# § Elliptic curve.

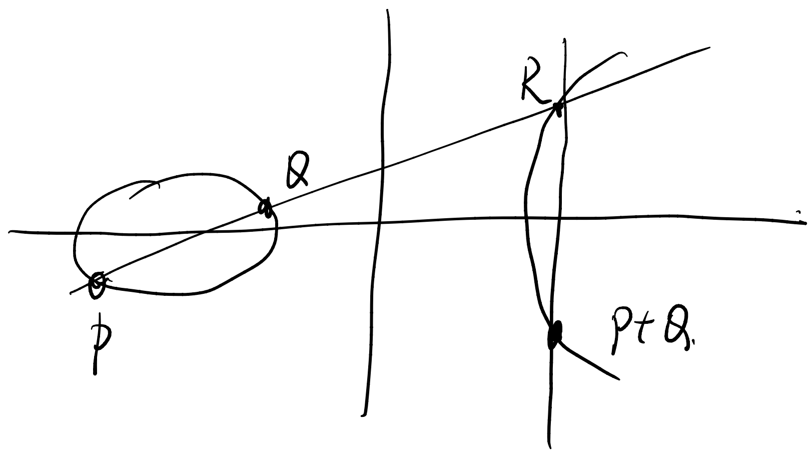
Definition.

(1) Smooth projective curve over $k$ of genus one with distinguished rational point $O \in E(k)$

when char $k \neq 2, 3$. It is defined by a Weierstrass equation.

$$y^2 z = x^3 + Ax^2 z + Bz^3 \quad \text{with discriminat } \Delta = 4A^3 + 27B^2 \neq 0$$

We can define group law on $E(k)$ to make it become abelian group.




(2). Elliptic curve is an abelian variety of dimension 1.

Weierstrass equation is not intrinsic. We can change it if we embeded the elliptic curve into $\mathbb{P}^2$ by different ways.

However, $j(E) = \dfrac{2^8 \cdot 3^3 A^3}{4A^3 + 27B^2}$ is independent of choice of Weierstrass equation. We call it $j$-invariant.

(J1) If $E$ and $E'$ are $\bar{k}$- elliptic curves, then $E \cong E'$ $\Longleftrightarrow$ $j(E) = j(E')$

(J2) For every $j \in \mathbb{C}$, there exists an $E$ with $j(E) = j$

" $j$-line is the moduli space of elliptic curves "

" $j$-line parametrizes elliptic curves "

Our goal is to define Shimura curves.

" Shimura curves parametrize abelian surfaces with potential quaternionic multiplication (PQM) "

## § lattices

Over $\mathbb{C}$, $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, where $\Lambda \cong \mathbb{Z}^2$ is a lattice

(Lattice in $\mathbb{C}$ is a two-dimensional $\mathbb{R}$-vector space)

Hence topologically, $E(\mathbb{C})$ is a torus.

View $\mathbb{C} = \mathbb{R}^2$, we can determine a lattice $\Lambda$ by giving its basis $v_1, v_2 \in \mathbb{R}^2$. The matrix $[v_1 | v_2] \in GL_2(\mathbb{R})$

$$\{\text{lattice in } \mathbb{C}\} \underset{\text{not 1 to 1.}}{\longleftrightarrow} GL_2(\mathbb{R})$$

need reduce it by equivalent relation

Fact:

Two elliptic curve $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda' \iff \exists\, \alpha \in \mathbb{C}^\times$ s.t. $\alpha\Lambda = \alpha\Lambda'$

Hence we need consider the quotient $GL_2(\mathbb{R})/\mathbb{C}^\times$

In other words whenever we have a basis $[z_1 | z_2]$

We can change it into the form $[1, \tau]$ by multiplying a complex number $\frac{1}{z_1}$

Hence. $GL_2(\mathbb{R}) / \mathbb{C}^\times \cong \mathcal{H}^{\pm} = \{ x+yi \mid y \neq 0 \}$

Now we require $\tau \in \mathcal{H}^+$. This can be viewed as requiring our basis vector $[z_1 | z_2]$ to be positively oriented.

$$\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$$

Fact: $\Lambda_\tau \cong \Lambda_{\tau'} \iff \exists \begin{bmatrix} a, & b \\ c, & d \end{bmatrix} \in SL_2(\mathbb{Z})$ s.t $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \tau = \tau'$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

$$\{ \text{elliptic curves}/\mathbb{C} \} \xleftrightarrow{1:1} \mathcal{H} / SL_2(\mathbb{Z}) = GL_2(\mathbb{Z}) \backslash GL_2(\mathbb{R}) / \mathbb{C}^\times$$

$$\{ \text{elliptic curves}/\mathbb{C} \} \xleftrightarrow{j} \mathbb{A}^1$$

## Modular Curve

We get moduli space of elliptic curves over $\mathbb{C}$ by looking at the quotient space $SL_2(\mathbb{Z})$ acting on $\mathcal{H}$.

We can generalize the idea by using subgroup $\Gamma \subset SL_2(\mathbb{Z})$ acting on $\mathcal{H}$.

Define:

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

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \bmod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \bmod N \right\}$$

We have $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z}) = \Gamma(1)$

Def. A group $\Gamma$ such that $\Gamma(N) \subset \Gamma \subset SL_2(\mathbb{Z})$ is called congruence group of $SL_2(\mathbb{Z})$

Def. $Y(\Gamma) = \Gamma \backslash \mathcal{H}$.

We have a natural map

$$Y(\Gamma(N)) \to Y(\Gamma_1(N)) \to Y(\Gamma_0(N)) \to Y(1)$$

Prop.

① $Y(\Gamma_0(N)) \xleftrightarrow{1 \text{ to } 1} \{ \text{pair } (E, C), \text{ where } C \text{ is cyclic subgroup of } E[N] \} / \sim$

$$[\tau] \longmapsto [(E_\tau, \langle \tfrac{1}{N} + \Lambda_\tau \rangle)]$$

② $Y(\Gamma_1(N)) \xleftrightarrow{1 \text{ to } 1} \{ \text{pair } (E, Q), \text{ where } Q \text{ is a point in } E[N] \} / \sim$

$$[\tau] \longmapsto [(E_\tau, \tfrac{1}{N} + \Lambda_\tau)]$$

③ $Y(\Gamma(N)) \xleftrightarrow{1 \text{ to } 1} \{ \text{pair } (E, (P, Q)) \text{ where } P, Q \text{ are two points that generate } E[N] \text{ with a fixed weil pairing value} \} \sim$

$$[\tau] \longrightarrow [\,(E_\tau, (\tfrac{\tau}{N} + \Lambda_\tau, \ \tfrac{1}{N} + \Lambda_\tau)\,)$$

§ Rational model.

In previous section, $Y(\Gamma)$ are curves defined over $\mathbb{C}$. In fact, they can be defined over number field.

Prop. There are curves $Y(\Gamma_0(N))$, $Y(\Gamma_1(N))$ defined over $\mathbb{Q}$ such that

$$Y(\Gamma_0(N)) \otimes_{\mathbb{Q}} \mathbb{C} = \Gamma_0(N)\backslash\mathcal{H}.$$

$$Y(\Gamma_1(N)) \otimes_{\mathbb{Q}} \mathbb{C} = \Gamma_1(N)\backslash\mathcal{H}.$$

In general, if $\Gamma \supset \Gamma(N)$, there are curves $Y(\Gamma(N))$ defined over $\mathbb{Q}(\zeta_N)$ where $\zeta_N$ is a primitive $N$th root of unity such that

$$Y(\Gamma(N)) \otimes_{\mathbb{Q}(\zeta_N)} \mathbb{C} = \Gamma(N)\backslash\mathcal{H}$$