Elliptic Curves (Part 2, ISOGENIES)

– Last Session (review and complement)

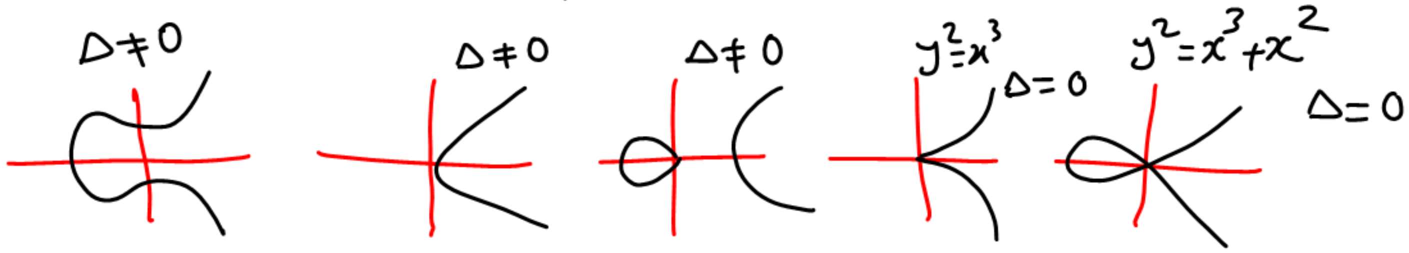
Weierstrass Equation$/K$: (coeff of W.E. $\in K$)

$$\begin{cases} E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 & \text{general} \\ E: y^2 = 4x^3 + b_2x^2 + b_4x + b_6 & \text{char}(K) \neq 2 \\ E: y^2 = x^3 + Ax + B & \text{char}(K) \neq 2, 3 \end{cases}$$

Δ_E, j_E

– E is nonsingular iff $\Delta_E \neq 0$

– Every nonsingular W.E.$/K$ defines an E.C.$/K$ and vice versa.



– If E.C.$/K$ (W.E.$/K$), then we can think about

K-points (K-rational points), or more generally L-points

for any field extension L/K:

$$E(L) = \{(x, y) \in L \text{ s.t. } y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\}$$

(When we just write E, we mean $E(\overline{K})$)

– for $K \subseteq L \subseteq M$ and E/K, we have: $E(L) \otimes_L M \simeq E(M)$

This is called "base change".

$$E/\mathbb{Z} \longrightarrow \begin{cases} E_i / \mathbb{F}_{p_i} \\ E_\infty / \mathbb{Q} \end{cases}$$

– For a curve C/K, a divisor D is defined as a formal sum

$$D=\sum_{P\in C} n_P\cdot P \quad \text{where } n_P=0 \text{ for almost all } P\in C$$

If $D_1=\sum_{P\in C} n_P\cdot P$ and $D_2=\sum_{P\in C} m_P\cdot P$, $D_1+D_2:=\sum (n_P+m_P)\cdot P$

Consider the set of all divisors of C with $\mathrm{Div}(C)$.

Then $\mathrm{Div}(C)$ is an abelian group.

for $D=\sum n_P\cdot P$, we define degree D as $\deg(D)=\sum n_P$.

If D_1, D_2 are degree-zero divisors, then so is D_1+D_2.

So, the set of degree-zero divisors, $\mathrm{Div}^0(C)$, form a subgroup of $\mathrm{Div}(C)$.

For a $\underset{\text{irreducible}}{\text{curve}}$ C/K, the function field of it defines as

$\mathrm{frac}\left(\frac{K[X]}{I}\right)$ where I is the ideal generated by the $= \mathrm{frac}(\underbrace{K[C]}_{\text{coordinate ring}}) = K(C)$

equations that define C. For example, for an elliptic curve E/K,

$$K(E) = \mathrm{frac}\left[\frac{K[x,y]}{\langle y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x^4-a_6\rangle}\right] = \mathrm{frac}\,[K[E]]$$

The elements of $K(C)$ are called (rational) functions on C. For $f \in K(C)^\times$, the divisor of f is defined as

$$\mathrm{div}(f) := \sum_{P \in C} \underbrace{\mathrm{ord}_P(f)}_{\text{the order of vanishing of } f \text{ at } P.} \cdot P \;.$$

Note that $\mathrm{div}(f)$ is of degree zero for all $f \in K(C)^\times$.
So, $K^\times \hookrightarrow K(C)^\times \hookrightarrow \mathrm{Div}^0(C) \hookrightarrow \mathrm{Div}(C)$

A divisor $D \in \mathrm{Div}(C)$ is called a principall divisor if $\exists f \in K(C)^\times$ s.t. $D = \mathrm{div}(f)$

We define $\mathrm{Pic}(C) := \dfrac{\mathrm{Div}(C)}{\mathrm{Princ.Div}(C)}$ & $\mathrm{Pic}^0(C) = \dfrac{\mathrm{Div}^0(C)}{\mathrm{Pric.Div}(C)}$.

$\mathrm{Prin.Div}(C) = \dfrac{K(C)^\times}{K^\times}$

geometric group law $\longleftrightarrow$ algebraic group law

For an E.C. E, we have an isomorphis $E \xrightarrow{\simeq} \mathrm{Pic}^0(E)$.
$P \longmapsto [(P) - (O_E)]$

For an elliptic curve E/K, we have:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & \bar{K}^\times & \longrightarrow & \bar{K}(E)^\times & \longrightarrow & \mathrm{Div}^0(E) & \longrightarrow & \mathrm{Pic}^0(E) & \longrightarrow & 0 \\
0 & \longrightarrow & K^\times & \longrightarrow & K(E) & \longrightarrow & \mathrm{Div}^0_K(E) & \longrightarrow & \mathrm{Pic}^0_K(E) & \longrightarrow & 0
\end{array}$$

taking Gal. invarint

base change

— Isogenies:

Theorem: For $E/_K$, the maps $+: E\times E \longrightarrow E$ & $-: E \longrightarrow E$ are morphism.
$(P,Q) \longmapsto P+Q$ $\quad P \mapsto -P$

Remark: For a map of curves $f: C_1 \longrightarrow C_2$, it is constant or surjective.

Def: Let E_1 and E_2 be two E.C.. An isogeny from E_1 to E_2 is

a morphism $\varphi: E_1 \rightarrow E_2$ s.t. $\varphi(O_{E_1}) = O_{E_2}$.

(some authors restric their attention to nonconstant maps)

Remark: $\underbrace{\text{An isogeny}}_{\text{nonconstant}}$ between elliptic curves E_1 and E_2 is a

finite map of curves, i.e. $K[E_1]$ is a finitely generated $K[E_2]$-mod.

(for a map of curves $g: C_1 \rightarrow C_2$ we have map of rings

$g^*: K[C_2] \longrightarrow K[C_1]$ and map of fields $g^*: K(C_2) \longrightarrow K(C_1)$)

Def: Two E.C. $/_K$ E_1, E_2 are called isogenous if there is

an isogeny between them.

Def: For the nonconstant isogeny φ, $\varphi^*: \overline{K}(E_2) \longrightarrow \overline{K}(E_1)$ is injective.

The degree of φ, $\deg(\varphi)$, is the degree of the finite extension

$$\overline{K}(E_1) \big/ \psi^* \overline{K}(E_2) \quad \left(\overline{K}(E_1) \big/ \overline{K}(E_2) \right)$$; and similarly for the sep. and insep. degree.

$\underbrace{\text{sep.}}_{\deg_s \psi}$ $\underbrace{\text{insep.}}_{\deg_i \psi}$

Notation:

$$\mathrm{Hom}(E_1, E_2) = \{E_1 \xrightarrow{\text{isogeny}} E_2\} \rightsquigarrow (\psi+\psi')(P) = \psi(P) + \psi'(P)$$

$$\text{If } E_1 = E_2 = E \rightsquigarrow \mathrm{End}(E) = \mathrm{Hom}(E,E) \rightsquigarrow \begin{cases} (\psi+\psi')(P) = \psi(P) + \psi'(P) \\ (\psi\psi')(P) = \psi(\psi'(P)) \end{cases}$$

The invertible elements of $\mathrm{End}(E)$ form the automorphism group of E, denoted by $\mathrm{Aut}(E)$.

Remark: If E_1 and E_2 are defined $/K$, we can restrict our attention to those isogenies defined $/K$, denoted by $\mathrm{Hom}_K(E_1, E_2)$, $\mathrm{End}_K(E)$, $\mathrm{Aut}_K(E)$.

Example: for each $m \in \mathbb{Z}$, we define the multiplication-by-m isogeny $[m]: E \longrightarrow E$ as follows:

for $m > 0$, $[m](P) = \underbrace{P + \cdots + P}_{m \text{ times}}$, for $m = 0$, $[0](P) = O_E$

for $m<0$, $[m](P) = [-m](-P) = \underbrace{-P-P-\cdots-P}_{m \text{ times}}$

Note that if E is defined$/K$, then so is $[m]$.

Theorem: (a) Let E/K be an E.C. and let $0 \neq m \in \mathbb{Z}$. Then

multiplication-by-m map $[m]: E \longrightarrow E$ is nonconstant.

(b) $\mathrm{Hom}_{\overline{K}}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-mod.

(c) $\mathrm{End}(E)$ is a domain of char. 0 (not necessarily commutative).

Remark: If $\mathrm{char}(K)=0$, then the map $\begin{aligned} \mathbb{Z} &\longrightarrow \mathrm{End}(E) \\ m &\longmapsto [m] \end{aligned}$

is usually the whole story, i.e. $\mathrm{End}(E) \simeq \mathbb{Z}$.

If $\mathrm{End}(E) \supsetneq \mathbb{Z}$, the we say that E has complex multiplication (CM for short). E.C. with C.M. have many special proproties (Modularity and L-function, CFT (Class FT), ...). Note that if K is a finite field, then always $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

$y^2 = x^3 - d^2 x$

CNP

Example:

Let $\mathrm{Char}(K) \neq 2$. Let $E: y^2 = x^3 - x$ and

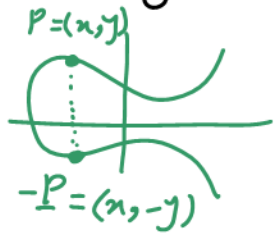
$$\begin{aligned} [i]: E &\longrightarrow E \\ (x,y) &\longmapsto (-x, iy) \end{aligned}$$

. Then $[i] \in \mathrm{End}(E)$ and so E has CM.

Note that $[i]$ is defined$/K$ iff $i \in K$. So we see that we may have $\mathrm{End}(E) \supsetneq \mathrm{End}_K(E)$.

We have $[i]\circ[i](x,y) = [i](-x, iy) = (x,-y) = \overset{\text{group operation}}{-}(x,y)$

(if $P = (x,y) \Rightarrow -P = (x,-y)$)



So, $[i]\circ[i] = [-1]$. Thus we have a ring homomorphism

$$\begin{aligned} \mathbb{Z}[i] &\longrightarrow \mathrm{End}(E) \\ m+ni &\longmapsto [m] + [n]\circ[i] \end{aligned}$$

If $\mathrm{char}(K) = 0$, this is an isomorphism and $\mathrm{Aut}(E) = \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Important Example:

Let $\mathrm{char}(K) = p > 0$ and $q = p^r$. Let E/K is an E.C. given by a W.E.. We define $E^{(q)}/K$ by raising the

$E: y^2 = x^3 + ax \to E^{(q)}: y^2 = x^3 + a^q x$

coefficients of W.E. of E to the q-th power, and the Frobenius morphism φ_q is defined as

$$\begin{aligned} \varphi_q : E &\longrightarrow E^{(q)} \\ (x,y) &\longmapsto (x^q, y^q) \end{aligned}.$$

Note that $\Delta(E^{(q)}) = \Delta(E)^q$ and $j(E^{(q)}) = j(E)^q$.

(Since $\begin{aligned} K &\to K \\ x &\mapsto x^q \end{aligned}$ is a homomorphism and Δ & j are defined by algebraic relations.).

So $E^{(q)}$ is nonsingular, because $E^{(q)}$ is the zero locus of a W.E..
Thus $E^{(q)}$ is also an E.C.. If $K = \mathbb{F}_q$, then the q-th power map $\begin{matrix} K \longrightarrow K \\ x \longmapsto x^q \end{matrix}$ is identity and so $E = E^{(q)}$. In this case,

$\varphi_q \in \mathrm{End}(E)$ is called the Frobenius endomorphism. Note that $E(\mathbb{F}_q) = E^{\varphi_q} = \{(x,y) \in E(\overline{\mathbb{F}_q}) \mid \underbrace{\varphi_q(x,y)}_{(x^q,\, y^q)} = (x,y)\}$.

Def: For $m \in \mathbb{N}$, the m-torsion subgroup of E/K is the set $E[m] := \{P \in E(\overline{K}) \mid [m](P) = 0\}$ (which is of exponent m).
$\hookrightarrow = \ker[m]$

The torsion subgroup of E is the set of points of finite order:

$$E_{tors} := \bigcup_{m=1}^{\infty} E[m].$$

$E[m](L)$ for $L \supseteq K$

If E/K, then $E[m](K)$ and $E_{tors}(K)$ denote the points of exponent m in $E(K)$ and points of finite order in $E(K)$, respectively.

example: Let E/K and $Q \in E$. Then, tranlation-by-Q

map $\eta_Q : E \longrightarrow E$ is an isomorphism since
$P \longmapsto P+Q$

η_{-Q} is its inverse. Note that it is not an isogeny unless $Q = O_E$.

Remark: Let $F : E_1 \longrightarrow E_2$ be an arbitrary morphism.

Then, $\underbrace{\Psi = \eta_{-F(O_{E_1})} \circ F}$ is an isogeny, since $\Psi(O_{E_1}) = O_{E_2}$.

So, $F = \eta_{F(O_{E_1})} \circ \Psi$. (analogy with Euclidean geomtry: every isometry can be written as a composition of a translation and a rotation.)

Theorem: Let $\Psi : E_1 \longrightarrow E_2$ be an isogeny. Then we have

$\Psi(P+Q) = \Psi(P) + \Psi(Q) \ \forall \, P, Q \in E_1$. In fact, isogenies are group homomorphisms. Note that, if $E_1, E_2 / K$, then each $\Psi' \in Hom_K(E_1(K), E_2(K))$ is also a group homomorphism.

Cor: For a non-zero isogeny $\Psi : E_1 \longrightarrow E_2$, $\ker(\Psi) = \Psi^{-1}(O_{E_2})$ is a finite group.

Theorem: Let $\psi : E_1 \to E_2$ be a non-zero isogeny.

(a) $\forall Q \in E_2 : \#\psi^{-1}(Q) = \deg_s \psi$ (and $\forall P \in E_1 : e_\psi(P) = \deg_i \psi$)

(b) The map
$$\ker\psi \longrightarrow \mathrm{Aut}\left(\overline{K}(E_1) / \psi^* \overline{K}(E_2)\right)$$
$$P \longmapsto \eta_P^*$$
is an isomorphism. (η_P is translation-by-P map, and η_P^* is the automorphism that η_P induces on $\overline{K}(E_1)$:
$$\eta_P : E_1 \to E_2 \implies \eta_P^* : \overline{K}(E_2) \hookrightarrow \overline{K}(E_1)$$
$$f \longmapsto f \circ \eta_P$$
)

(c) Suppose that ψ is separable. Then, (ψ is unramified and) $\#\ker\psi = \deg\psi$ and $\overline{K}(E_1)$ is a Galois extension of $\psi^* \overline{K}(E_2)$.

Theorem: Let E be an E.C. and $\Lambda \subseteq E$ is a finite subgroup. Then, there are a unique E.C. E' and a separable isogeny $\psi : E \to E'$ s.t. $\ker\psi = \Lambda$.

$E' \simeq E/\Lambda$ $\qquad\qquad$ $\dfrac{E}{\Omega} \simeq E'$

Dual Isogenies:

Theorem: Let $\varphi: E_1 \longrightarrow E_2$ be a nonconstant isogeny of degree m.

(a) There exist a unique isogeny $\hat{\varphi}: E_2 \longrightarrow E_1$ s.t. $\hat{\varphi} \circ \varphi = [m]$.

(b) As a group homomorphis, $\hat{\varphi}$ equals to the following composition:

$E_1 \xrightarrow{\varphi} E_2 \longrightarrow \varphi^* : \bar{K}(E_2) \longrightarrow \bar{K}(E_1)$

$$\begin{tikzcd} E_2 \arrow[r] & \mathrm{Div}^0(E_2) \arrow[r, "\varphi^*"] & \mathrm{Div}^0(E_1) \arrow[r, "\mathrm{sum}"] & E_1 \end{tikzcd}$$

$$Q \longmapsto (Q) - (O_{E_2})$$

$$\sum_{P \in E} n_P \cdot P \longmapsto \sum_{P \in E} [n_P] . P$$

$$(T) \longmapsto \sum_{S \in \varphi^{-1}(T)} e_{\varphi}(S) . S$$

Def: Let $E_1 \xrightarrow{\varphi} E_2$ be an isogeny. The dual isogeny to φ is the isogeny $\hat{\varphi}$ which defined in the last theorem.

(for $\varphi = [0]$, we set $\hat{\varphi} = [0]$)

Theorem: Let $\varphi: E_1 \longrightarrow E_2$ be an isogeny.

(a) Let $\deg \varphi = m$. Then $\hat{\varphi} \circ \varphi = [m]$ on E_1, and $\varphi \circ \hat{\varphi} = [m]$ on E_2.

(b) Let $\lambda: E_2 \to E_3$ be another isogeny. Then $\widehat{\lambda \circ \varphi} = \hat{\varphi} \circ \hat{\lambda}$:

$$
\begin{tikzcd}
E_1 \arrow[r, "\psi"'] \arrow[dr, "\lambda\circ\psi"] & E_2 \arrow[l, bend right, "\hat{\psi}"'] \arrow[d, "\lambda"'] \\
& E_3 \arrow[u, bend right, "\hat{\lambda}"'] \arrow[ul, bend left, "\widehat{\lambda\circ\psi}"]
\end{tikzcd}
$$

(c) Let $\psi' : E_1 \to E_2$ be another isogeny. Then:

$$\widehat{\psi+\psi'} = \hat{\psi} + \hat{\psi'}.$$

(d) For all $m \in \mathbb{Z}$ (including zero) we have $\widehat{[m]} = [m]$ and

$\deg([m]) = m^2$.

(e) $\deg(\hat{\psi}) = \deg(\psi)$.

(f) $\hat{\hat{\psi}} = \psi$.

Cor: Let E/K be an E.C. and let $0 \neq m \in \mathbb{Z}$.

(a) If $m \neq 0$ in K (i.e. $\operatorname{char}(K) = 0$ or $p = \operatorname{char}(K) \nmid m$), then

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(b) If $\operatorname{char}(K) = p$, then one of the following is true:

(i) $E[p^n] = \{O_E\} \quad \forall n \in \mathbb{N}$

(ii) $E[p^n] = \mathbb{Z}/p^n\mathbb{Z} \quad \forall n \in \mathbb{N}$

(C) If $m = 0$ in K (i.e. $\mathrm{char}(K) = p$ & $p \mid m$, so $m = p^\alpha m_1$, $(p, m_1) = 1$):

$$E[m] \overset{?}{=} E[m_1] \times E[p^\alpha] = \begin{cases} \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \{O_E\} \\ \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{p^\alpha\mathbb{Z}} \end{cases}.$$

Def: Let G be an abelian group. A function $d: G \to \mathbb{R}$ is called a quadratic form if:

(i) $d(g) = d(-g)$ $\forall g \in G$.

(ii) The pairing
$$G \times G \longrightarrow \mathbb{R}$$
$$(g, h) \longmapsto d(g+h) - d(g) - d(h)$$
is bilinear.

Also, a quadratic form d is called positive definite if:

(a) $d(g) \geq 0$ $\forall g \in G$.

(b) $d(g) = 0$ iff $g = 0$.

Cor: Let E_1, E_2 be two E.C.. Then, the degree map

$$\deg: \mathrm{Hom}(E_1, E_2) \longmapsto \mathbb{Z}$$

is a positive definite quadratic form.