Prop $E := \{[x:y:z] \mid y^2 z = x^3 + a_4 x z^2 + a_6 z^3\}$ is an elliptic curve if and only if

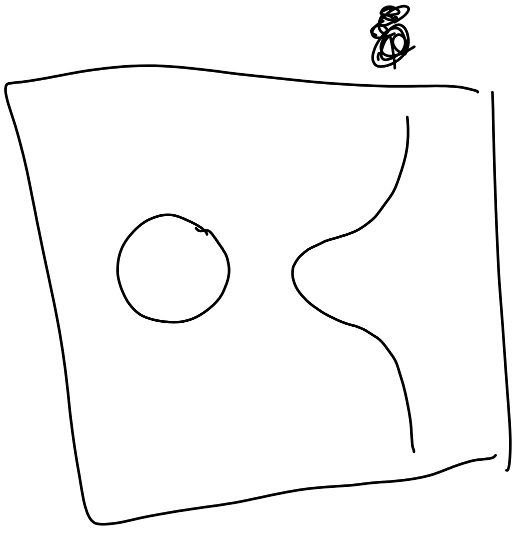
$f(x,z) := x^3 + a_4 x z^2 + a_6 z^3$ has no double root in $\mathbb{P}^1(\overline{K})$. ($\Leftrightarrow$ f is squarefree)

Pf Problem 1b on problem set 2 shows that

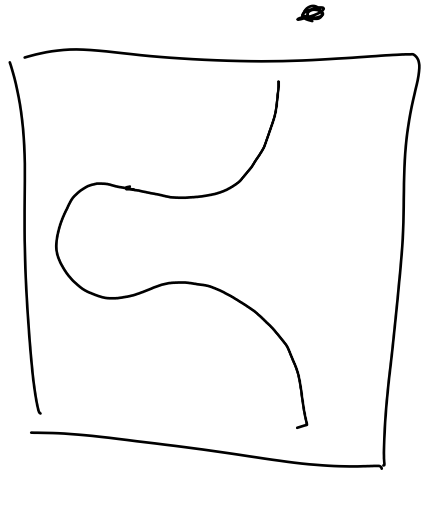
$E \cap \{[x:y:z] \mid z \neq 0\}$ is smooth if and only if $f(x,z)$ has no double root. E is automatically smooth at $[0:1:0] \in E$.

By problem 1c on problem set 4, the genus is then $g_E = \frac{1}{2}(3-1)(3-2) = 1$. $\square$

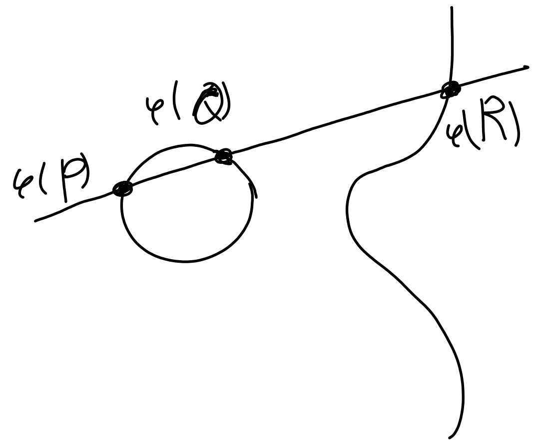
Prop Let E be an elliptic curve over $\mathbb{R}$. Then, $\{[x:y:1] \in \varphi(E(\mathbb{R}))\} \subset \mathbb{R}^2$ "looks like this":

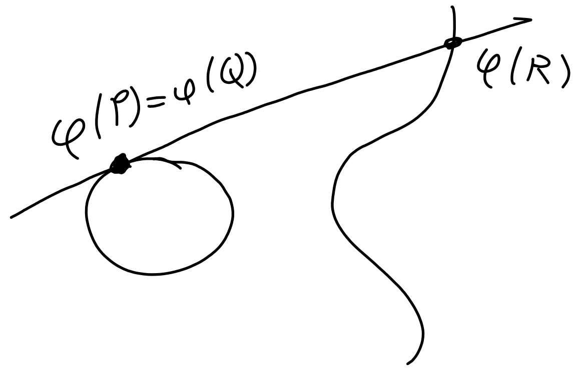


or



Thm Let $P, Q, R \in E(K)$. Then, $P+Q+R=0$ if and only if $\varphi(P), \varphi(Q), \varphi(R) \in \mathbb{P}^2_K$ are the three points of intersection of $\varphi(E)$ with a line $l \subset \mathbb{P}^2_K$ with multiplicities.





Pf $P+Q+R=0$

$\iff [P]-[O]+[Q]-[O]+[R]-[O]=0$ in $\mathrm{Cl}(E)$

$\iff \exists f \in K(E)^\times : \operatorname{div}(f)=[P]+[Q]+[R]-3[O]$.

"$\Leftarrow$" Say $\varphi(P), \varphi(Q), \varphi(R)$ are the intersections of E with l. Let $a(X,Y,Z)$ be the linear polynomial defining l.

Let $f=\varphi^*\left(\dfrac{a(X,Y,Z)}{Z}\right)$. Then,

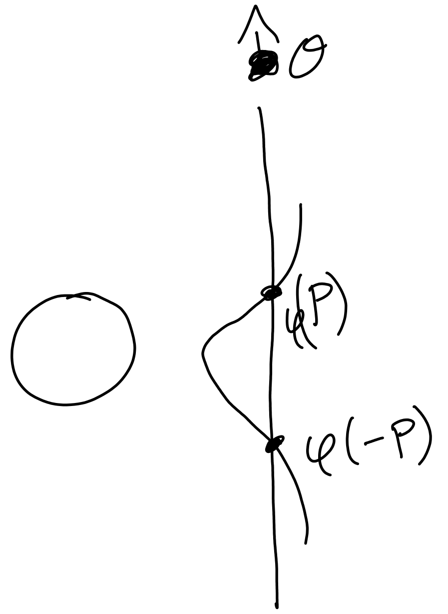
$\operatorname{div}(f)=[P]+[Q]+[R]-3[O]$
because $\varphi(O)$ is the only point of intersection of $\varphi(E)$ with $\{Z=0\}$ (with multiplicity 3).

"$\Rightarrow$" For any $P, Q \in E(K)$, there is exactly one line intersecting $\varphi(E)$ in $\varphi(P)$ and $\varphi(Q)$ with multiplicity. By Bézout, it intersects $\varphi(E)$ in exactly one more point $\varphi(R')$, which by "$\Leftarrow$" is the point satisfying $P+Q+R'=O$.

$\square$

Cor If $\varphi(P) = [x:y:z]$, then $\varphi(-P) = [x:-y:z]$.

Pf



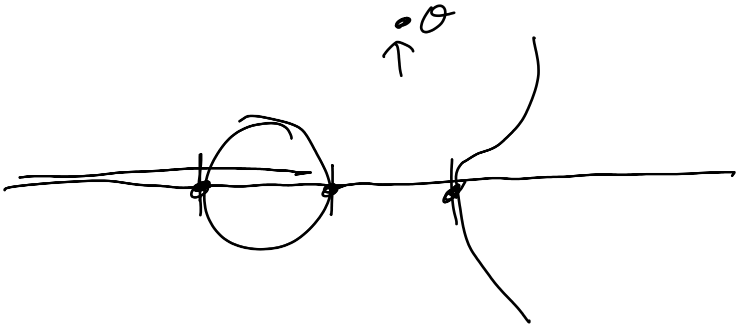
The "vertical" line through $\varphi(P)$ intersects $\varphi(E)$ in $[x:y:z], [x:-y:z], \underbrace{[0:1:0]}_{=\varphi(O)}$.

$\square$

Cor $2P = O$

$\Leftrightarrow y = 0$ or $P = O$

$\Leftrightarrow$ The morphism $y: E \to \mathbb{P}^1$ is ramified at P.

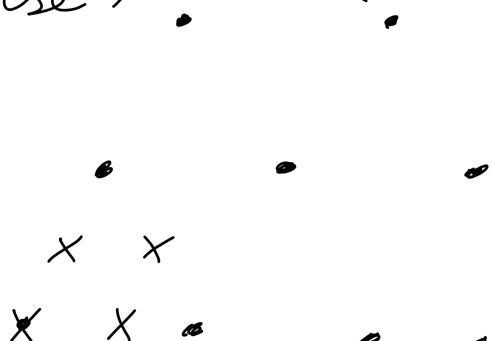


Rmk There are exactly four (distinct) points $P \in E(\overline{K})$ with $2P = O$.

Pf 1 They are $P = O$ and $P = [x : 0 : z]$, where $[x : z]$ is one of the roots of

$$f(x, z) = X^3 + a_4 X Z^2 + a_6 Z^3.$$ $\square$

Pf 2 Use that $E(\mathbb{C}) = \mathbb{C}/\Lambda$ if $K \subseteq \mathbb{C}$. Even if $K \not\subseteq \mathbb{C}$, we can assume that $K \subseteq \mathbb{C}$ by the Lefschetz principle:



Basically, show that we can assume that the field ext. $K | \mathbb{Q}$ is generated by finitely many elements. Then there is an embedding $K \hookrightarrow \mathbb{C}$ because $\mathbb{C}$ has infinite transcendence degree over $\mathbb{Q}$!

Pf 3 Riemann-Hurwitz for $\psi : E \longrightarrow \mathbb{P}^1$

$$\Rightarrow \underbrace{2g_E - 2}_{0} = \underbrace{\deg(\psi)}_{2} \cdot \underbrace{(2g_{\mathbb{P}^1} - 2)}_{-2} + \deg(R_\psi)$$

$$\Rightarrow \deg(R_\psi) = 4$$

Since $\deg(\psi) = 2$, every point has ramification index 1 or 2, so there are exactly 4 points of ramification. $\square$

Thm The maps $+ : E \times E \longrightarrow E$
$$(P, Q) \longmapsto P+Q$$

and $- : E \longrightarrow E$ are morphisms (defined over K).
$$P \longmapsto -P$$

(Cover $E \times E$ by open affine varieties U_i. Then, the restrictions $+ : U_i \longrightarrow E$ are morphisms.)

Ese Let $E = \{[x:y:z] \mid y^2 z = x^3 + a_4 x z^2 + a_6 z^3\}$, $P_1 = [x_1 : y_1 : 1]$, $P_2 = [x_2 : y_2 : 1]$.

If $P_1 \neq \pm P_2$, then $P_1 + P_2 = [x_3 : y_3 : 1]$, where
$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = \dots$$

If $P = [x : y : 1]$, $y \neq 0$, then $2P = [x' : y' : 1]$, where
$$x_3 = \frac{x^4 - 2a_4 x^2 - 8 a_6 x + a_4^2}{4x^3 + 4a_4 x + 4a_6}$$

$$y_3 = \dots$$

2.2. Isogenies

Def An *isogeny* between elliptic curves E_1, E_2 is a morphism $\phi: E_1 \longrightarrow E_2$ sending $O \in E_1$ to $O \in E_2$.

We denote the group of isogenies $\phi: E_1 \to E_2$ by $\mathrm{Hom}(E_1, E_2)$ (where $(\phi_1+\phi_2)(P) = \phi_1(P)+\phi_2(P)$).

Ex The trivial (= constant) isogeny $\phi = 0$:

$$\phi(P) = O \quad \forall P \in E_1(\bar{k})$$

Ex The multiplication by $m \in \mathbb{Z}$ isogeny

$$[m]: E \longrightarrow E$$
$$P \longmapsto mP$$

(It's a morphism because $+: E \times E \to E$ and $-: E \to E$ are.)

Rmk We get a commutative diagram

$$\begin{tikzcd}
P \in E_1 \arrow[r, "\phi"] \arrow[d, leftrightarrow] & E_2 \ni \phi(P) \arrow[d, leftrightarrow] \\
{[P]-[O]} \in \mathrm{Cl}^0(E_1) \arrow[r, "\phi"'] & \mathrm{Cl}^0(E_2) \ni [\phi(P)]-[O]
\end{tikzcd}$$

<u>Cor</u> Any isogeny is a group homomorphism.

<u>Rmk</u> Any isogeny $\phi \neq 0$ is unramified.

In other words: Any $Q \in E_2(\overline{K})$ has exactly $\deg(\phi)$ preimages in $E_1(\overline{K})$.

In particular: $|\ker(\phi)(\overline{K})| = \deg(\phi)$.

<u>Pf 1</u> Riemann-Hurwitz:

$$\underbrace{2g_{E_1}-2}_{0} = \deg(\phi)\cdot(\underbrace{2g_{E_2}-2}_{0}) + \deg(R_f)$$

$$\Rightarrow \deg(R_f) = 0 \qquad \square$$

<u>Pf 2</u> The preimage of $Q \in E_2(\overline{K})$ under the surjective group hom. $\phi : E_1(\overline{K}) \to E_2(\overline{K})$ is a coset of $\ker(\phi)(\overline{K})$.

$\Rightarrow$ All preimages have the same size.

$\Rightarrow$ Since ϕ can only be ramified at finitely many points, it's unramified everywhere.

$\square$

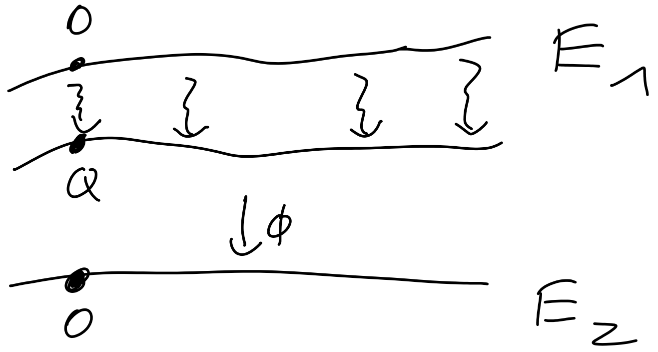
Lemma If $\phi : E_1 \to E_2$ is a nontrivial isogeny, then the map $\phi^* : K(E_2) \hookrightarrow K(E_1)$ makes $K(E_1)$ a **Galois** extension of $\phi^*(K(E_2))$.

We have a group isomorphism

$$\ker(\phi)(\bar{K}) \xrightarrow{\sim} \mathrm{Gal}(K(E_1) \mid \phi^*(K(E_2)))$$

$$Q \longmapsto \tau_Q^*$$

where $\tau_Q : E_1 \to E_1$ and $\tau_Q^* : K(E_1) \to K(E_1)$.
$P \mapsto P+Q$



Pf well-defined: We have

$$\phi(\tau_Q(P)) = \phi(P+Q) = \phi(P) \quad \forall P \in E_1(\bar{K}), \text{ so } \phi \circ \tau_Q = \phi.$$

$$\Rightarrow \tau_Q^* \circ \phi^* = \phi^*.$$

Hence, $\tau_Q^*(x) = x \quad \forall x \in \phi^*(K(E_1))$.

$$\Rightarrow \tau_Q^* \in \mathrm{Gal}(K(E_1) \mid \phi^*(K(E_2))).$$

group hom: clear

injective: τ_Q^* determines τ_Q and therefore
$$Q = \tau_Q(O)$$

Gal. ext. + surjective: $[K(E_1):\phi^*(K(E_2))] = \deg(\phi) = |\ker(\phi)(\overline{K})|$.

$\square$

Lemma If $\alpha : E_1 \to E_3$, $\beta : E_1 \to E_2$ are isogenies, there is an isogeny $\gamma : E_2 \to E_3$ with $\alpha = \gamma \circ \beta$ if and only if
$$\ker(\alpha)(\overline{K}) \supseteq \ker(\beta)(\overline{K})$$

$$\begin{tikzcd} E_1 \arrow[r, "\alpha"] \arrow[d, "\beta"'] & E_3 \\ E_2 \arrow[ur, dashed, "\gamma"'] & \end{tikzcd}$$

Rmk If $\beta \neq 0$, then $\beta : E_1(\overline{K}) \to E_2(\overline{K})$ is surjective, so γ is unique.

Pf of Lemma

Assume $\alpha, \beta \neq 0$. There is a (unique) group homomorphism $\gamma : E_2(\bar{K}) \longrightarrow E_3(\bar{K})$ satisfying $\alpha = \gamma \circ \beta$. We need to show that it is a morphism.

$$\begin{tikzcd}
K(E_1) & & K(E_3) \arrow[ll, "\alpha^*"'] \arrow[dl, dashed, "\gamma^*"] \\
& K(E_2) \arrow[ul, bend left, "\beta^*"] &
\end{tikzcd}$$

$\ker(\alpha) \supseteq \ker(\beta)$ implies that

$\mathrm{Gal}(K(E_1)/\alpha^*(K(E_3))) \supseteq \mathrm{Gal}(K(E_1)/\beta^*(K(E_2)))$

$\Rightarrow \alpha^*(K(E_3)) \subseteq \beta^*(K(E_2))$

$\Rightarrow$ There is a field homomorphism $\bar{\gamma}^* : K(E_3) \hookrightarrow K(E_2)$ with $\alpha^* = \beta^* \circ \bar{\gamma}^*$.

Let $\bar{\gamma} : E_2 \dashrightarrow E_3$ be the corresponding rational map. Since $\alpha^* = \beta^* \circ \bar{\gamma}^*$, we have $\alpha = \bar{\gamma} \circ \beta$ on some nonempty open subset of $E_1(\bar{K})$. Then, $\bar{\gamma} = \gamma$ on some nonempty open subset U of $E_2(\bar{K})$ where $\bar{\gamma}$ is defined. Let $P \in U$ and consider any $Q \in E_2(\bar{K})$. Then,

$$\begin{aligned}
\gamma(R) &= \gamma(R - Q + P) + \gamma(Q - P) \\
&= \bar{\gamma}(R - Q + P) + \gamma(Q - P)
\end{aligned}$$

for any $R \in U + Q - P$.

But then

$$\bar{\bar{\gamma}} : E_2 \dashrightarrow E_3$$
$$R \longmapsto \bar{\gamma}(R-Q+P) + \gamma(Q-P)$$

is a rational function which

a) is defined at every point in the open neighborhood $U+Q-P$ of Q, and

b) agrees with γ, and therefore with $\bar{\gamma}$, wherever both $\bar{\gamma}$ and $\bar{\bar{\gamma}}$ are defined, so in fact $\bar{\gamma} = \bar{\bar{\gamma}}$.

(some nonempty open subset of E_2)

$\Rightarrow \bar{\gamma}$ is defined everywhere.

$\square$

<u>Note</u> Any rational map $C \dashrightarrow \mathbb{P}^n$ for a <u>smooth</u> curve C is a morphism!

(so the last part of the proof is unnecessary in this case. But it generalises nicely to higher-dimensional abelian varieties).