}\right)\left(2+\sqrt{2}-\sqrt{3}\right)\left(3+\sqrt{2}-\sqrt{3}\right)}{\left(-3+\sqrt{2}+\sqrt{3}\right)\left(-2+\sqrt{2}+\sqrt{3}\right)\left(-1+\sqrt{2}+\sqrt{3}\right)\left(-4+\sqrt{2}+2\sqrt{3}\right)}.$$

This equals

$$\frac{219+53\sqrt{2}}{23}.$$

Mysterious factorisations II

So $F_{\tau_1}[\tau_2]$ equals

$$\frac{(4+\sqrt{2}-2\sqrt{3})\,(1+\sqrt{2}-\sqrt{3})\,(2+\sqrt{2}-\sqrt{3})\,(3+\sqrt{2}-\sqrt{3})}{(-3+\sqrt{2}+\sqrt{3})\,(-2+\sqrt{2}+\sqrt{3})\,(-1+\sqrt{2}+\sqrt{3})\,(-4+\sqrt{2}+2\sqrt{3})}.$$

This equals

$$\frac{219+53\sqrt{2}}{23}.$$

Again, we have factorisations

$$\begin{aligned}
\left(4+\sqrt{2}-2\sqrt{3}\right)\left(2+\sqrt{2}-\sqrt{3}\right) &= -(\sqrt{3}-2)(8+3\sqrt{2})\\
\left(1+\sqrt{2}-\sqrt{3}\right)\left(3+\sqrt{2}-\sqrt{3}\right) &= -(\sqrt{3}-2)(4+2\sqrt{2})\\
\left(-1+\sqrt{2}+\sqrt{3}\right)\left(-3+\sqrt{2}+\sqrt{3}\right) &= -(\sqrt{3}-2)(4-2\sqrt{2})\\
\left(-2+\sqrt{2}+\sqrt{3}\right)\left(-4+\sqrt{2}+2\sqrt{3}\right) &= -(\sqrt{3}-2)(8-3\sqrt{2}).
\end{aligned}$$

What's going on here?

Key Lemma

Lemma

Let $M \in \mathrm{GL}_2(\mathbb{Q})$ interchange τ and τ'. Then M^2 acts trivially.

Proof: We claim that $\mathrm{tr}(M) = 0$, so that $M^2 = -\det(M)$ acts trivially.

Key Lemma

Lemma

Let $M \in \mathrm{GL}_2(\mathbb{Q})$ interchange τ and τ'. Then M^2 acts trivially.

Proof: We claim that $\mathrm{tr}(M) = 0$, so that $M^2 = -\det(M)$ acts trivially. Indeed, we have $M\tau = \tau'$ precisely when

$$a\tau + b = c\tau\tau' + d\tau' \iff (a+d)\tau = c\tau\tau' - b + d(\tau + \tau') \in \mathbb{Q}.$$

Since $\tau \notin \mathbb{Q}$, we must have $a + d = 0$. □

Key Lemma

Lemma

Let $M \in \mathrm{GL}_2(\mathbb{Q})$ interchange τ and τ'. Then M^2 acts trivially.

Proof: We claim that $\mathrm{tr}(M) = 0$, so that $M^2 = -\det(M)$ acts trivially. Indeed, we have $M\tau = \tau'$ precisely when

$$a\tau + b = c\tau\tau' + d\tau' \iff (a+d)\tau = c\tau\tau' - b + d(\tau + \tau') \in \mathbb{Q}.$$

Since $\tau \notin \mathbb{Q}$, we must have $a + d = 0$. □

Key Lemma

If $p\tau^2 + q\tau + r = 0$ and $M \in \mathrm{GL}_2(\mathbb{Q})$ interchanges τ and τ', then

$$p(x - \tau)(Mx - \tau) = \frac{a - c\tau}{cx - a}(px^2 + qx + r).$$

Key Lemma

Lemma

Let $M \in \mathrm{GL}_2(\mathbb{Q})$ interchange τ and τ'. Then M^2 acts trivially.

Proof: We claim that $\mathrm{tr}(M) = 0$, so that $M^2 = -\det(M)$ acts trivially. Indeed, we have $M\tau = \tau'$ precisely when

$$a\tau + b = c\tau\tau' + d\tau' \iff (a+d)\tau = c\tau\tau' - b + d(\tau + \tau') \in \mathbb{Q}.$$

Since $\tau \notin \mathbb{Q}$, we must have $a + d = 0$. □

Key Lemma

If $p\tau^2 + q\tau + r = 0$ and $M \in \mathrm{GL}_2(\mathbb{Q})$ interchanges τ and τ', then

$$p(x-\tau)(Mx-\tau) = \frac{a - c\tau}{cx - a}(px^2 + qx + r).$$

Proof: Just write everything out. The equation will be true when

$$pb = qa + rc.$$

Rewrite this as

$$b = -a(\tau + \tau') + c\tau\tau' \iff M\tau = \tau'$$

by the previous proof. □

Idea of the proof

Set $x = \tau_1$ and $\tau = \tau_2$. Then the lemma reads:

Key Lemma

If $p\tau_2^2 + q\tau_2 + r = 0$ and $M \in \mathrm{GL}_2(\mathbb{Q})$ interchanges τ_2 and τ_2', then

$$p(\tau_1 - \tau_2)(M\tau_1 - \tau_2) = \frac{a - c\tau_2}{c\tau_1 - a}(p\tau_1^2 + q\tau_1 + r).$$

Idea of the proof

Set $x = \tau_1$ and $\tau = \tau_2$. Then the lemma reads:

Key Lemma

If $p\tau_2^2 + q\tau_2 + r = 0$ and $M \in \mathrm{GL}_2(\mathbb{Q})$ interchanges τ_2 and τ_2', then

$$p(\tau_1 - \tau_2)(M\tau_1 - \tau_2) = \frac{a - c\tau_2}{c\tau_1 - a}(p\tau_1^2 + q\tau_1 + r).$$

We make pairs $\tau_1, M\tau_1$ in the numerator. This gives us $(a - c\tau_2) \cdot \ldots$

Idea of the proof

Set $x = \tau_1$ and $\tau = \tau_2$. Then the lemma reads:

Key Lemma

If $p\tau_2^2 + q\tau_2 + r = 0$ and $M \in \mathrm{GL}_2(\mathbb{Q})$ interchanges τ_2 and τ_2', then

$$p(\tau_1 - \tau_2)(M\tau_1 - \tau_2) = \frac{a - c\tau_2}{c\tau_1 - a}(p\tau_1^2 + q\tau_1 + r).$$

We make pairs $\tau_1, M\tau_1$ in the numerator. This gives us $(a - c\tau_2) \cdot \ldots$ **If we assume that** $\tau_1' \in \mathrm{SL}_2(\mathbb{Z})\tau_1$, then in the denominator we will have the pairs $\tau_1', M\tau_1'$ which also give $(a - c\tau_2) \cdot \ldots$ These cancel, hence the result is in $\mathbb{Q}(\tau_1)$. This assumption is generally necessary.

Idea of the proof

Set $x = \tau_1$ and $\tau = \tau_2$. Then the lemma reads:

Key Lemma

If $p\tau_2^2 + q\tau_2 + r = 0$ and $M \in \mathrm{GL}_2(\mathbb{Q})$ interchanges τ_2 and τ_2', then

$$p(\tau_1 - \tau_2)(M\tau_1 - \tau_2) = \frac{a - c\tau_2}{c\tau_1 - a}(p\tau_1^2 + q\tau_1 + r).$$

We make pairs $\tau_1, M\tau_1$ in the numerator. This gives us $(a - c\tau_2) \cdot \ldots$
If we assume that $\tau_1' \in \mathrm{SL}_2(\mathbb{Z})\tau_1$, then in the denominator we will have the pairs $\tau_1', M\tau_1'$ which also give $(a - c\tau_2) \cdot \ldots$ These cancel, hence the result is in $\mathbb{Q}(\tau_1)$. This assumption is generally necessary.
Concern: How do we choose M**?**

Idea of the proof

Set $x = \tau_1$ and $\tau = \tau_2$. Then the lemma reads:

Key Lemma

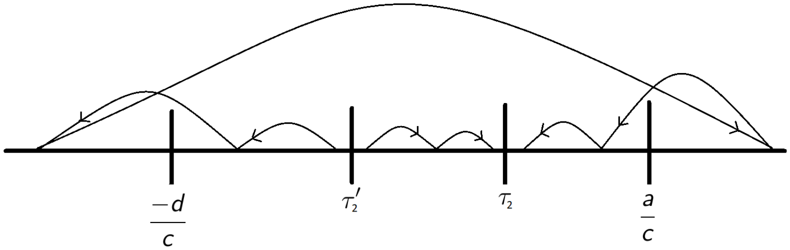
If $p\tau_2^2 + q\tau_2 + r = 0$ and $M \in \mathrm{GL}_2(\mathbb{Q})$ interchanges τ_2 and τ_2', then

$$p(\tau_1 - \tau_2)(M\tau_1 - \tau_2) = \frac{a - c\tau_2}{c\tau_1 - a}(p\tau_1^2 + q\tau_1 + r).$$

We make pairs $\tau_1, M\tau_1$ in the numerator. This gives us $(a - c\tau_2) \cdot \ldots$
If we assume that $\tau_1' \in \mathrm{SL}_2(\mathbb{Z})\tau_1$, then in the denominator we will have the pairs $\tau_1', M\tau_1'$ which also give $(a - c\tau_2) \cdot \ldots$ These cancel, hence the result is in $\mathbb{Q}(\tau_1)$. This assumption is generally necessary.
Concern: How do we choose M?
If M interchanges τ_2 and τ_2', then so does $\gamma_{\tau_2}^k M$ for any k.
We need that M preserves being $> \gamma_{\tau_2}\infty$ and $< \gamma_{\tau_2}\infty$.

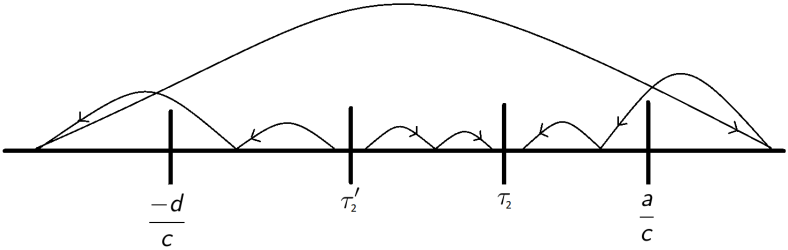
Choosing the right involution

Note that γ_{τ_2} acts on the number line as follows:



Choosing the right involution

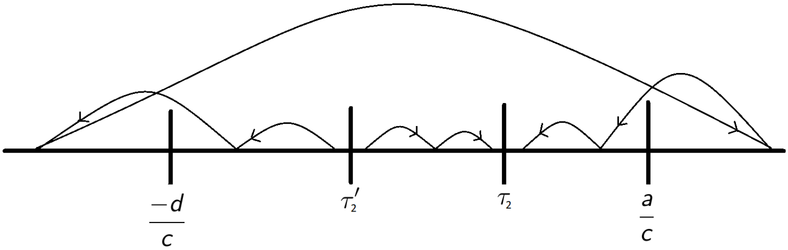
Note that γ_{τ_2} acts on the number line as follows:



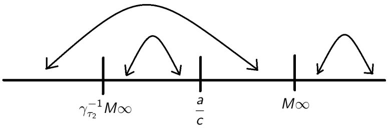
We see: let M interchange τ_2 and τ_2' and suppose that $\det(M) = -1$.
Then there is a unique $k \in \mathbb{Z}$ such that $\gamma_{\tau_2}^k M\infty > \gamma_{\tau_2}\infty = a/c$.

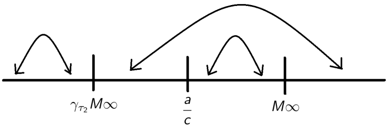
Choosing the right involution

Note that γ_{τ_2} acts on the number line as follows:

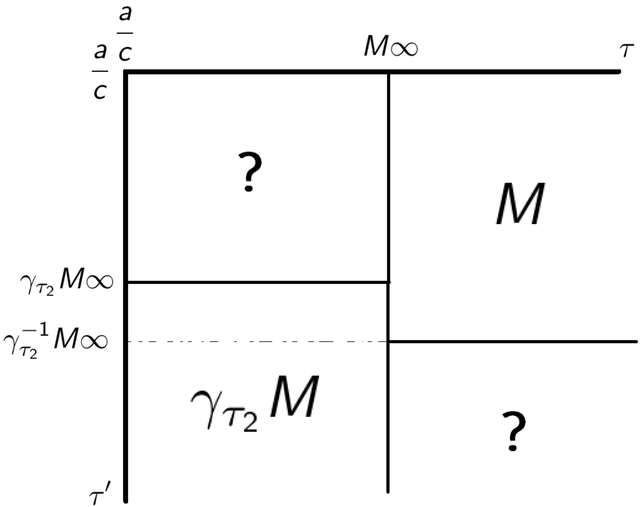


We see: let M interchange τ_2 and τ_2' and suppose that $\det(M) = -1$. Then there is a unique $k \in \mathbb{Z}$ such that $\gamma_{\tau_2}^k M\infty > \gamma_{\tau_2}\infty = a/c$. Choose this involution to be M. Then M and γM act like:





More MS Paint pictures



The final steps

What about the questionmarks? We use the associations

$$\tau \mapsto \gamma_{\tau_2}\tau' \quad \text{and} \quad \tau \mapsto \gamma_{\tau_2}^{-1}\tau'.$$

One can check these interchange the regions appropriately. Why do they induce factorisations?

The final steps

What about the questionmarks? We use the associations

$$\tau \mapsto \gamma_{\tau_2}\tau' \quad \text{and} \quad \tau \mapsto \gamma_{\tau_2}^{-1}\tau'.$$

One can check these interchange the regions appropriately. Why do they induce factorisations?

Lemma

There exists a unique involution N in $\mathrm{GL}_2(\mathbb{Q})/\mathbb{Q}$ interchanging both τ_1, τ_1' and τ_2, τ_2'.

Proof: We saw before that interchanging is equivalent to $\mathrm{tr}(N) = 0$ and

$$p_1 b = q_1 a + r_1 c \quad \text{and} \quad p_2 b = q_2 a + r_2 c.$$

These equations are independent over $\mathbb{Q}$ so give a unique solution up to scalars. □

The final steps

What about the questionmarks? We use the associations

$$\tau \mapsto \gamma_{\tau_2}\tau' \quad \text{and} \quad \tau \mapsto \gamma_{\tau_2}^{-1}\tau'.$$

One can check these interchange the regions appropriately. Why do they induce factorisations?

Lemma

There exists a unique involution N in $\mathrm{GL}_2(\mathbb{Q})/\mathbb{Q}$ interchanging both τ_1, τ_1' and τ_2, τ_2'.

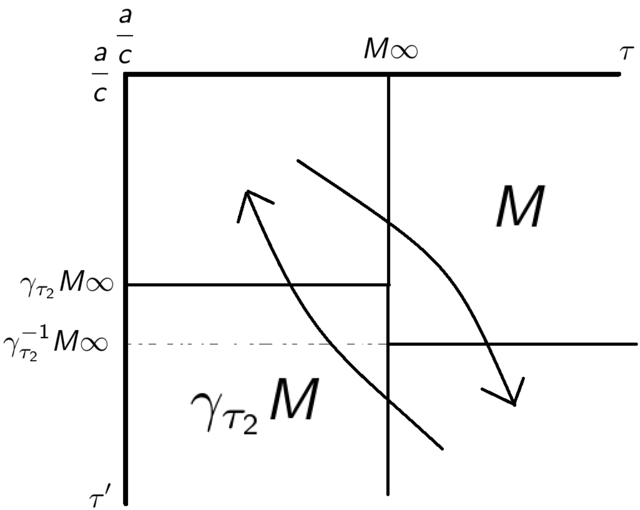
Proof: We saw before that interchanging is equivalent to $\mathrm{tr}(N) = 0$ and

$$p_1 b = q_1 a + r_1 c \quad \text{and} \quad p_2 b = q_2 a + r_2 c.$$

These equations are independent over $\mathbb{Q}$ so give a unique solution up to scalars. □

Consider $\gamma_{\tau_2} N$. It still interchanges τ_2, τ_2', but now maps τ_1 to $\gamma_{\tau_2}\tau_1'$. So our associations above are secretly acting by involutions and thus give factorisations.

Fin



$\frac{a}{c}$
$\frac{a}{c}$
$M\infty$
τ
M
$\gamma_{\tau_2} M\infty$
$\gamma_{\tau_2}^{-1} M\infty$
$\gamma_{\tau_2} M$
τ'