Elliptic curves over $\mathbb{C}$

Recall the proposition:-

Proposition

If $\tau' \in \mathfrak{H}$ is fixed by a non-trivial element $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$, then $\mathrm{PSL}_2(\mathbb{Z})\tau' = \mathrm{PSL}_2(\mathbb{Z})\tau$ with $\tau^3 = 1$ or $\tau^4 = 1$.

We sketched a proof of the above proposition using a moduli interpretation of $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathfrak{H}$. We provide some more details here.

An elliptic curve over $\mathbb{C}$

Definition

An elliptic curve over $\mathbb{C}$ is $\mathbb{C}/\Lambda$, where $\Lambda \subset \mathbb{C}$ is a lattice.

Definition

Two elliptic cuvers X and Y are isomorphic if there exists a biholomorphic map $f\colon X \to Y$ such that $f(0) = 0$.

Definition

An isogeny between elliptic curves is a non-constant holomorphic map $f\colon X \to Y$ such that $f(0) = 0$.

Let $f\colon X \to Y$ be an isogeny between elliptic curves.

Proposition

f is surjective.

Proof.

A holomorphic map is open. Also, $f(X)$ is compact because X is compact. These two imply $f(X) = Y$ because Y is connected. $\square$

Let $X = \mathbb{C}/\Lambda_X, Y = \mathbb{C}/\Lambda_Y$ be elliptic curves. Let $f \colon X \to Y$ be a holomorphic map.

Proposition

There exists $\alpha \in \mathbb{C}$ such that $f(z) = \alpha z$. In particular, $\alpha\Lambda_X \subset \Lambda_Y$.

Proof.

Lift f to a map $\tilde{f} \colon \mathbb{C} \to \mathbb{C}$. Fix $\lambda \in \Lambda_X$. For any $z \in \mathbb{C}$, $\tilde{f}(z) - \tilde{f}(z + \lambda) \in \Lambda_Y$. Since Λ_Y is discrete, $\tilde{f}(z) - \tilde{f}(z + \lambda)$ is constanct. Differentiating it with respect to z, we conclude $\tilde{f}'(z)$ is doubly periodic. Any doubly periodic continuous map as compact image. By Liouville's theorem, $\tilde{f}'(z)$ is constant. Since $f(0) = 0$, we have $f(z) = \alpha z$ for some α. $\square$

Corollary

An isogeny between elliptic curves is a group homomorphism

Proof.

The map $z \longmapsto \alpha z$ is a group homomorphism. $\square$

Endomorphism ring of an elliptic curve

Let $E = \mathbb{C}/\Lambda$ be an elliptic curve. Let $\mathrm{End}(E)$ be the monoid of self-maps on E fixing zero. By the previous corollary, $\mathrm{End}(E)$ is a ring. We have a ring homomorphism

$$\mathrm{End}(E) \to \mathbb{C}$$

given by $(f\colon z \mapsto \alpha z) \mapsto \alpha$. This map is also injective. We can regard $\mathrm{End}(E)$ as a subring of $\mathbb{C}$. In particular, it is commutative.

Proposition

The $\mathbb{Z}$-rank of $\mathrm{End}(E)$ is at most two.

Proof.

Acting $\mathrm{End}(E)$ on Λ, we get an embedding of $\mathrm{End}(E) \hookrightarrow M_2(\mathbb{Z})$. It is a commutative subalgebra, which can have rank at most two. $\square$

We always have

$$\mathbb{Z} \subset \mathrm{End}(E).$$

If $\mathrm{End}(E)$ has rank one, then $\mathbb{Z} = \mathrm{End}(E)$.

If $\mathrm{End}(E)$ has rank two, we have two possibilities for $K = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$, which is a quadratic field extension of $\mathbb{Q}$. (Note that $\mathbb{Q} \times \mathbb{Q}$ doesn't embed into $\mathbb{C}$.)

1. $K = \mathbb{Q}(\sqrt{d})$ with $d > 0$, d square-free.
2. $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$, d square-free.

The former can't happen because it doesn't embed into $\mathbb{C}$.

Proposition

If $\mathbb{Z} \neq \mathrm{End}(E)$, $\mathrm{End}(E)$ is an order of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$.

Here, an order of a number field F of degree n means a subring $O \subset F$ of rank n.

Proposition

Let d be a square-free integer. The maximal order of $K = \mathbb{Q}(\sqrt{d})$ is given by $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3$ modulo 4, and by $\mathbb{Z}[\frac{\sqrt{d}+1}{2}]$ if $d \equiv 1$ modulo 4.

sketch of proof.

Maximal order consists of all algebraic integers. Classify all algebraic integers of the form $a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. $\square$

Proposition

Let $O \subset K$ be the maximal order of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$, d square-free. Then,

$$\#\left(O^{\times}\right) = \begin{cases} 1 & \text{if } d \neq 1, 3 \\ 2 & \text{if } d = 1 \\ 3 & \text{if } d = 3. \end{cases}$$

Proof.

One has to solve $a^2 + b^2(-d) = 1$ or $a^2 + b^2(-d) = 4$ depending on residue of d modulo 4. □

Proposition

Let $\tau \in \mathfrak{H}$, $\Lambda_\tau = \mathbb{Z} \oplus \tau\mathbb{Z}$, and $E_\tau = \mathbb{C}/\Lambda_\tau$. Then, E_τ has an automorphism other than ± 1 if and only of τ is fixed by a non-trivial $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$.

Proof.

An automorphism of E_τ is an auotmorphism of $\mathbb{C}/\Lambda_\tau$. Thus, it preserves Λ_τ. Writing it with respect to the basis $\langle 1, \tau \rangle$, we get an element of $\mathrm{SL}_2(\mathbb{Z})$. Conversely, $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ fixing τ yields an automorphism: multiplication by $c\tau + d$. Indeed,

$$\begin{aligned}(c\tau + d)\left(\mathbb{Z} + \tau\mathbb{Z}\right) &= (c\tau + d)\mathbb{Z} + \left(c\tau^2 + d\tau\right)\mathbb{Z} \\ &= (c\tau + d)\mathbb{Z} + (a\tau + b)\,\mathbb{Z} \\ &= \mathbb{Z} + \tau\mathbb{Z}.\end{aligned}$$

$\square$

Conclusion: up to $\mathrm{PSL}_2(\mathbb{Z})$-equivalence, only

$$\tau = \sqrt{-1}$$
$$\tau = \frac{1+\sqrt{-3}}{2}$$

have non-trivial fixed points.