Elliptic Curves (Basics)

Weierstrass Equations:

An E.C. "E" has an equation of the form:

$$E: y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

if $\underline{\text{char}(K) \neq 2}$ $\rightarrow$ $y \mapsto \frac{1}{2}(y - a_1x - a_3)$

$$E: y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \quad \begin{cases} b_2 = a_1^2 + 4a_2 \\ b_4 = 2a_4 + a_1a_3 \\ b_6 = a_3^2 + 4a_6 \end{cases}$$

if $\text{char}(K) \neq 2, 3$ $(x,y) \longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$

$$E: y^2 = x^3 - 27c_4 + 54c_6$$

$$\underline{c_4} := -b_2^3 + 36\, b_2b_4 - 216\, b_6$$

$\underline{\Delta}$ (disc), $\underline{j}$ (j-inv) $\longrightarrow$ $\underline{\text{if } E \simeq E' \Rightarrow j(E) = j(E')}$

Remark: $E \subset \mathbb{P}^2$

$E \cap$ line at ∞ = one point $\underline{[0,1,0]}$.

Prop.

If $\text{char}(K) \neq 2, 3 \Rightarrow E: y^2 = x^3 + Ax + B$

and $\begin{cases} \Delta = -16(4A^3 + 27B^2) \\ j = -1728\left(\frac{4A^3}{\Delta}\right) \end{cases}$

Prop.

(a) E is nonsingular iff $\Delta \neq 0$. $\rightarrow$ (E elliptic curve)

(b) E has a node if $\Delta = 0$ & $c_4 \neq 0$.

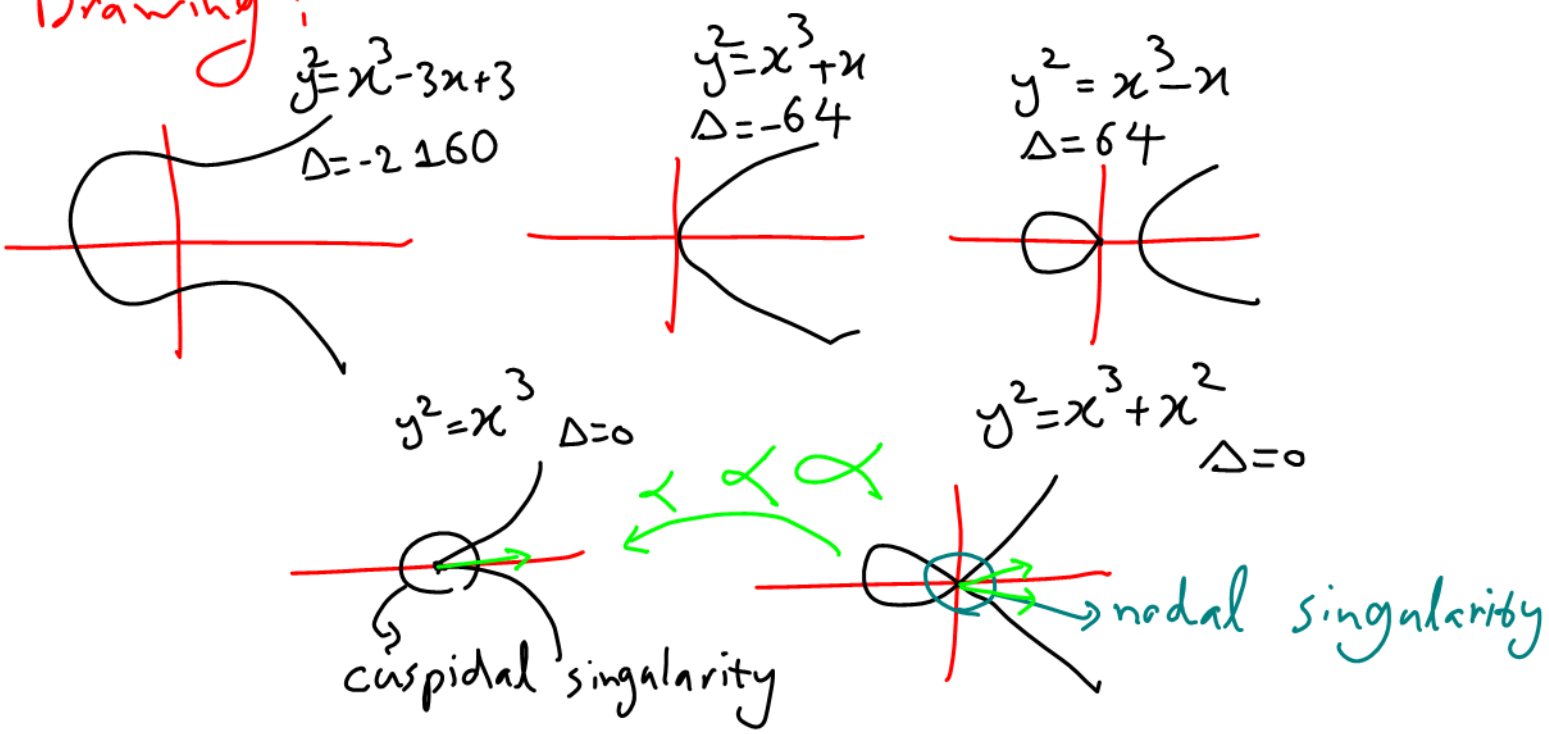
(c) E has a cusp if $\Delta = c_4 = 0$.

(d) if E, E' defined over an alg. closed field and $\Delta_E, \Delta_{E'} \neq 0$ (E, E' are E.C.) then, $E \simeq E'$ iff $j(E) = j(E')$

$$\left[\mathbb{Q} \rightarrow \mathbb{Q}\left(\sqrt[4]{\cdot}, \sqrt[6]{\cdot}\right) \rightarrow K\left(\sqrt[4]{\cdot}, \sqrt[6]{\cdot}\right) \cdots \right]$$

$$\left.\begin{aligned} y^2 &= x^3 + Ax + B \\ y'^2 &= x'^3 + A'x + B' \end{aligned}\right\} \rightarrow \begin{aligned} A &= u^4 A' \\ B &= u^6 B' \end{aligned}$$

Drawing:



[if $E: y^2 = f(x)$ where $f(x)$ has degree 3, then E has a nodal sing iff f has a double root, and E has a cuspidal sing iff f has a triple root. E has no sing iff f has distict roots]

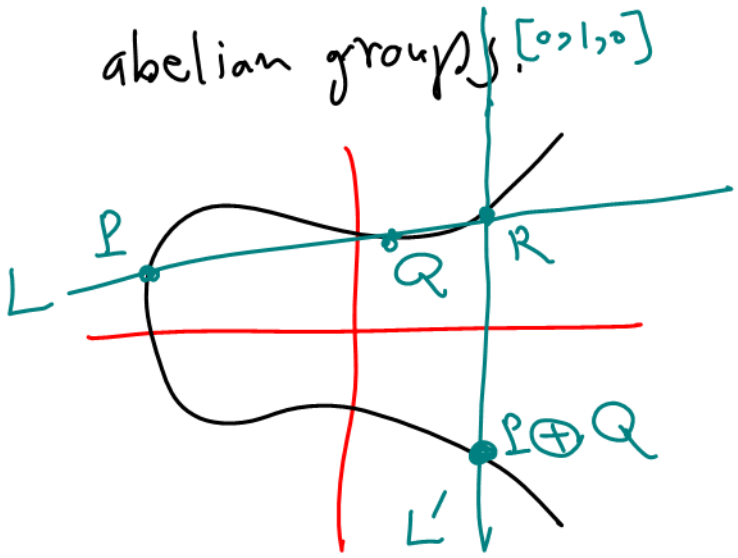
Prop. if E has a W.E. and $\Delta = 0$,

(a) for $K = \overline{K}$ $\begin{cases} E_{ns} := E \setminus \{\text{singular point}\} \simeq \overline{K}^{+} & \text{if } c_4 = 0 \text{ (cusp)} \\ E_{ns} \simeq \overline{K}^{\times} & \text{if } c_4 \neq 0 \text{ (node)} \end{cases}$

(b) for general K $\begin{cases} E_{ns} \simeq K^{+} & \text{if } c_4 = 0 \\ E_{ns} \simeq K^{\times} \text{ or } \ldots & \end{cases}$

Group Law:

E.C. are not only algebraic curve, but also abelian groups. $[0,1,0]$



$P \oplus Q = ?$

L: goes from P & Q

$L \cap E = \{P, Q, R\}$

L': goes from R to $[0,1,0]$

$L' \cap E = \{R, [0,1,0], P \oplus Q\}$

Theorem: The above drawing make E into an abelian group with identity $[0,1,0]$.

We write $P + Q$, for $P \oplus Q$.

Def: An E.C. is a pair $(E, \mathcal{O})$ where E is a nonsingular curve (dim 1) of genus one and $\mathcal{O} \in E$ (base point).

Theorem: Every Elliptic Curve has a W.E. and conversely every W.E. with $\Delta \neq 0$ gives an E.C.

$E \rightsquigarrow$ W.E of E is not unique.

Def: for a curve C, the divisor D is defined as follows: $D = \sum_{P \in C} n_P \cdot P$ (formal sum) where $n_P \in \mathbb{Z}$ and $n_P = 0$ for almost all P.

we can add $D = \sum n_P P$ & $D' = \sum m_P P$:

$$D + D' = \sum (n_P + m_P) P .$$

We denote the group of divisors on C by $\mathrm{Div}(C)$. We say that the divisor D has degree m if for $D = \sum n_P \cdot P$, $\sum n_P = m$

notation: we denote the subgroup of divisors on C

with degree zero by $\mathrm{Div}^0(C)$.

def: for $f \in K(C) = \mathrm{Frac}\left(\frac{K[X] = K[x_1, \dots, x_n]}{\langle \text{polynomials that} \rangle}\right)$ defined on C

we define $\mathrm{div}(f)$ as $\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) \cdot P$. (order of "vanishing")

def: We call a divisor D principal if comes from the function field of C, $K(C)$.

def: $(\text{Princ. div} = K(C))$

1) $\mathrm{Pic}(C) = \frac{\mathrm{Div}}{\text{Princ. div}(C)}$

2) $\mathrm{Pic}^0(C) = \frac{\mathrm{Div}^0(C)}{\text{Princ. div.}(C)}$

[Prop. Princ. div. $\subseteq \mathrm{Div}^0(C)$]

Th:

$$E \simeq \mathrm{Pic}^0(E)$$

$$P \xmapsto{g} [(P) - (O)]$$

and:

(doing base change)

$$0 \longrightarrow \bar{K}^\times \longrightarrow \bar{K}(E)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(E) \xrightarrow{g^{-1}} E \longrightarrow 1$$

(taking Galois invariant)

$$0 \longrightarrow K^\times \longrightarrow K(E)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(E(K)) \longrightarrow E(K) \longrightarrow 1$$