§1. Elliptic Curves

Def An elliptic curve is a pair (E, P), where E is a smooth projective curve of genus one over ~~an algebraically closed~~ an alg. closed field k together with a k-rational point P. ("basepoint")

~~and $O \in |E|$ is a fixed basepoint.~~ ↓ closed points

Prop Let E be an elliptic curve. There exist functions $x, y \in k(E)$ such that the map

$$\begin{aligned} \phi : E &\hookrightarrow \mathbb{P}^2 \\ a &\mapsto [1 : x(a) : y(a)], \quad a \neq P \\ P &\mapsto [0 : 1 : 0] \end{aligned}$$

gives an isomorphism of E onto a curve given by the Weierstraß equation

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in k.$$

Proof (idea):

~~Look at $\mathcal{L}(nP)$ for $n = 1, \ldots$~~

By Riemann-Roch, $\dim \mathcal{L}(nP) = n$.

Take basis $\{1, x\}$ of $\mathcal{L}(2P)$ and extend it to a basis $\{1, x, y\}$ of $\mathcal{L}(3P)$.

Because $\ell(6P) = 6$, the 7 functions

$$1, x, y, x^2, xy, y^2, x^3$$

must satisfy a relation

$$A_1 + A_2 x + A_3 y + A_4 x^2 + A_5 xy + A_6 y^2 + A_7 x^3 = 0.$$

x must have a pole of order 2 at P, because it isn't in $\mathcal{L}(1P)$, same with y, it must have a pole of order 3 at P. Thus both A_6 and A_7 must be non-zero. □

Remark Conversely, every smooth cubic curve given by a Weierstraß equation (like above is an elliptic curve with basepoint $P = [0:1:0]$

Cor The map $Q : \mathcal{L}(h) \to \mathrm{Pic}^0(E)$, $Q \mapsto [Q - P]$ is a bijection.

Lemma Let C be a curve of genus 1. Then

$$(P) \sim (Q) \text{ iff } P = Q$$

Proof "$\Leftarrow$" clear.

"$\Rightarrow$" Choose $f \in \mathcal{L}(C)$ s.t. $\mathrm{div}(f) = P - Q$. Riemann-Roch says that $\dim \mathcal{L}(Q) = 1$, but $\mathcal{L}(Q)$ contains the constant functions $\Rightarrow f \in h \Rightarrow P = Q$. □

Proof (of Prop)

injectivity ✓ (Lemma)

Surjectivity: Let $A \in Cl^0(E)$

Riemann-Roch: $\dim \mathcal{L}(A+P) = 1$

$\Rightarrow \exists f \in k(C)$ s.t. ~~$\operatorname{div}(f) \geq$~~

$\operatorname{div}(f) \geq -A - P$. From a previous talk we know $\deg(\operatorname{div} f) = 0$, so

$$\underbrace{\operatorname{div}(f) + A + P}_{\text{degree } 1} \geq 0$$

since effective of degree 1

thus it's a point Q: $\operatorname{div}(f) + A + P = Q \iff Q \sim A + P$,

$\mathcal{L}(A)$ ~~$\Leftrightarrow$ $\operatorname{div}(f) =$~~

and so $\alpha(Q) = A$. □

We can now 'transport' the group structure of $\mathrm{Pic}^0(E)$ onto $\mathcal{L}(A)$ using α:

Lemma ~~Given~~ Let A, B, C be k-rational points of $\mathcal{L}$. Then $A \oplus B \oplus C = P$ iff A, B, C are the three intersection points of $\mathcal{L}$ with a line.

Proof "$\Rightarrow$": Suppose $A + B + C \sim 3P$, this means $\exists f \in k(C)$: $\operatorname{div}(f) = A + B + C - 3P$

$\Rightarrow f \in \mathcal{L}(3P) \Rightarrow f = c_1 1 + c_2 X + c_3 Y$. f has zeroes at A, B, C, so they lie on the line $c_1 X_1 + c_2 X_2 + c_3 X_3 = 0$.

"⇐": Suppose A, B, C lie on the line

$$c_1X_1 + c_2X_2 + c_3X_3 = 0.$$

Let $f = c_1 1 + c_2 x + c_3 y$. By Bézout the only zeroes of f are A, B, C. It further has a pole at P, since $\operatorname{ord}_P y = -3$.

Thus $\operatorname{div}(f) = A + B + C - 3P$

$\Leftrightarrow$ $A + B + C \sim 3P$. □

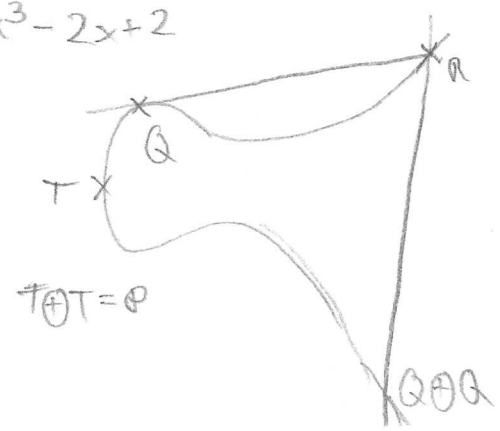
Using this lemma we can now efficiently write down the addition in $E(k)$:

Composition law Let $Q, R \in E(k)$, let L be the line through Q and R (if $Q = R$, let L be the tangent line to E at Q), and let S be the third point of intersection of L with E. Let L' be the line through S and P. Then L' intersects E at S, P, and a third point, ~~we denote that third point by~~ namely $Q \oplus R$.

Example



$y^2 = x^3 - 2x + 2$



Remark You can write out explicit formulas for the addition of points. E.g.:

Let E be given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two points on E.

If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P_1 \oplus P_2 = P_\infty$. Otherwise define

	λ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$	$\dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$

Then $P_3 = P_1 \oplus P_2$ has the coordinates

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

Remark Given a non-smooth curve E given by a Weierstraß equati (i.e. $\Delta = 0$), the set of nonsingular points $E_{ns}(k)$ still forms an abelian group using the same composition law.

2. Elliptic Integrals, Weierstraß ℘, Lattices

We are trying to integrate on $E(\mathbb{C})$: $\int_{QP}^{R} \omega$, $\omega = \frac{dx}{y}$ hol. diff. form on E

however it isn't really clear how to do so since integral is path-dependent

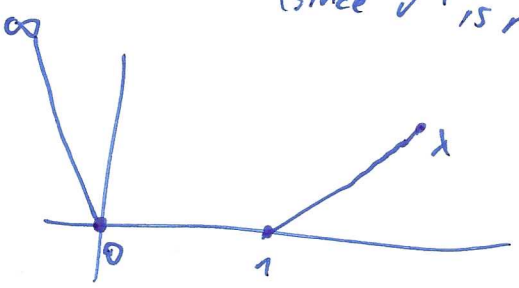
→ pass to $\mathbb{P}^1(\mathbb{C})$ first

$$E(\mathbb{C}) \hookrightarrow \mathbb{P}^1(\mathbb{C})$$

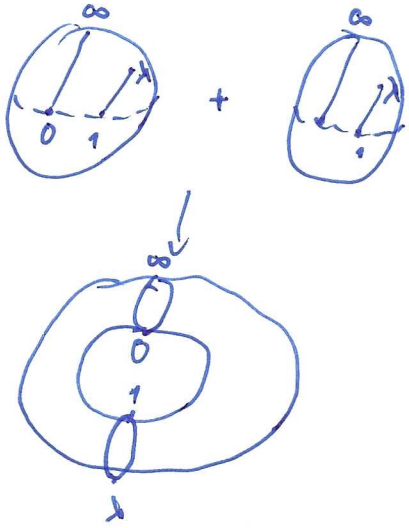
$$\downarrow 2:1$$

$$\mathbb{C} \xleftarrow{\int_\infty^x \frac{dt}{\sqrt{t(t-1)(t-\lambda)}}} \quad \text{since } \mathbb{C} \text{ alg closed, can write } E \text{ in Legendre form } y^2 = x(x-1)(x-\lambda)$$

~~We now see~~ This still isn't well-defined, need to add branch cuts: (since $\sqrt{\ }$ is multi-valued)



→ should take 2x $\mathbb{P}^1(\mathbb{C})$s, make branch cuts & glue ($+\sqrt{\ }$ and $-\sqrt{\ }$)



Integrating on this RS still isn't well defined: integrating around non-contractible loops adds a constant corresponding to that loop.

$\rightsquigarrow \int_p^Q \omega$ is well defined up to addition of these constants ω_1, ω_2.

Let α, β be the generators of $\pi_1(RS)$

$\Rightarrow \quad \omega_1 = \int_\alpha \omega, \quad \omega_2 = \int_\beta \omega$

$\Rightarrow$ We get a map

$$RS \longrightarrow \mathbb{C}/\Lambda, \text{ where } \Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \text{ lattice}$$

As it turns out, $\mathcal{E}(\mathbb{C})$ is also well-defined and an iso.

We will now turn to the other direction of this map.

<u>Definition</u> An elliptic function (relative to Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ s.t.

$$f(z+\omega) = f(z) \quad \forall z \in \mathbb{C}, \omega \in \Lambda.$$

(Uses Liouville's Thm)

Proposition A holomorphic elliptic function is constant. *1

(In fact, a nonconstant elliptic function has order at least 2

*1 An ell. function with no zeros is constant. (take $1/f$)

Def/Prop Let $\Lambda \subseteq \mathbb{C}$ be a lattice. The Weierstraß $\wp$-function defined by the series

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

is an ell. function. The Eisenstein series of weight $2k$ defined by the series

$$G_{2k}(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-2k}$$

$\left(\text{ex: } \Lambda = \mathbb{Z}[i], \; G_4(\Lambda) = \frac{\Gamma(1/4)^8}{960\pi^2} \right)$

is absolutely convergent $\forall k > 1$.

Thm $\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z))$.

$\mathbb{C}(\Lambda)$: field of elliptic functions.

Notation We set

$$g_2 = g_2(\Lambda) = 60\, G_4(\Lambda)$$

$$g_3 = g_3(\Lambda) = 140\, G_6(\Lambda)$$

Thm (Uniformization Theorem)

Let $A, B \in \mathbb{C}$ s.t. $4A^3 - 27B^2 \neq 0$. Then $\exists! \Lambda$ s.t. $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$.

Let $\Lambda \subset \mathbb{C}$ be a lattice.

Prop The curve

$$y^2 = 4x^3 - g_2 x - g_3$$

is an elliptic curve over $\mathbb{C}$ with discriminant $g_2^3 - 27 g_3^2 \neq 0$. The map

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$$
$$z \mapsto [\wp(z) : \wp'(z) : 1]$$

is a complex analytic iso of complex Lie groups (iso of RS + group hom).

(elliptic curve: showing that the poly has distinct roots $\Rightarrow \Delta \neq 0$)

Def An isogeny between two elliptic curves E_1 and E_2 is a morphism of curves

$$\phi : E_1 \to E_2$$

with $\phi(P) = P$.

(thus either $\phi(E_1) = \{P\}$ or $\phi(E_1) = E_2$)

Let Λ_1, Λ_2 be lattices in $\mathbb{C}$. Suppose $\alpha \in \mathbb{C}$ has the property that $\alpha\Lambda_1 \subseteq \Lambda_2$. Then scalar mult. induces a well-defined holomorphic homomorphism

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$
$$z \mapsto \alpha z \pmod{\Lambda_2}.$$

Thm a) $\{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subseteq \Lambda_2\} \longrightarrow \{$holomorphic maps $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ with $\phi(0)=0\}$

$$\alpha \longmapsto \phi_\alpha$$

is a bijection.

b) Let $\mathcal{E}_1, \mathcal{E}_2$ be the elliptic curves corresponding to Λ_1, Λ_2. Then

$$\{\text{isogenies } \phi : \mathcal{E}_1 \to \mathcal{E}_2\} \longhookrightarrow \{\text{holom. maps } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \text{ with } \phi(0)=0$$

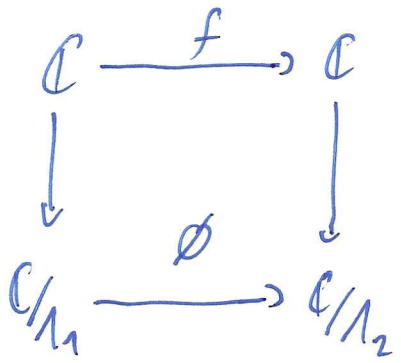
is a bijection.

Proof a) inj: If $\phi_\alpha = \phi_\beta$ then

$$\alpha z \equiv \beta z \pmod{\Lambda_2} \quad \forall z \in \mathbb{C}$$

$\Rightarrow z \mapsto (\alpha-\beta)z$ maps $\mathbb{C}$ to Λ_2, but Λ_2 is discrete, so this map must be constant $\Rightarrow \alpha = \beta$.

surj: Let $\phi: \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ s.t. $\phi(0)=0$. Since $\mathbb{C}$ is simply connected we get a lift



By commutativity, $f(z+\omega) \equiv f(z) \pmod{\Lambda_2}$ $\forall \omega \in \Lambda_1, z \in \mathbb{C}$

Again by discreteness of Λ_2, $f(z+\omega)-f(z)$ must be independent of z. Differentiating we get

$$f'(z+\omega) = f'(z) \quad \forall \omega \in \Lambda_1, z \in \mathbb{C}$$

$\Rightarrow$ f' is a holomorphic elliptic function

$\Rightarrow$ f' is constant

$\Rightarrow$ $f(z) = \alpha z + r$ for some $\alpha, r \in \mathbb{C}$

$f(0)=0 \Rightarrow r=0$, but also $f(\Lambda_1) \subseteq \Lambda_2 \Rightarrow \phi = \phi_\alpha$.

b) ~~From~~ By a) it suffices to look at a ϕ_α, $\alpha \in \mathbb{C}^\times$.

The induced map on Weierstraß equations is given by

$$\mathcal{E}_1 \longrightarrow \mathcal{E}_2$$
$$[\wp(z,\Lambda_1) : \wp'(z,\Lambda_1) : 1] \mapsto [\wp(\alpha z, \Lambda_2) : \wp'(\alpha z, \Lambda_2) : 1]$$

$\Rightarrow$ Need to show that ~~$\wp(z, \Lambda_2)$~~ $\wp(\alpha z, \Lambda_2)$ and $\wp'(\alpha z, \Lambda_2)$ can be expressed as rational ~~fun~~ expressions in $\wp(z, \Lambda)$ and $\wp'(z, \Lambda_1)$. (isogenies are rational maps)

We have

$$\wp(\alpha(z+\omega), \Lambda_2) = \wp(\alpha z + \alpha\omega, \Lambda_2) = \wp(\alpha z, \Lambda_2).$$

(since $\alpha\Lambda_1 \subseteq \Lambda_2$)

Same with $\wp'(z, \Lambda_2)$.

$\Rightarrow$ $\wp(z, \Lambda)$ and $\wp'(z, \Lambda_2)$ are in $\mathbb{C}(\Lambda)$

$\square$ by Thm.

Corollary $\mathcal{E}_1 \cong \mathcal{E}_2 \iff \Lambda_1$ and Λ_2 are homothetic

$\iff$

$\exists \alpha \in \mathbb{C}: \alpha\Lambda_1 \subseteq \Lambda_2$