Fact 4: For a morphism $C \xrightarrow{\phi} Y$ of nonsingular projective curves, ϕ is an isomorphism ($\exists$ a morphism $\psi: C \to Y$: $\phi \circ \psi = id$, $\psi \circ \phi = id$) iff $\deg(\phi) = 1$.

Review of Galois theory
(finite & infinite)

Friday 5pm ET.

Prop: Let $(E, \mathcal{O})$ be an elliptic curve over k.

① $\exists\ x, y \in k(E)$ such that the rational map

$$\phi : E \dashrightarrow \mathbb{P}^2 \text{ given by } [x, y, 1]$$

gives an isomorphism of E over k to a projective curve $C \hookrightarrow \mathbb{P}^2$ given by a Weierstrass equation

Rmk: if $\mathrm{char}\, k \neq 2$, complete the square to arrange $a_1 = a_3 = 0$; if $\mathrm{char}\, k \neq 3$, complete cube $\Rightarrow a_2 = 0$

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with $a_1, \dots, a_6 \in k$; moreover $\phi(\mathcal{O}) = [0, 1, 0]$.

② Conversely, any nonsingular cubic $C \hookrightarrow \mathbb{P}^2$ given by such a Weierstrass equation has genus 1, hence $(C, \mathcal{O} = [0, 1, 0])$ is an elliptic curve over k.

Pf: ② is a generalization of the pset 4 problem (show $\mathrm{div}(\omega) = 0$, where $\omega = \frac{dx}{2y + a_1x + a_3}$, and then apply R-R: $2g - 2 = 0$, so $g = 1$).

---

① follows from R-R. Consider for any $n \geq 1$ $n \cdot [\mathcal{O}] \in \mathrm{Div}_k(E)$. By R-R,

$$\ell(n \cdot [\mathcal{O}]) = \dim L(n \cdot [\mathcal{O}]) = \dim \{ f \in \bar{k}(E)^\times \mid \mathrm{div} f \geq -n[\mathcal{O}] \} \cup \{0\}$$

$$= n - 1 + 1 = n. \quad (\forall\ n \geq 1).$$

$L([\mathcal{O}]) =$ constants

$L(2\cdot[\mathcal{O}])$ is 2-dim'l, has basis $1, x$ for some $x \in k(E)\setminus k$ (so $v_P(x) \geq 0 \ \forall P \neq \mathcal{O}$, and $v_{\mathcal{O}}(x) = -2$.

$L(3\cdot[\mathcal{O}])$: 3-D, has basis $1, x, y$ for some $y \in k(E)$ with $v_P(y) \geq 0 \ \forall P \neq \mathcal{O}$ and $v_{\mathcal{O}}(y) = -3$.

$L(4\cdot[\mathcal{O}]) = 4$-D, contains $1, x, y, x^2$, and these are a basis (compare $v_{\mathcal{O}}(\cdot)$ to show these are lin. ind.).

$L(5\cdot[\mathcal{O}])$: basis $1, x, y, x^2, xy$

$L(6\cdot[\mathcal{O}])$: 6-D and contains $\underbrace{1, x, y, x^2, xy, x^3, y^2}_{7 \text{ functions}}$

so $\exists$ k-linear dependence

$$c_1\cdot 1 + c_2\cdot x + c_3\cdot y + c_4\cdot x^2 + c_5\cdot xy + c_6\cdot x^3 + c_7\cdot y^2 = 0 \quad (\text{in } k(E))$$

c_6 and c_7 must both be non-zero:
if either c_6 or c_7 is 0, then every term in the above equation's LHS has a different $v_{\mathcal{O}}$. This $= 0$ would contradict $v_{\mathcal{O}}(a+b) = \min(v_{\mathcal{O}}(a), v_{\mathcal{O}}(b))$ when $v_{\mathcal{O}}(a) \neq v_{\mathcal{O}}(b)$.

After a suitable rescaling of x & y we can then assume $c_6 = -1$, $c_7 = 1$, and then we obtain an equation of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Thus $[x, y, 1] : E \dashrightarrow \mathbb{P}^2$ gives a rational map with image contained in the curve $C \hookrightarrow \mathbb{P}^2$ given by the stated Weierstrass

equation (w.E.)

Since E is a nonsing curve, ϕ is regular everywhere: $\phi: E \to \mathbb{P}^2$.

ϕ is clearly non-constant, so it is a surjective morphism $\phi: E \to C \hookrightarrow \mathbb{P}^2$.

Why is ϕ an isomorphism:

Check $\deg(\phi) = 1$ & C nonsingular.

- $\deg(\phi) := [k(E) : \phi^* k(C)]$. $\phi^*: k(C) \to k(E)$ has image $k(x,y) \subset k(E)$.

But $k(x,y) = k(E)$ because:

- $[k(E) : k(x)] = 2$
- $[k(E) : k(y)] = 3$
- $\gcd(2,3) = 1$.

$x: E \to \mathbb{P}^1$ degree 2. $\longleftrightarrow$ $k(x) \subset k(E)$

Since $y: E \to \mathbb{P}^1$ has degree ?

- We'll be done by Fact 4 from last time once we check C nonsing. Suppose not [Using a exercise! COV, w.l.o.g. C given by $y^2 + a_1 xy = x^3 + x^2$ with unique singular point $(0,0)$.] Then the rat'l map $C \xrightarrow{\psi} \mathbb{P}^1$ has degree 1. Now consider $(x,y) \longmapsto [x,y]$

So C must be nonsing.

$$E \xrightarrow[\deg 1]{\phi} C \xrightarrow[\deg 1]{\psi} \mathbb{P}^1$$

$\psi \circ \phi$ is a rat'l map of deg 1 from E to $\mathbb{P}^1$, which forces $E \cong \mathbb{P}^1$

Contradiction!

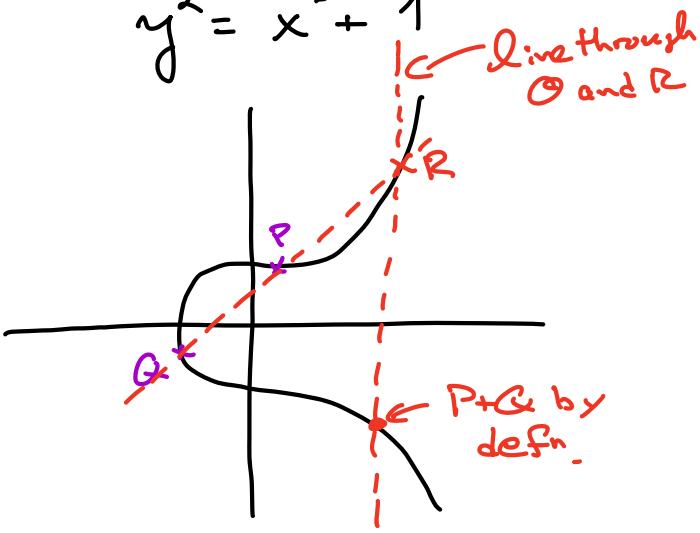
- $\phi(\mathcal{O}) = [0,1,0]$: ex. (use $v_{\mathcal{O}}(x) = -2$, $v_{\mathcal{O}}(y) = -3$ ---).

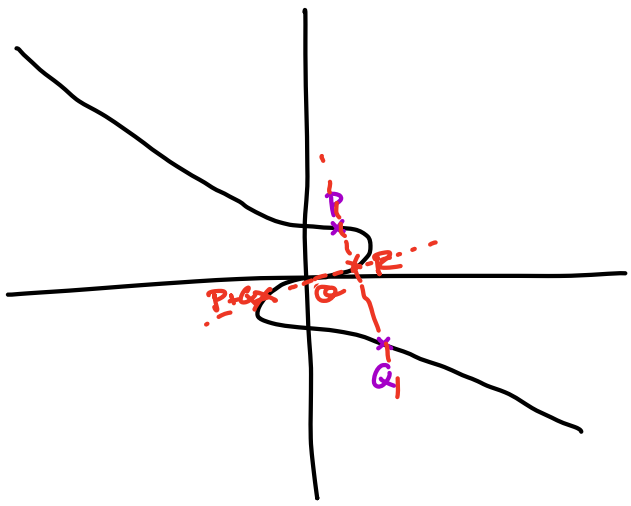
The group law on an elliptic curve

- $E \hookrightarrow \mathbb{P}^2$, $\mathcal{O} = [0,1,0]$ an elliptic curve given by a Weierstrass equation.
- Since this is a cubic, every line in $\mathbb{P}^2$ intersects E 3 times (counting multiplicity)
- Use this to define a group operation on E, with identity $\mathcal{O}$:

$y^2z = x^3 + z^3$ $\quad v = z/y,\ u = x/y$

$y^2 = x^3 + 1$ $\qquad v = u^3 + v^3$ $\quad \mathcal{O} = (0,0)$





$\{z \neq 0\} \cap E$ $\qquad$ $\{y \neq 0\} \cap E$

That is, $\overline{PQ}$ intersects E at a 3rd point R

$\overline{RO}$ " " " at a 3rd point S

We define $P \oplus Q = S$

When $P = Q$, the line $\overline{PQ}$ means the tangent line to E (nonsingular!) at P.

Theorem ⑥ The operation $\oplus : E \times E \longrightarrow E$ is well-defined

① $\forall\, P \in E,\ P \oplus \mathcal{O} = P$

② $\forall\, P, Q \in E,\ P \oplus Q = Q \oplus P$

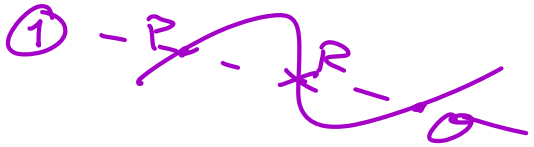
③ $\forall\, P \in E,\ \exists!$ point "$-P$" $\in E$: $P \oplus (-P) = \mathcal{O}$

④ $\forall\, P, Q, R \in E,\ (P \oplus Q) \oplus R = P \oplus (Q \oplus R)$

⑤ For any field $L \supset k$, $(E(L), \oplus)$ is an abelian group.

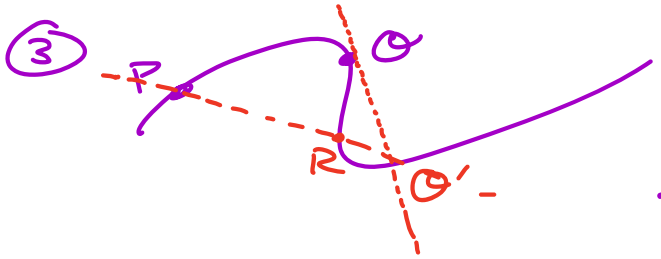
⑥ $\oplus : E \times E \longrightarrow E$ is a <u>morphism</u> of algebraic varieties over k. $\underset{P \longmapsto -P}{E \longrightarrow E}$ is a morphism. (strengthens ⑤)

Pf: ⑤ Check left as an exercise. More conceptually, Bézout's theorem in a very special case shows a line intersects a cubic (in $\mathbb{P}^2$) in 3 points counting multiplicity.

① 

$\overline{RO}$ hits E at $P \rightsquigarrow P \oplus \mathcal{O} = P$.

② clear. ($\overline{PQ} = \overline{QP}$).

③ 

Then $R = -P$. (i.e. $P \oplus R = \mathcal{O}$) Here the picture allows $\mathcal{O} \neq \mathcal{O}'$. In fact for a WE with $\mathcal{O} = [0,1,0]$, $\mathcal{O} = \mathcal{O}'$

(i.e. the tangent line $Z=0$ to E at $\mathcal{O}$ intersects E with mult. 3).

④ Harder: can use brute force or can use Bezout's theorem (Milne's notes, or Silverman-Tate, or Fulton). Assume this after now.

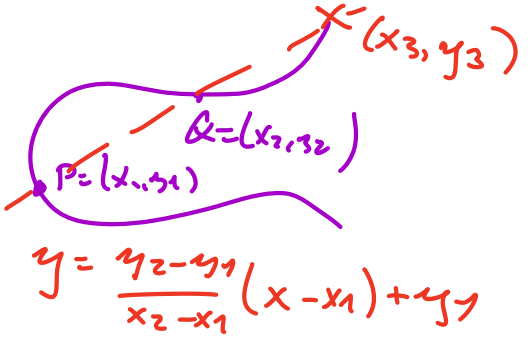
⑤ For $P, Q \in E(L)$, the line between P & Q has equation with coeff's in L; plugging this equation into that of E, get a cubic equation $\in L[x]$ with 2 known roots in L, hence all roots in L.

⑥ (Assume $\mathcal{O}$) In $\{Z \neq 0\}$, writing down the formulas for

$\oplus : E \times E \to E$ shows that they are

$- : E \to E$ rational maps, "$-$" is then a morphism since E nonsing. proj.

The formulas for $\oplus$ won't obviously be regular at points (P, Q): $P = \pm Q$ or at least one of P, Q is $\mathcal{O}$.



Could brute force this, but let's not.

$\forall\, Q \in E$, the map

$\tau_Q : E \to E$ is an isomorphism

$P \mapsto P \oplus Q$

For any $Q_1, Q_2 \in E$, the rational map

$$E \times E \to E \times E \xrightarrow{\oplus} E \xrightarrow{\tau_{Q_1}} E \xrightarrow{\tau_{Q_2}} E$$

$$(P, Q) \mapsto (P+Q_1, Q+Q_2) \mapsto (P \oplus Q_1) \oplus (Q \oplus Q_2) \mapsto P \oplus Q$$

(uses associativity)

This composite is clearly regular at all (P, Q): $P + Q_1 = \pm(Q + Q_2)$ or one of $P+Q_1$, $Q+Q_2 = \mathcal{O}$ and where it is regular it agrees with $\oplus : E \times E \to E$. Easy exercise: by making appropriate choices of Q_1, Q_2, find that $\oplus$ is regular everywhere.

not true in higher genus!

Proof of associativity using Riemann-Roch

Prop: $P \xmapsto{J} [P]-[\mathcal{O}]$ defines a bijection

$$E \longrightarrow \mathrm{Pic}^0(E) \quad \left(= \mathrm{Div}^0(E)/\mathrm{div}(\bar{k}(E)^*)\right)$$

under which addition of divisor classes in $\mathrm{Pic}^0 E$ corresponds to "$\oplus$" on E. In particular, $\oplus$ is associative.

Pf: **Injective:** Suppose $[P]-[\mathcal{O}] \sim [Q]-[\mathcal{O}]$ (equiv. in Pic).

Then $[P]-[Q] = \mathrm{div}(f)$ for some $f \in \bar{k}(E)^*$.

As we have noted already, the resulting morphism $f: E \to \mathbb{P}^1$ unless constant has degree 1, hence is an iso. $\Rightarrow\Leftarrow$. Thus f is constant & $P = Q$.

Surjective: Let $D \in \mathrm{Div}^0(E)$. Apply R-R to

$D+[\mathcal{O}] \rightsquigarrow \ell(D+[\mathcal{O}]) = 1 - 1 + 1 = 1$

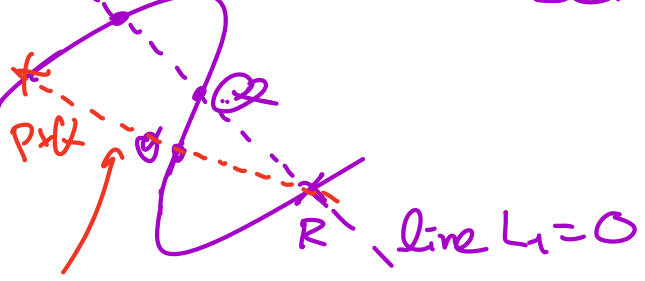
so $\exists\, f \in \bar{k}(E)^*$: $\underbrace{\mathrm{div}(f) + D + [\mathcal{O}]}_{\text{degree 1 div. with all coeffs} \geq 0} \geq 0$

so we must have $\mathrm{div}(f) + D + [\mathcal{O}] = [P]$ for some $P \in E$.

Thus $D = [P]-[\mathcal{O}]$ in $\mathrm{Pic}^0(E)$, so J is surjective.

- Now we must show $J(P)+J(Q) = J(P+Q)$ $\forall P, Q \in E$

If P [illegible] Let $f = \frac{L_1}{L_2}$ (ratio of has linea



regarded as an element of $\bar{K}(E)$.

$$\operatorname{div}(f) = [P]+[Q]+[R] - ([P+Q]+[\mathcal{O}]+[R])$$
$$= [P]-[\mathcal{O}]+[Q]-[\mathcal{O}]-([P+Q]-[\mathcal{O}])$$

Thus in $\mathrm{Pic}^0(E)$, $J(P)+J(Q)-J(P+Q)=\mathcal{O}$. ∎

Our goal in the next two weeks: prove the Mordell-Weil Theorem: Let K be a number field. Let $(E,\mathcal{O})$ be an elliptic curve over K. Then the abelian group $E(K)$ is finitely-generated. (Hence $\cong$ (finite torsion group) $\times \mathbb{Z}^r$ some $r \geq 1$).

Isogenies:

Defn: Let $(E,\mathcal{O})$ and $(E',\mathcal{O}')$ be elliptic curves over k. An isogeny from $(E,\mathcal{O})$ to $(E',\mathcal{O}')$ is a non-constant (hence surjective) morphism

$$\phi: E \longrightarrow E' \text{ such that}$$
$$\phi(\mathcal{O}) = \mathcal{O}'$$

Key example: $m \in \mathbb{Z}\setminus 0$. The multiplication by m isogeny: $[m]: E \longrightarrow E$