§1 The complex half-plane

<u>Seen</u>: Any $EC/\mathbb{C}$ of form $\mathbb{C}/\Lambda$

+ Λ unique up to $\Lambda \mapsto a\Lambda$, $a \in \mathbb{C}^\times$

<u>Aim</u> Understand $\{ECs/\mathbb{C}\}/\cong \xleftarrow{\sim} \{\Lambda \subseteq \mathbb{C}\}/\mathbb{C}^\times$

May overparametrize further and consider

$$\underbrace{\left\{ (\Lambda, \lambda, \mu) \;\middle|\; \begin{array}{l} \Lambda \subset \mathbb{C} \\ \lambda, \mu \in \Lambda \\ \mathbb{Z}\text{-basis} \end{array} \right\}}_{=: X} \Big/ GL_2(\mathbb{Z}) \times \mathbb{C}^\times \xrightarrow{\sim} \{ECs/\mathbb{C}\}/\cong$$

Then $X/\mathbb{C}^\times \xrightarrow{\sim} \mathcal{H}^\pm := \mathbb{C} \setminus \mathbb{R}$

$$(\Lambda, \lambda, \mu) \sim (\mu^{-1}\Lambda, \mu^{-1}\lambda, 1) \longmapsto \tau := \mu^{-1}\lambda$$

$$(\mathbb{Z} + \mathbb{Z}\tau, \tau, 1) \longleftarrow\!\shortmid \tau$$

$GL_2(\mathbb{Z})$-action descends: $\quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$g(\mathbb{Z}+\mathbb{Z}\tau, \tau, 1) = (\mathbb{Z} + \mathbb{Z}\tau, a\tau + b, c\tau + d)$$

$$\underset{\mathbb{C}^\times}{\sim} (\mathbb{Z} + \mathbb{Z}g\tau, g\tau, 1)$$

<u>Def</u>: $GL_2(\mathbb{Z}) \circlearrowright \mathcal{H}^\pm$ as $\quad g\tau := \dfrac{a\tau+b}{c\tau+d}$

Immediate properties (See yourself)

- Have $\mathrm{Im}(g\tau) = \det(g) \dfrac{\mathrm{Im}\,\tau}{|c\tau+d|^2}$,

  so $SL_2(\mathbb{Z})$ preserves $\mathcal{H} := \{\mathrm{Im}\,\tau > 0\} \subseteq \mathcal{H}^{\pm}$ upper half plane.

  & $GL_2(\mathbb{Z}) \backslash \mathcal{H}^{\pm} \xleftarrow{\sim} SL_2(\mathbb{Z}) \backslash \mathcal{H}$

- $\begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$ acts trivially

Recall Had functions g_2, g_3, Δ, j of Λ. Can now be viewed on $\mathcal{H}^{\pm}$:

$$G_k(\tau) := \sum_{(m,n)\neq(0,0)} (m\tau+n)^{-k} \qquad k \geq 3$$

$$\left.\begin{aligned} g_2(\tau) &= 60\, G_4(\tau) \\ g_3(\tau) &= 140\, G_6(\tau) \\ \Delta(\tau) &= g_2^3 - 27 g_3^2 \\ j(\tau) &= g_2^3 / \Delta \end{aligned}\right\} \begin{aligned} &\text{holom fcts on } \mathcal{H}^{\pm} \\ &\Delta(\tau) \neq 0 \ \forall \tau \end{aligned}$$

What is relation w/ $GL_2(\mathbb{Z})$-action?

$$G_k\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k \cdot G_k(\tau) \quad \text{from definition!}$$

Def 1) $g \in GL_2(\mathbb{Z})$, $\tau \in \mathcal{H}^{\pm}$

$$j(g,\tau) := (c\tau + d)$$

2) Holom fct $f : \mathcal{H}^{\pm} \to \mathbb{C}$ modular of weight k

if $$f(g\tau) = j(g,\tau)^k \cdot f(\tau).$$

Prop (already seen)

	g_2	g_3	Δ	j
modular of weights	4	6	12	0

§2 The quotient $SL_2(\mathbb{Z}) \backslash \mathcal{H}$

<u>Lem</u> $SL_2(\mathbb{Z})$ is generated by

$$S := \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \qquad T := \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}.$$

Prf

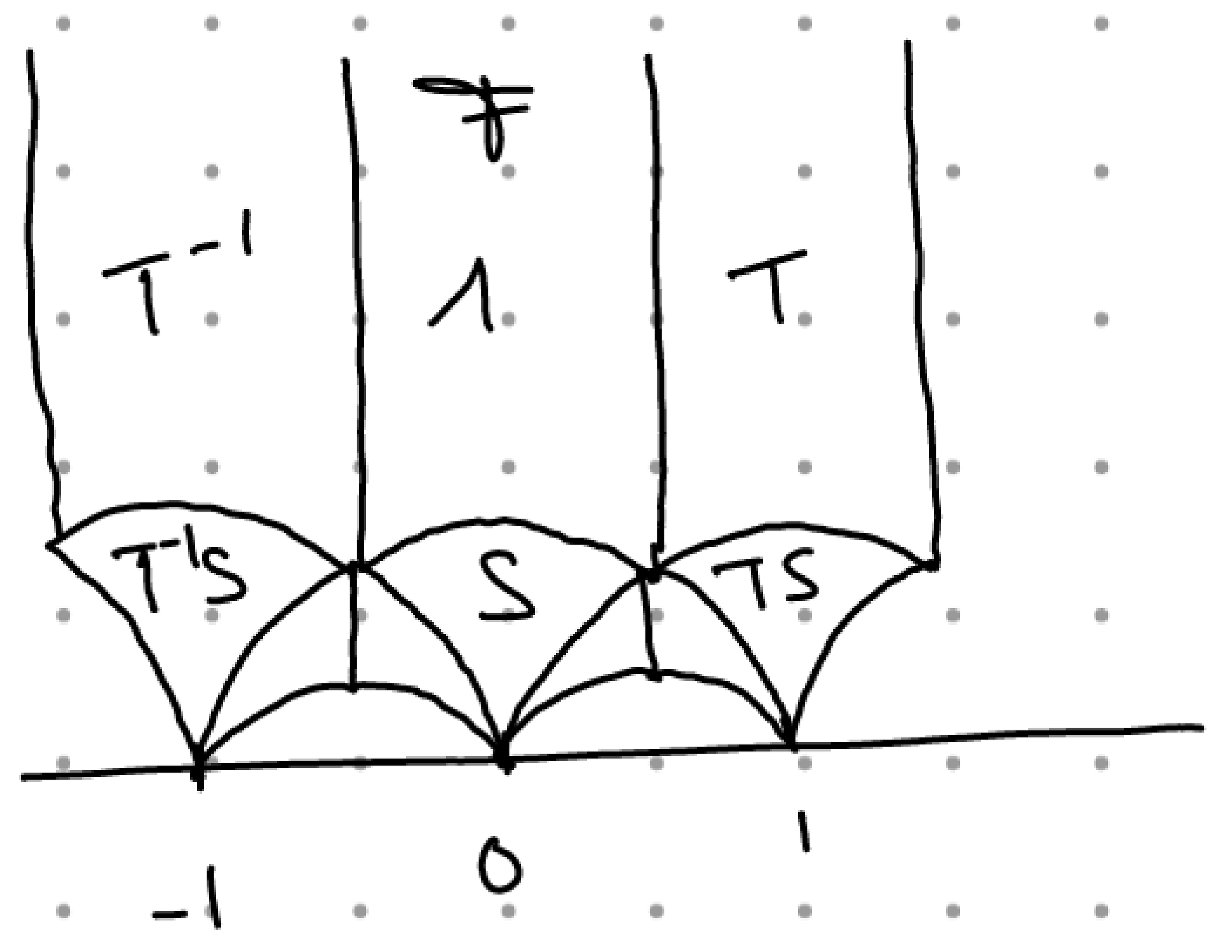
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \xrightarrow{S\cdot} \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \xrightarrow{T\cdot} \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

$\Rightarrow$ May perform Euclidean alg. on first column by $\langle S, T\rangle$-left-mult.

Remainder of form $\begin{pmatrix} \pm 1 & x \\ & \pm 1 \end{pmatrix} \in \langle S, T \rangle$. $\square$

Def $\mathcal{F} := \left\{ \tau \in \mathcal{H} \;\middle|\; \begin{array}{l} -1/2 \le \operatorname{Re} \tau \le 1/2 \\ |\tau| \ge 1 \end{array} \right\}$



<u>Prop</u> $\mathcal{F}$ is fundamental domain for $SL_2(\mathbb{Z})/_{\{\pm 1\}}$-action:

·) $SL_2(\mathbb{Z}) \cdot \mathcal{F} = \mathcal{H}$

·) $g \mathring{\mathcal{F}} \cap \mathcal{F} = \emptyset \quad \forall g \neq \{\pm 1\}$.

Prf Given τ, $|\mathrm{Re}\, T^n\tau| \leq 1/2$ for suitable n.

If $|T^n\tau| \geq 1$, done.

Otherwise, $\mathrm{Im}(ST^n\tau) = \dfrac{\mathrm{Im}\, T^n\tau}{|T^n\tau|} > \mathrm{Im}\, T^n\tau$.

Iterating shows $\mathcal{F} \cap SL_2(\mathbb{Z})\tau \neq \phi$.

For other property: See Serre VII.1 Thm 1. $\square$

Prop Given $\tau \in \mathcal{H}$, Stab τ conjugate to

$$\{\pm 1\}, \quad \underset{\simeq\, \mathbb{Z}/4}{\overset{(A)}{\left\langle \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \right\rangle}}, \quad \underset{\simeq\, \mathbb{Z}/6}{\overset{(B)}{\left\langle \begin{pmatrix} & -1 \\ 1 & 1 \end{pmatrix} \right\rangle}}$$

Prf $\mathrm{Stab}\, g\tau = g(\mathrm{Stab}\,\tau)g^{-1} \rightsquigarrow$ wlog $\tau \in \mathcal{F}$.

$$\mathrm{Im}\, g\tau = \frac{\mathrm{Im}\,\tau}{|c\tau+d|^2} = \mathrm{Im}\,\tau \implies |c\tau + d| = 1$$

$d = 0 \implies c = \pm 1$, implies $\tau = i$, Case (A)

$d = \pm 1 \implies \tau = \zeta_6$ or ζ_6^2. Case (B). $\square$

§3 $SL_2(\mathbb{Z})\backslash\mathcal{H}$ as a R.S.

Set $Y := SL_2(\mathbb{Z})\backslash\mathcal{H}$

<u>Thm</u> j is a homeomorphism $j : Y \xrightarrow{\sim} \mathbb{C}$ and, in ptic, endows Y w/ structure of R.S. It is the unique R.S. structure s.th. $\mathcal{H} \xrightarrow[pr]{} Y$ is holomorphic.

<u>Prf of bijectivity of j:</u> Holomorphic maps are open, so $j(Y) \subseteq \mathbb{C}$ is open.

show also closed: Let $(z_n)_n \subseteq j(Y)$ be converging seq. Choose $\tau_n \in \mathcal{F}$, $j(\tau_n) = z_n$.

If $\operatorname{Im}\tau_n$ bounded, $\exists$ converging subseq. by compactness of $\mathcal{F} \cap \{\operatorname{Im}\tau \leq C\}$ and we see $\lim z_n \in j(Y)$ as well.

<u>Lem</u> $\lim_{\operatorname{Im}\tau\to\infty} j(\tau) = \infty$.

<u>Prf</u> $\lim_{\operatorname{Im}\tau\to\infty} G_k(\tau) = 2\cdot \sum_{n\geq 1} \frac{1}{n^k}$

$\Rightarrow \lim_{\operatorname{Im}\tau\to\infty} g_2(\tau) = 120\,\frac{\pi^4}{90}$ $\quad \lim g_3(\tau) = 280\,\frac{\pi^6}{945}$

Yields $\lim_{\operatorname{Im}\tau\to\infty} \Delta(\tau) = 0$, $\lim j(\tau) = \infty$ $\square$

(The R.S. str. on Y is now defined purely formally:

$$Y \supseteq U \xrightarrow{\varphi} \mathbb{C} \text{ holomorphic } (\text{i.e. } \in \mathcal{O}_Y(U))$$

$$\Leftrightarrow \quad \varphi \circ j^{-1} : j(U) \longrightarrow \mathbb{C} \text{ holom.}$$
)

Pf of 2nd characterization

Composition $\mathcal{H} \xrightarrow{j} \mathbb{C} \xrightarrow{\sim} Y$ holomorphic

since by defn this map is holomorphic.

Uniqueness is following statement: For $U \subseteq \mathbb{C}$ open, connected

$f, g : U \longrightarrow \mathbb{C}$ non-constant holomorphic

& $\varphi : f(U) \longrightarrow g(U)$ $g = \varphi \circ f$.

Then φ is holomorphic.

$$\begin{tikzcd} & U \arrow[dl, "f"'] \arrow[dr, "g"] & \\ f(U) \arrow[rr, "\varphi"] & & g(U) \end{tikzcd}$$

Pf f', g' holomorphic, $\neq 0$ outside a discrete set. Shrinking U, may assume $\neq 0$ outside finite set S. Then φ holomorphic away from $f(S)$. Since also bounded near every $y \in f(S)$, extends holomorphically over $f(S)$. (Riemann Hebbarkeitsatz.) $\square$

§4 Back to ECs

<u>Prop</u> 1) $\forall j \in \mathbb{C}$ $\exists$ $E/\mathbb{C}$ w/ $j(E) = j$

2) $\forall (x,y) \in \mathbb{C}^2$ s.th. $x^3 - 27y^2 \neq 0$, $\exists \Lambda$ w/

$g_2(\Lambda) = x$, $g_3(\Lambda) = y$.

<u>Pf</u> 1) ok. 2) $j := x^3 / x^3 - 27y^2$, pick Λ_0 s.th. $j(\Lambda_0) = j$

If $j = 1$, $g_3(\Lambda_0) = y = 0$ ok, setting $\Lambda = a\Lambda_0$

for suitable a gives $g_2(\Lambda) = x$ while preserving $g_3(\Lambda) = 0$.

O/w, replacing Λ_0 by $a\Lambda_0$, may assume $g_2(\Lambda_0) = y$.

Then $g_2(\Lambda)^3 = \dfrac{-27y^2}{(1-j)} = x^3$

Then multiply Λ by suitable 6-th root of 1. $\square$

<u>Fundamental Observation</u>

<u>Prop</u> Given j, $\exists (x,y) \in \mathbb{Q}(j)^2$ s.th. $j = x^3 / x^3 - 27y^2$.

<u>Pf</u>: see Silverman §III.1 Prop 1.4. $\square$

In other words, the algebraic curve underlying E is defined over $\mathbb{Q}(j)$!

<u>Will see</u> Group structure also defined over $\mathbb{Q}(j)$.

§5 CM-elliptic curves

Prop 1) $\mathrm{Hom}(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda') = \{ a \in \mathbb{C} \mid a\Lambda \subseteq \Lambda' \}$

2) $\mathrm{End}(E) \cong \begin{cases} \mathbb{Z} \\ \text{order in imag-quad } K/\mathbb{Q}. \end{cases}$

Pf Any $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ lifts to univ covers

$\tilde{\varphi} : \mathbb{C} \to \mathbb{C}$ and is hence linear $\varphi(z) = az + c$.

Since group homo, $\tilde{\varphi}(0) = 0 \Rightarrow 1)$.

In prtic, $\mathrm{Hom}(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda') \subseteq \mathbb{C}$ discrete abelian group.

$\to 2)$. □

Def E is said to have <u>complex multiplication by K</u>

if $\mathrm{End}(E) \cong$ order of K. ($K/\mathbb{Q}$ imag quad.)

Prop Let $K/\mathbb{Q}$ quadratic extension.

1) If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ is the maximal order $\subseteq K$, then all orders are of form $\mathbb{Z}[n \cdot \alpha]$, $n \geq 1$. (n uniquely det.)

2) Let $\mathfrak{a} \subseteq K$ be a rank 2 sub $\mathbb{Z}$-module and $\mathcal{O} := \{ x \in K \mid x\mathfrak{a} \subseteq \mathfrak{a} \}$.

Then $\mathcal{O}$ is an order and $\mathfrak{a}$ is projective of rk 1 over $\mathcal{O}$. (Proof omitted.)

<u>Prop</u> 1) $\mathbb{C}/_{\mathbb{Z}+\mathbb{Z}\tau}$ CM by K $\iff$ $\tau \in K$
(wrt. any $K \hookrightarrow \mathbb{C}$.)

2) $\mathcal{O} \subseteq K$ order.

$$\{\text{ECs}/_{\mathbb{C}} \text{ w/ } \mathrm{End}(E) \simeq \mathcal{O}\}/_{\cong} \xrightarrow{\sim} \mathrm{Pic}(\mathcal{O})$$

3) If E has CM (by some K), then E is defined over $\overline{\mathbb{Q}}$.

<u>Proof</u> 1) From $a \cdot (\mathbb{Z}+\mathbb{Z}\tau) \subseteq \mathbb{Z}+\mathbb{Z}\tau$ & $a \notin \mathbb{Z}$

we can write $a \cdot 1 = x + y\tau$ w/ $y \neq 0$ and get

$$\tau = y^{-1}(a-x) \in \mathbb{Q}(a).$$

Conversely, if $\tau \in K$, then $n \cdot \tau^2 = x + y\tau$ w/ $x, y \in \mathbb{Z}$ if $n \gg 0$,

and hence $n\tau \in \mathrm{End}(\mathbb{C}/_{\mathbb{Z}+\mathbb{Z}\tau})$.

2) E w/ $\mathrm{End}(E) = \mathcal{O}$, pick Λ s.th. $E \simeq \mathbb{C}/_{\Lambda}$.

1) $\Rightarrow$ May assume $\Lambda \subseteq K$ (wrt some $K \hookrightarrow \mathbb{C}$)

Prev. prop. $\Rightarrow$ Λ is projective over $\mathcal{O}$, hence defines element of $\mathrm{Pic}(\mathcal{O})$. See yourself: This is an isomorphism.

3) By results in §4, need to see $j(E) \in \overline{\mathbb{Q}}$.

This is equivalent to the orbit

$$\mathrm{Aut}(\mathbb{C}/\mathbb{Q}) \cdot j(E) \text{ being finite.}$$

Choose Λ, write $E \cong V_+(p(X,Y,Z)) \subseteq \mathbb{P}^2_{\mathbb{C}}$

in corresponding Weierstraß eq.

Then, for $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$, $E^\sigma := \mathrm{Spec}\,\mathbb{C} \times_{\sigma, \mathrm{Spec}\,\mathbb{C}} E$

$$\cong V_+(\sigma(p)(X,Y,Z))$$

§4 $\Rightarrow$ Coeff. of <u>every Weierstraß eq</u> may be used to compute j!

Hence $j(E^\sigma) = \sigma \cdot j(E)$.

But, by functoriality, also $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$.

2) $\Rightarrow$ Only fin. many Es w/ given $\mathrm{End}(E)$.

$\Rightarrow \square$.

Rmk Points of Y for CM-ellipt curves are called special.

$GL_2(\mathbb{R}) \mathrel{\reflectbox{$\circlearrowright$}} \mathcal{H}^{\pm}$ transitively & $Stab(i) = SO(2)$.

This leads to Shimura variety presentation of Y:

$$Y = GL_2(\mathbb{Q}) \backslash \Big(GL_2(\mathbb{A}_f) / GL_2(\hat{\mathbb{Z}}) \times \underbrace{GL_2(\mathbb{R}) / SO(2)}_{= \mathcal{H}^{\pm}} \Big)$$

Given $K/\mathbb{Q}$ imag-quad + embedding of alg grps over $\mathbb{Q}$

$K^{\times} := Res_{K/\mathbb{Q}} \mathbb{G}_m \overset{\rho}{\hookrightarrow} GL_2$

+ choice of embedding $K \hookrightarrow \mathbb{C}$ (CM-type),

one gets by functoriality of Shimura data a finite subset

$$K^{\times} \backslash \mathbb{A}_{K,f}^{\times} / \rho^{-1}(GL_2(\hat{\mathbb{Z}})) \hookrightarrow Y.$$

Image is union of ECs w/ CM by K.

These special points play crucial role in defn of Shimura varieties as varieties over number fields (instead of $\mathbb{C}$).