Recall: E an elliptic curve over k. There is a group law on $E(k)$

$$\begin{array}{ccc} E(k) & \longrightarrow & \mathrm{Pic}^0(E) \\ x & \longmapsto & [x]-[e] \end{array}$$

Cor: The group law does not depend on the chosen embedding. If $\bar{k}$ is an algebraic closure, then we have a commutative diagram

$$\begin{array}{ccc} E(k) & \longrightarrow & \mathrm{Pic}^0(E) \\ \downarrow & & \downarrow \\ \bar{E}(\bar{k}) & \longrightarrow & \mathrm{Pic}^0(\bar{E}) \end{array} \qquad \bar{E} = E \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, \bar{k}$$

where $\bar{E}$ is the elliptic curve obtained by extending scalars to $\bar{k}$, i.e. the one with function field $K(E) \otimes_k \bar{k}$.

It is easier to understand the group law when $E \subseteq \mathbb{P}^2$ and e is a flex. It is always possible to this by taking the embedding

$$i_{3[e]} : E \hookrightarrow \mathbb{P}(H^0(3[e])^*) \simeq \mathbb{P}^2$$

$$i_{3[e]}(e) = [0:0:1] \quad \text{is a flex.}$$

Prop: The group law comes from a morphism of algebraic varieties

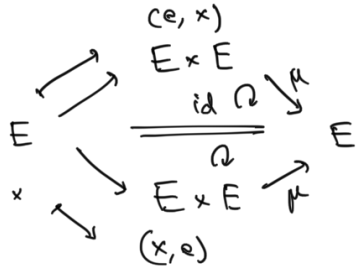
$$\mu : E \times_k E \longrightarrow E$$

together with a morphism $i : E \to E$ satisfying the following properties:

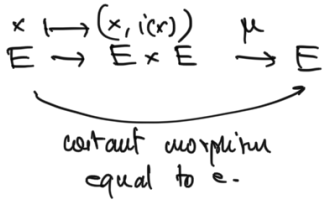
$$\begin{array}{ccc} E \times_k E \times_k E & \xrightarrow{\mathrm{pr}_1 \times \mu} & E \times_k E \\ {\scriptstyle \mu \times \mathrm{pr}_3}\downarrow & \circlearrowright & \downarrow{\scriptstyle \mu} \\ E \times_k E & \xrightarrow{\mu} & E \end{array} \qquad \begin{array}{ccc} (x,y,z) & \mapsto & (x, \mu(y,z)) \\ \downarrow & & \downarrow \\ (\mu(x,y), z) & \mapsto & \mu(\mu(x,y), z) \end{array} \qquad \begin{array}{c} \downarrow \\ \mu(x, \mu(y,z)) \\ \| \\ \downarrow \end{array}$$

(associativity)

(neutral element)

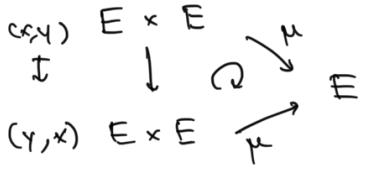


(inverse)



Rmk: This defines a group

(commutative)



Rmk: [illegible] a group object in the category of alg. varieties

The functor $S \mapsto \mathrm{Hom}_{k\text{-alg.var}}(S, E)$ is a functor in commutative groups.

Proof: It suffices to show that the group law is algebraic.

Therefore we may assume that E has equation

$$y^2 = F(x) \quad \text{with } F(x) \in k[x] \text{ of deg } 3$$

$\boxed{\mathrm{char}(k) \neq 2,3}$ (k)

For $p \in E \setminus \{\underbrace{[0:0:1]}_{e}\}$ write $p = (x_p, y_p)$

For $p, q \in E \setminus \{e\}$ the line passing through p, q has equation

$$(y_q - y_p)(x - x_p) + (x_q - x_p)(y - y_q) = 0.$$

Suppose $x_p \neq x_q$ (i.e. the line is not vertical). Ex: cover this case!

$$(y - y_p + y_p)^2 = F(p) + (x - x_p) F'(p) + \frac{(x-x_p)^2}{2} F''(p)$$

$$(y-y_p)^2 + 2(y-y_p)y_p + y_p^2 \qquad + \frac{(x-x_p)^3}{6} F'''(p)$$

Since p is a solution of this equation there are no constant terms.

Plug-in $\quad y - y_p = \underbrace{\frac{y_q - y_p}{x_q - x_p}}_{\mu} (x - x_p)$

$$\mu^2 (x-x_p)^2 + 2 y_p \mu (x-x_p) = (x-x_p) F'(p) + (x-x_p)^2 \frac{F''(p)}{2} + (x-x_p)^3 \frac{F'''(p)}{6}$$

We are not interested in the solution $x = x_p$, so we divide by it:

$$G(x) = \mu^2 (x-x_p) + 2 y_p \cdot \mu - \left(F'(p) + (x-x_p) \frac{F''(p)}{2} + (x-x_p)^2 \frac{F'''(p)}{6} \right)$$

We know that this polynomial has solution for $x = x_q$.

$$G(x) = \underbrace{G(x_q)}_{0} + G'(x_q)(x-x_q) + \frac{G''(x_q)}{2} (x-x_q)^2$$

$$G'(x) = \mu^2 - \left(\frac{F''(p)}{2} + 2 (x-x_p) \frac{F'''(p)}{6} \right) = \mu^2 - \frac{F''(p)}{2} - (x-x_p) \frac{F'''(p)}{3}$$

$$G''(x) = -\frac{F'''(p)}{3}$$

$$\frac{G(x)}{x-x_q} = G'(x_q) + \frac{G''(x_q)}{2} (x-x_q). \quad = 0.$$

$x - x_q$

$$\Longrightarrow \quad x - x_q = - \frac{G'(x_q)}{G''(x_q)/2}$$

$$= + \frac{\mu^2 - \frac{F''(p)}{2} - (x_q - x_p)\cdot\frac{F'''(p)}{8}}{+\frac{F'''(p)}{6}} \overset{(*)}{=}$$

For simplicity, assume $F(x) = x^3 + ax + b$.

$$F'(x) = 3x^2 + a \qquad F''(x) = 6x \qquad F'''(x) = 6.$$

$$\overset{(*)}{=} \frac{\mu^2 - \frac{6x_p}{2} - (x_q - x_p)\frac{6}{3}}{1} = \mu^2 - 3x_p - 2x_q + 2x_p$$

$$= \mu^2 - x_p - 2x_q.$$

$$\Longrightarrow \quad x = \mu^2 - x_p - x_q$$

In the end, the point $p+q$ has coordinates:

$$\left(\mu^2 - (x_p + x_q),\ -\left[y_p + \mu\left[\mu^2 - 2x_p - x_q\right]\right]\right)$$

Since $\mu = \frac{y_q - y_p}{x_q - x_p}$ we see that the group law is a polynomial expression in (x_p, y_p) and (x_q, y_q).

Moreover, the inverse is given by $(x_p, y_p) \mapsto (x_p, -y_p)$. □

MORPHISMS OF ELLIPTIC CURVES

Inseparable morphisms & Frobenius twists.

Let $\pi: C' \to C$ be a non constant morphism between smooth projective curves over a perfect field k:

$$\begin{array}{ccccc} C' & & K' = K(C') & \xleftarrow{\text{purely inseparable}} & \\ \pi\downarrow & & \uparrow & & K(C)^{sep} = K^{sep} \\ C & & K = K(C) & \xrightarrow{\text{separable}} & \text{separable closure} \end{array}$$

$$\deg(\pi) := [K' : K] = \underbrace{[K' : K^{sep}]}_{\deg_i(\pi)} \underbrace{[K^{sep} : K]}_{\deg_s(\pi)}$$

Lemma: Let K'/K be a purely inseparable extension of function fields of curve of degree q. (Here $\mathrm{char}(k) = p > 0$ and q is a power of p).

Then $K = K'^q$.

Proof: ($\geq$) Every element of K' satisfies an equation of the form $X^{q'} - \alpha$ with $\alpha \in K$ and $q' \mid q$. Therefore,

$$K'^q \subseteq K.$$

($\leq$) It suffices to show $[K' : K'^q] = q$. Pick $v \in C_{K'}$ and a uniformizer t at v.

We know that $K'/k(t)$ is separable (because dt generates $\Omega_{C_{K'}/k}$).

$\Rightarrow$ K' is an extension of $K'^q k(t)$ which is at the same time separable & purely inseparable

$\Rightarrow$ $K' = K'^q k(t)$.

It follows that $[K' : K]$ is the degree of the minimal polynom of t over K'^q, that is the smallest power q' of q s.t. $q' \mid q$ and $t^{q'} \in K'^q$. Since t is a uniformizer

$$v(t^{q'}) = q'$$

while for every element $f \in K'^q$, q divides $v(f)$. Therefore if q' as above is s.t. $t^{q'} \in K'^q$, then $q = q'$. □

Cor: Suppose π is purely inseparable ($\deg(\pi) = \deg_i(\pi)$). Then $g(C) = g(C')$ and π is a homeomorphism.

Pf: Identify $K(C)$ of $K(C')^q$. In order to show that π is a homeomorphism, it suffices to show that it is injective. For $v \in C'$ $\alpha \in K(C')$, then $\alpha^q \in K(C) = K(C')^q$ and

$$v(\alpha) = \frac{1}{q} v(\alpha^q)$$

Thus v is completely determined by $\alpha \mapsto v(\alpha^q)$. ($\in v|_{K^q}$).

I want to show that $h^0(K_C) = h^0(K_{C'})$. Since π is inseparable

$$\Omega_{K(C)/k} \otimes_{K(C)} K(C') \longrightarrow \Omega_{K(C')/k}$$

is the zero map. On the other hand

$$\begin{array}{ccc} K(C') & \longrightarrow & K(C')^q = K(C) \\ f & \longmapsto & f^q \end{array}$$

is an isomorphism, which lifts to an isomorphism

$$K(C')^q \otimes_{K(C')} \Omega_{K(C')/k} \longrightarrow \Omega_{K(C')^q/k} = \Omega_{K(C')/k}.$$

$$1 \otimes \omega \longmapsto \omega^{(q)}$$

We can see that, for each $x \in C'$, we have the equality

$$\mathrm{ord}_x(\omega) = \mathrm{ord}_{\pi(x)}\left(\omega^{(q)}\right).$$

[Indeed, $\mathcal{O}_{C,\pi(x)} = [\mathcal{O}_{C',x}]^q$ so that we have an isomorphism

$$\mathcal{O}_{C',x} \longrightarrow \mathcal{O}_{C,\pi(x)} \quad \text{which leads to an iso}$$
$$f \longmapsto f^q$$

$$\mathcal{O}_{C,\pi(x)} \otimes \Omega_{C',x} \xrightarrow{\sim} \Omega_{C,x}$$
$$1 \otimes \omega \longmapsto \omega^{(q)}$$

In particular, the map $\omega \mapsto \omega^{(q)}$ induces an isomorphism

$$H^0(\Omega_{C'}) \longrightarrow H^0(\Omega_C)$$
$$\omega \longmapsto \omega^{(q)}$$

$$\Longrightarrow \quad h^0(\Omega_{C'}) = h^0(\Omega_C). \qquad \square$$

Def: Let C be a smooth projective curve of a perfect field of $\mathrm{char}_{C^{(q)}} p > 0$. Let q be a power of p. The q-th Frobenius twist of C is the smooth projective curve with function field $K($ It is endowed with a purely inseparable morphism of degree q.

$$F_q : C \longrightarrow C^{(q)}$$

Properties: 1) F_q is a homeomorphism and $g(C^{(q)}) = g(C)$.

2) $\pi : C' \to C$ non constant morphism, $q = \deg_i(\pi)$, then π factors as follows

separable

$$C' \xrightarrow{F_q} C'^{(q)} \xrightarrow{\tilde{\pi}} C$$
$$\pi$$

3) $\left(C^{(q)}\right)^{(q')} = C^{(qq')}$.

Morphisms & isogenies: k = perfect field

Lemma: Let (E,e) and (E',e') be elliptic curves over k. Let $\pi : E' \to E$ be a morphism.

1) π is non constant $\Longrightarrow$ $\mathrm{ord}_x(\pi) = \deg_i(\pi)$ for all $x \in E$;

2) $\pi(e) = e'$ $\Longrightarrow$ π is a group morphism.

<u>Proof:</u> 1) π factors as

$$E' \longrightarrow \underset{\text{elliptic curve}}{E'^{(q)}} \xrightarrow{\text{separable}} E$$

It suffices to show that $\mathrm{ord}_x(\pi) = 1$ if π is separable.

We can apply the Hurwitz formula:

$$0 = 0 \cdot \deg \pi + \deg(R_\pi) \Rightarrow \deg(R_\pi) = 0$$

But $R_\pi \geq 0$ by definition, so $R_\pi = 0$.

2) It suffices to prove it for $k = \bar{k}$. Look at the following diagram:

$$\begin{array}{ccccc}
x' & E'(\bar{k}) & \longrightarrow & \mathrm{Pic}^0(E') & [x'] - [e'] \\
\downarrow & \downarrow \varphi & \circlearrowright & \downarrow & \downarrow \\
\varphi(x') & E(\bar{k}) & \longrightarrow & \mathrm{Pic}^0(E) & [\varphi(x')] - [\varphi(e')] \\
 & x & \longmapsto & [x] - [e] & \varphi(e') = e
\end{array}$$

(top arrow: $x' \longmapsto [x'] - [e']$)

This implies that φ is a group morphism. $\square$

<u>Def:</u> Let E, E' be elliptic curves. A morphism of elliptic curves is a morphism of alg. varieties $f: E' \to E$ s.t. $f(0_{E'}) = 0_E$.

A morphism of elliptic curves is an isogeny if it is non constant.

<u>Multiplication by m:</u> Let $m \in \mathbb{N} \setminus \{0\}$. We want to define the map

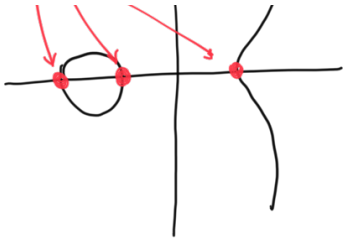
$$[m] : E \longrightarrow E$$
$$x \longmapsto \text{"}mx\text{"}$$

Consider the m-fold product

$$E \xrightarrow{\text{diagonal}} \underbrace{E \times \cdots \times E}_{m\text{-copies}} \xrightarrow{\overbrace{\mu \times \cdots \times \mu}^{m-1 \text{ times}}} E$$

$$x \longmapsto (x, \dots, x) \longmapsto \underbrace{x + \cdots + x}_{m \text{ times}}.$$

This is a morphism of elliptic curves. It is non constant: Suppose for the moment $\mathrm{char}(k) \neq 2$. It suffices to show it when k is algebraically closed. Let $x \in E(k)$ with a point with order 2.



If $2 \nmid m$, then $[m](x) = x$ while $[m](e) = e$ so $[m]$ is non-const

Since $[mn] = [m] \cdot [n]$, it suffices to show that $[2]$ is non constant. Take $f \in H^0(2[e])$

$$E \xrightarrow{f} \mathbb{P}^1$$

The points of 2-torsion are exactly the ramification points:

if $f(x) = f(x') \neq \infty$ and $x \neq x'$, then

$$\operatorname{div}(f-a) = [x] + [x'] - 2[e] = \big([x]-[e]\big) + \big([x']-[e]\big)$$

$$\Longrightarrow \quad x + x' = 0 \quad \text{in } E.$$

Since $\operatorname{char}(k) \neq 2$, f is separable (it has degree 2) and Hurwitz formula gives

$$0 = -4 + \text{number of ramification points} \qquad \text{(because } \operatorname{ord}_x(f) = 1 \text{ or } 2\text{)}.$$

There are exactly 4 points of 2-torsion. In particular, $[2]$ is non-constant.

Invariant differentials.

Rmk: Let E be an elliptic curve. Then $h^0(\Omega_E) = 1$. Let ω be a basis of $H^0(\Omega_E)$. Let E, E' be elliptic curves and ω, ω' basis of $H^0(\Omega_E)$ and $H^0(\Omega_{E'})$.

If $f: E \to E'$ is a morphism of elliptic curves,

$$\Rightarrow f^* \omega' = \lambda_f \omega \qquad \text{with } \lambda_f \in k.$$

$H^0(\Omega_E)$

This depends on the chosen basis. In the following I keep the basis fixed.

Rmk: $\lambda_f \neq 0 \iff f$ is non constant and separable.

Thm: i) $x \in E(k)$, $t_x : E \to E$, $y \mapsto x+y$

$$\Longrightarrow \quad \lambda_{t_x} = 1 \qquad \text{(here } E = E' \text{ and } \omega = \omega'\text{)}.$$

2) $\varphi, \psi : E \to E'$ morphisms of elliptic curves

$$\Longrightarrow \quad \lambda_{\varphi+\psi} = \lambda_\varphi + \lambda_\psi .$$

In particular, $\lambda_{[m]} = m$, and $[m]$ is separable iff $\mathrm{char}(k) \nmid m$.

Cor: If $k = \bar{k}$ and $\mathrm{char}(k) \neq 2$, then $\ker([2^n]) = E[2^n] \simeq (\mathbb{Z}/2^n\mathbb{Z})^2$.

Pf: We know that $[2]$ is separable of degree 4

$$\Longrightarrow \quad [2^n] \text{ ——————— } 4^n$$

(induction)

$$\Longrightarrow \quad \#E[2^n] = 4^n = (2^n)^2 .$$

By induction

$$0 \to E[2] \to E[2^n] \xrightarrow{[2]} E[2^{n-1}] \to 0.$$

$(\mathbb{Z}/2\mathbb{Z})^2$ — because it is a $\mathbb{Z}/2\mathbb{Z}$-vector space of dim 2.

$(\mathbb{Z}/2^{n-1}\mathbb{Z})^2$ — inductive hypothesis.

$$\Longrightarrow \quad E[2^n] \simeq (\mathbb{Z}/2^n\mathbb{Z})^2 . \qquad \square$$

Cor: The map $\lambda : \mathrm{End}(E) \to k$, $\varphi \mapsto \lambda_\varphi$ (Here $E = E'$ and $w = w'$.) does not depend on the chosen w, it is a ring w.r.t. composition with kernel made of the isogenies φ s.t. $\deg_i(\varphi) \geq 1$.

In particular, if $\mathrm{char}(k) = 0$, then λ is an injective ring map. Thus $\mathrm{End}(E)$ is a commutative integral domain.

Cor: If E is an elliptic curve over $\mathbb{Q}$, then $\mathrm{End}(E) = \mathbb{Z}$.

Pf: Tomorrow we will see that $\deg([m]) = m^2$. In particular, if $m \neq 1$, then m is not invertible. So $\mathrm{End}(E)$ cannot contain $\mathbb{Z}$ strictly. $\square$