Curves of genus one

Lemma X ns proper genus one

1) $\omega_X \cong \mathcal{O}_X$
2) $\deg(\mathcal{L}) > 0 \Rightarrow h^0(\mathcal{L}) = \deg(\mathcal{L})$
3) $\deg(\mathcal{L}) = 1 \Rightarrow \exists q \in X(k) : \mathcal{L} \cong \mathcal{O}_X(q)$
4) $\deg(\mathcal{L}) \geq 2 \Rightarrow \mathcal{L}$ globally generated
5) $\deg(\mathcal{L}) \geq 3 \Rightarrow \mathcal{L}$ very ample.

Pf By Riemann-Roch:

$$\left.\begin{array}{l} \deg(\omega_X) = 0 \\ h^0(\omega_X) = 1 \end{array}\right\} \Rightarrow \omega_X \cong \mathcal{O}_X$$

2), 4), 5) immediate special cases e.g.

$$h^0(\mathcal{L}) = 1 - g + \deg(\mathcal{L})$$

3) $\deg(\mathcal{L}) = 1 = h^0(\mathcal{L})$

$\Rightarrow \mathcal{L} \cong \mathcal{O}_X(\mathrm{div}(s))$ $\quad s \in H^0(\mathcal{L}) \setminus \{0\}$

$\cong \mathcal{O}_X(q)$ $\quad \Rightarrow \mathrm{div}(s)$ effective degree one

$\square$

Cor X ns proper genus one curve $/k = \bar{k}$

$$\mathcal{O}_X(-) : X(k) \longrightarrow \mathrm{Pic}^1(X) \quad q \longmapsto \mathcal{O}_X(q)$$

Pf inj. by ex.sh. 4, surj. by lemma 3) $\square$.

Def An <u>elliptic curve</u> $/k$ is a ns proper genus one curve E w/ a k-point $e \in E(k)$

Prop Let (E, e) be an elliptic curve.

Then E is isomorphic to a cubic curve

$$y^2z + a_1xyz + a_3yz^2 = x^3 - a_2xz - a_4xz^2 - a_6z^3$$

where $a_i \in k$.

If $\mathrm{char}(k) \neq 2$, then E is isomorphic to a cubic of the form

$$y^2z = x^3 - a_2x^2z - a_4xz^2 - a_6z^3$$

If $\mathrm{char}(k) \neq 2, 3$, then E is isomorphic to a cubic of the form

$$y^2z = x^3 - a_4xz^2 - a_6z^3$$

The isomorphism can be chosen s.t. $e \mapsto [0:1:0]$

Proof We use embedding(s) given by the very ample line bundle $\mathcal{O}_E(3e)$:

$$i : E \hookrightarrow \mathbb{P}(H^0(\mathcal{O}_E(3e))) \cong \mathbb{P}^2$$

$$\begin{array}{cccccccccccc} & H^0(\mathcal{O}(e)) & \subseteq & H^0(\mathcal{O}(2e)) & \subseteq & H^0(\mathcal{O}(3e)) & \subseteq & H^0(\mathcal{O}(4e)) & \subseteq & H^0(\mathcal{O}(5e)) & \subseteq & H^0(\mathcal{O}(6e)) \\ & \| & & & & & & & & & & \\ H^0(\mathcal{O}) & 1 & & x & & y & & x^2 & & xy & & x^3, y^2 \end{array}$$

$$\Rightarrow \underbrace{H^0(\mathcal{O}(6e)) / H^0(\mathcal{O}(5e))}_{1\text{-dimensional.}} = \mathrm{span}\{[x^3], [y^2]\}$$

$\Rightarrow \exists\ u, v \in k^\times$, $a_1', a_2', a_3', a_4', a_6' \in k$ s.t.

$$vy^2 + a_1'xy + a_3'y = ux^3 - a_2'x^2 - a_4'x - a_6'$$

replace y by u^2vy and x by uvx:

$$u^4v^3y^2 + a_1''xy + a_3''y = u^4v^3x^3 - a_2''x^2 - a_4''x - a_6''$$

divide by $u^4 v^3$:

$$y^2 + a_1 xy + a_3 y = x^3 - a_2 x^2 - a_4 x - a_6$$

Specify $i : E \hookrightarrow \mathbb{P}^2$ by the line bundle with globally generating sections $(\mathcal{O}_E(3e), (x, y, 1))$ as chosen above.

$$E \subseteq \underbrace{\mathbb{V}(y^2 z + a_1 xyz + a_3 y z^2}_{\text{integral.}} - x^3 - a_2 x z^2 - a_4 x z^2 - a_6 z^3)$$

$$\Rightarrow E \cong \mathbb{V}(- \text{"} \text{———} \cdot)$$

If $\mathrm{char}(k) \neq 2$, can replace y by $y - \frac{1}{2}(a_1 x + a_3)$

$$(y^2 + a_1 xy + a_3 y) = (y + \tfrac{1}{2}(a_1 x + a_3))^2 - (\tfrac{1}{2}(a_1 x + a_3))^2$$

so that $y^2 = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6$

If $\mathrm{char}(k) \neq 2, 3$, can replace x by $x - \frac{1}{3}\tilde{a}_2$

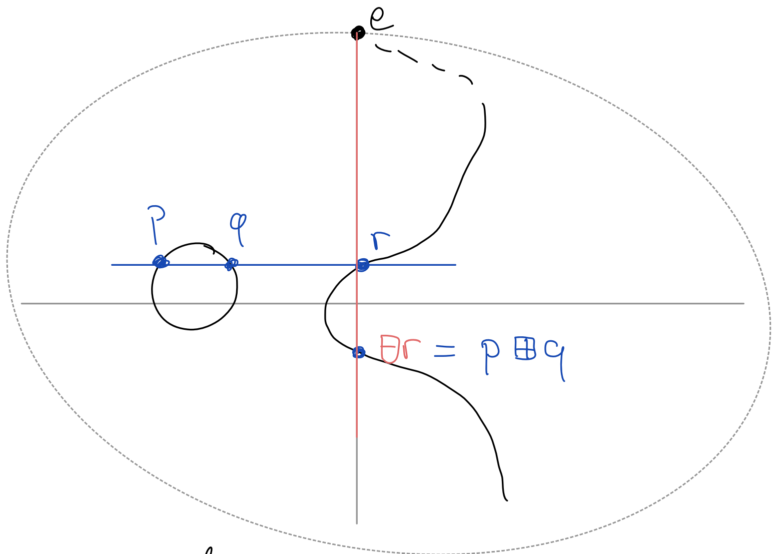
x has a pole of order 2 at e

y has a pole of order 3 at e

$$\Rightarrow [x(e) : y(e) : 1] = [\underbrace{\frac{x(e)}{y(e)}}_{=0} : 1 : \underbrace{\frac{1}{y(e)}}_{=0}] \qquad \square$$

<ins>Rmk</ins> $x \mapsto u^2 x$, $y \mapsto u^3 y$

then get new Weierstrass eqn w/ coefficients $u^{-i} a_i$



The group law:

Let (E, e) be an elliptic curve.

We have a canonical bijection

$$\begin{array}{ccccc} E(k) & \longrightarrow & \mathrm{Pic}^1(E) & \longrightarrow & \mathrm{Pic}^0(E) \\ q & \longmapsto & \mathcal{O}_X(q) & \longmapsto & \mathcal{O}_X(q-e) \\ & & \mathcal{L}(e) & \longleftarrow & \mathcal{L} \end{array}$$

which endows $E(k)$ with a group structure $(E(k), \boxplus, e)$

where $\boxplus : E(k) \times E(k) \to E(k)$ can be explicitly described by: $\forall p, q, r \in E(k)$

$p \boxplus q \boxplus r = 0 \iff \mathcal{O}(p+q+r) \cong \mathcal{O}(3e) = i^*\mathcal{O}(1)$

$\iff$ p, q, r are the intersection pts of a line $\ell \subset \mathbb{P}^2$ with E in its Weierstrass embedding.

Since intersection points can be described explicitly as rational functions in the coordinates, can upgrade E to a group variety. We give a more abstract app.

Jacobians

Def (degree 0 Picard functor)

X ns proper curve over $k = \bar{k}$

T scheme over k.

$$\mathrm{Pic}^0(X \times T) := \left\{ \mathcal{L} \in \mathrm{Pic}(X \times T) \;\middle|\; \begin{matrix} \forall t \in T \\ \mathcal{L}|_t \in \mathrm{Pic}^0(X_t) \end{matrix} \right\}$$

$$pr_T^*: \mathrm{Pic}(T) \longrightarrow \mathrm{Pic}^0(X \times T)$$

b/c $pr_T^* \mathcal{N}$ trivial on each fibre.

$$\mathrm{Pic}^0(X/T) := \mathrm{Pic}^0(X \times T) / pr_T^* \mathrm{Pic}(T)$$

$$\begin{aligned} \mathrm{Pic}^0_X : \mathrm{Sch}_k^{op} &\longrightarrow \mathrm{Sets} \\ T &\longmapsto \mathrm{Pic}^0(X/T) \\ f: T \to S &\longmapsto f^*: \mathrm{Pic}(X/S) \to \mathrm{Pic}(X/T) \end{aligned}$$

Is the <u>degree 0 Picard functor of</u> X

Def (Jacobian)

The Jacobian of a curve X is a scheme $\mathrm{Jac}(X)$ together with a "universal degree 0 line bundle $\mathcal{U} \in \mathrm{Pic}^0(X/\mathrm{Jac}(X))$ s.t. for any $T \in \mathrm{Sch}_k$, $\mathcal{L}_T \in \mathrm{Pic}^0(X/T)$ there is a unique morphism $f: T \to \mathrm{Jac}(X)$ s.t.

$$f^* \mathcal{U} = \mathcal{L}_T$$

<u>Rmk</u> $\mathrm{Jac}(X)$ is unique if it exists

<u>Theorem</u> X ns proj. curve $/k$.
then $\mathrm{Jac}(X)$ exists and is an abelian variety of dimension $g(X)$.

We will show existence and dimension only for X of genus one.

<u>Reason</u> that $\mathrm{Jac}(X)$ is a commutative group scheme:
Need to give a morphisms

$\mu: \mathrm{Jac}(X) \times \mathrm{Jac}(X) \longrightarrow \mathrm{Jac}(X)$

and $e: pt \longrightarrow \mathrm{Jac}(X)$

satisfying certain compatibility conditions.

for μ can take the morphism corresponding to the line bundle,

$pr_1^* \mathcal{U} \otimes pr_2^* \mathcal{U} \in \mathrm{Pic}^0_X(\mathrm{Jac}(X)^{\times 2})$

for e can take morphism corresponding to $\mathcal{O}_X \in \mathrm{Pic}^0_X(pt)$ $\square$

Definition of inverse?

Theorem Let (E,e) be an elliptic curve. Then E together with the line bundle

$$\mathcal{U}_E := \mathcal{O}_{E\times E}(\Delta) \otimes pr_1^* \mathcal{O}_E(-e) \in \mathrm{Pic}^0_E(E)$$

is the Jacobian variety for E.

Pf later (need cohomology and base change)
which is an extremely useful technical tool to know about. $\square$

Cor If X is a genus one curve, then $\mathrm{Aut}(X) \curvearrowright X$ is transitive.

Pf pick $e \in X(k)$ making X into a group scheme with identity $e \in X$.

$\forall x \in X(k)$
$$\varphi : X \longrightarrow X, \quad p \longmapsto xp$$
is an automorphism with $\varphi(e) = x$ $\square$

j-invariant

Suppose $\mathrm{char}(k) \neq 2$. (E, e) elliptic curve$/k$ with Weierstrass form $y^2 = x^3 + a_2 x^2 + a_4 x + a_6$

$$\begin{tikzcd} E \arrow[r, "\pi"] \arrow[dr] & \mathbb{P}(H^0(\mathcal{O}(2e))) \cong \mathbb{P}^1_{x,z} \\ & \mathbb{P}(H^0(\mathcal{O}(3e))) \cong \mathbb{P}^2_{x,y,z} \arrow[u, "\pi'"] \end{tikzcd}$$

hyperelliptic cover

Weierstrass form

$$\pi(e) = \pi'([x(e) : y(e) : 1])$$
$$= \pi'\left(\left[\frac{x(e)}{y(e)} : 1 : \frac{1}{y(e)}\right]\right)$$
$$= \left[\frac{x(e)}{y(e)} : \frac{1}{y(e)}\right] = [1:0] = \infty \in \mathbb{P}^1$$

vanishes to higher order

$\Rightarrow \pi$ ramified at ∞ and zeroes $(x;1)$ of

$$x^3 + a_2 x^2 + a_4 x + a_6 = (x-a)(x-b)(x-c)$$

$PGL(2) \curvearrowright \mathbb{P}^2$ is three transitive:

hidden choice of ordering

replace $x \mapsto \dfrac{x-a}{b-a}$: wlog $= x(x-1)(x-\lambda)$

$$\lambda = \frac{c-a}{b-a}$$

ic

Corollary If $\mathrm{char}(k) \neq 2$ every elliptic curve is isomorph to a cubic of the form $y^2 z = x(x-1)(x-\lambda)$

<u>Lemma</u> The elliptic curves

$E_\lambda \quad y^2 = x(x-1)(x-\lambda) \qquad \lambda \neq 0,1$

$E_{\lambda'} \quad y^2 = x(x-1)(x-\lambda') \qquad \lambda' \neq 0,1$

are isomorphic iff

$$\lambda' \in \left\{ \lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda} \right\} = S_3 \cdot \lambda$$

<u>Pf</u> If $E_\lambda \cong E_{\lambda'}$, then $\lambda' = \dfrac{c-a}{b-a}$ where $a,b,c \in \{0,1,\lambda\}$, since they must be in the same liner system.

Similarly if $\lambda' = \dfrac{c-a}{b-a}$ for $a,b,c \in \{0,1,\lambda\}$ then the substitution yields an iso $\square$

<u>Def</u> (j-invariant)

$$j(\lambda) := 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2}$$

Key point:

<u>Prop</u>: (1) Two elliptic curves are isomorphic iff their j-invariants are the same.

(2) For any $j \in k$ there is an elliptic curve with j-invariant $= j$

Proof (1) follows from

$$j(\lambda) = j(\lambda') \text{ iff } \lambda' \in S_3 . \lambda$$

(2) solve equation

$$j = \frac{2^8 (\lambda^2 - \lambda + 1)}{\lambda^2 (\lambda - 1)^2}$$

for λ.

$$\Rightarrow j(E_\lambda) = j$$

□.

The involution $[x:y:z] \longmapsto [x:-y:z]$ restricts to E and commutes with π

$$\begin{tikzcd} E \arrow[rr, "\sigma"] \arrow[dr] & & E \arrow[dl] \\ & \mathbb{P}^1 & \end{tikzcd}$$

"hyperelliptic involution" corresponding to the non-trivial element of the Galois extension $K(E)/K(\mathbb{P}^1)$

Lemma Let X be a genus one curve $\pi_1, \pi_2 : X \to \mathbb{P}^1$ deg. 2 map. Then there are automorphism $\varphi \in \mathrm{Aut}(X)$, $\tau \in \mathbb{P}^1$ s.t.

$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[d, "\pi_1"'] & X \arrow[d, "\pi_2"] \\ \mathbb{P}^1 \arrow[r, "\tau"] & \mathbb{P}^1 \end{tikzcd}$$

commutes.

Pf let $p_1 \in Ram(\pi_1)$, $p_2 \in Ram(\pi_2)$

choose $\varphi \in Aut(X)$ s.t. $\varphi(p_1) = p_2$

Then both $\pi_2 \circ \varphi$ and π_1

are ramified at p_1 and correspond

to map given by $\mathcal{O}_X(2p_1)$ $\square$.

Prop (E, e) elliptic curve

$Aut(E, e)$ finite of order.

2 if $j(E) \neq 0, 1728$

4 if $j = 1728$ $char(k) \neq 3$

6 if $j = 0$ $char(k) \neq 3$

12 if $j = 0 (= 1728)$ $char(k) = 3$

Pf $E = E_\lambda \xrightarrow{\pi} \mathbb{P}^1$

lemma $\Rightarrow$ For any $\varphi \in Aut(E, e)$ $\exists \tau \in Aut(\mathbb{P}^1)$

s.t. $\pi \circ \varphi = \tau \circ \pi$

and τ permutes $\{0, 1, \lambda\}$

$\Rightarrow |Aut(E, e)| \leq |Aut(\pi)| \, |S_3| = 12$

if $\tau = id$ $\Rightarrow$ $\varphi = \sigma$ or id.

if $\tau \neq id$ $\Rightarrow$ $\lambda \in \{\frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\}$

rest is

"Elementary argument" $\square$

"moduli of elliptic curves is DM"