VI. Complex multiplication (I)

VI.1. Complex elliptic curves

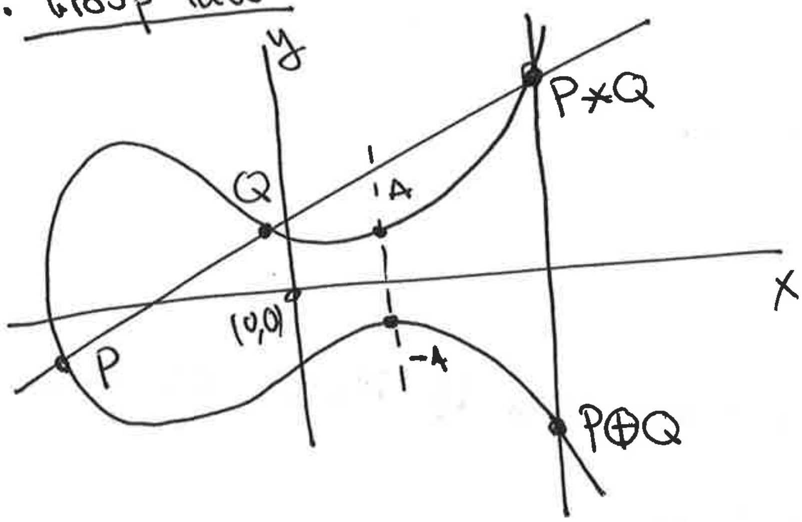
Def: K field. An elliptic curve over K is a pair (E, O) where $E = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(K),\ f(x_0 : x_1 : x_2) = 0\}$ smooth projective curve defined by $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ homogeneous of degree 3, and $O \in (x_0 : x_1 : x_2) \in E(K)$.

- If $\mathrm{char}(K) \neq 2, 3$, after a change of vbles we can suppose that $E = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(K) \mid x_1^2 x_2 = x_0^3 + A x_0 x_2^2 + B x_2^3\}$; $A, B \in K$ and $O = (0:1:0)$.
- The fact that E is smooth means that $\left(\frac{\partial F}{\partial x_0}(P), \frac{\partial F}{\partial x_1}(P), \frac{\partial F}{\partial x_2}(P)\right) \neq (0,0,0)$ $\forall P \in E(\overline{K})$. This is equivalent to $\Delta_E := -16(4A^3 - 27B^2) \neq 0$. (Exercise)

Def: The quantity Δ_E is called the discriminant of E.
The quantity $j_E := 1728 \frac{(4A)^3}{\Delta_E}$ is called the j-invariant of E.

- Setting $x_2 = 0$ to be the ∞ line, in the affine plane $x_2 = 1$ we have: $E: y^2 = x^3 + Ax + B$ (Weierstrass equation).

- Group law



$\oplus : E(K) \times E(K) \to E(K)$
$(P, Q) \longmapsto P \oplus Q$

defines a group law where the neutrom is O.

Prop: $P, Q, R \in E(K)$ are colinear $\Leftrightarrow P \oplus Q \oplus R = O$.

Actually, M can be taken to be of the form $\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & 1 \end{pmatrix}$; $\lambda, \mu \in \overline{K}$.

Prop (Sil. I, Thm 1.4) a) $E_1 \simeq E_2 \Leftrightarrow j_{E_1} = j_{E_2}$. In that case, the isomorphism is given by $\begin{pmatrix} u^2 & 0 & 0 \\ 0 & u^3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $u \in \overline{K}$. (exercise).

b) $\forall j \in K$, $\exists E_x$ elliptic curve s.t. $j(E_x) = j$.

· The uniformisation theorem (Sil. I, Ch. VI)

Def: Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subseteq \mathbb{C}$ be a full rank lattice.

$$P_\Lambda(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}}' \frac{1}{(\omega - z)^2} - \frac{1}{\omega^2} \equiv \text{the Weierstrass } \wp\text{-function.}$$

This is a doubly periodic meromorphic function with poles at Λ.

Def: $(k \geq 2)$. (The Eisenstein functions)

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^{2k}}. \qquad g_2(\Lambda) := 60\, G_4(\Lambda), \qquad g_3(\Lambda) := 140\, G_6(\Lambda).$$

If $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$, where $\operatorname{Im}(\tau) > 0$, then $G_{2k}(\tau) := G_{2k}(\Lambda)$ is a weakly-modular form of weight $2k$:

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \qquad G_{2k}\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{2k} G_{2k}(\tau).$$

Moreover $G_{2k}(\infty) = \lim_{\operatorname{Im}(\tau) \to \infty} G_{2k}(\tau) = 2\zeta(2k)$. ($\Rightarrow$ indeed, G_{2k} are modular forms).

Thm: Let $E/\mathbb{C}$ be a complex elliptic curve $\Rightarrow \exists \Lambda \subseteq \mathbb{C}$ full rank lattice s.t.

$$\Psi_E : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$$
$$\overline{z} \longmapsto (P_\Lambda(z) : P'_\Lambda(z) : 1)$$

is an analytic isomorphism. In particular, $\Psi_E(\overline{z}_1 + \overline{z}_2) = \Psi_E(\overline{z}_1) \oplus \Psi_E(\overline{z}_2)$.

Obs: For $\Lambda \subseteq \mathbb{C}$, $\operatorname{Im}(\Psi_{E_\Lambda}) = E_\Lambda : y^2 = 4x^3 - g_2 x - g_3$.

<u>Def</u>: E_1/K and E_2/K elliptic curves are isogenous if ~~$\exists\phi$:~~
$\exists\, \phi: E_1 \to E_2$ morphism of curves s.t. $\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$
$\forall P, Q \in E_1, E_2$. Such ϕ is called an isogeny.

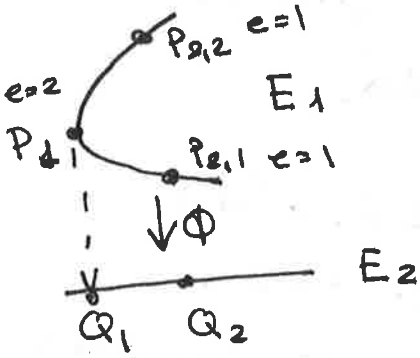
<u>Prop</u>: $\phi: E_1 \to E_2$ morphism of curves is an isogeny $\Leftrightarrow$ $\phi(O_{E_1}) = O_{E_2}$
("$\Leftarrow$" non-trivial, see Silverman I, ch. III.4).

If $\phi: E_1 \to E_2$ is an isogeny, then $\phi^*: K(E_2) \longrightarrow K(E_1)$.
$$f \longmapsto f \circ \phi = \phi^* f$$

<u>Def</u>: $\deg(\phi) = [K(E_1) : \phi^* K(E_2)]$, $\boxed{\text{e.g. } [n]: E \to E \text{ isogeny. } \operatorname{Ker}[n] = E[n] = n\text{-torsion}}$

<u>Prop</u>: $\phi: E_1 \to E_2$ morphism of curves. Then, either ϕ is constant or ϕ is surjective. See Silverman I, ch. 2.

<u>Def</u>: Let $Q \in E_2$, $P \in E_1$, $\phi(P) = Q$. Take t_Q uniformiser at Q, i.e. $t_Q \in K(E_2)$, $\operatorname{ord}_Q(t_Q) = 1$.
$$e_P(\phi) = \operatorname{ord}_P(t_Q \circ \phi).$$



<u>Prop</u>: a) $\forall Q \in E_2$, $\sum_{P \in \phi^{-1}(Q)} e_P(\phi) = \deg(\phi)$

b) $\deg [n] = n^2$.

<u>Def</u>: $\phi: E_1 \to E_2$ isogeny is an isomorphism if it's bijective and ϕ^{-1} is an isogeny $\Leftrightarrow$ $\deg(\phi) = 1$.

In that case, $\phi(X_0 : X_1 : X_2) = M \begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix}$, $M \in GL_2(\bar{K})$.

Def.: 2 lattices Λ_1, Λ_2 are homothetic if $\exists \alpha \in \mathbb{C} \mid \alpha \Lambda_1 = \Lambda_2$.

So, can assume $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$, $\tau \in \mathcal{H} = \{ z \in \mathbb{C} \mid \mathrm{Im}(z) > 0 \}$.

Prop: There is a bijection between

$$\left\{ \begin{array}{l} \text{complex tori} \\ \mathbb{C}/\Lambda \end{array} \right\} / \text{homothety} \xrightarrow{\sim} \left\{ \begin{array}{l} \text{complex} \\ \text{elliptic curves} \end{array} \right\} / \text{isomorphism}.$$

Def: $\Delta : \mathcal{H} \longrightarrow \mathbb{C}$
$\tau \longmapsto g_2(\tau)^3 - 27 g_3(\tau)^2$

$j : \mathcal{H} \longrightarrow \mathbb{C}$
$\tau \longmapsto 1728 \dfrac{g_2(\tau)^3}{\Delta(\tau)}$.

Prop: Δ is a modular form of weight 12.
j is a weakly modular function (weight $=0$). It's meromorphic at ∞, namely, $j(q) = \frac{1}{q} + \sum_{n \geq 0} a_n q^n$, $q = e^{2\pi i z} = 0 \Longleftrightarrow z := \infty$.