Exercise class 28.5.2025

discrete subgp. $\mathbb{Z}w_1 \oplus \mathbb{Z}w_2$ $\quad w_i \in \mathbb{R}$

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

In lectures we defined:

$$\varphi_\Lambda : \mathbb{C}/\Lambda - \{0\} \longrightarrow \{(z,w) \in \mathbb{C}^2 \mid w^2 = 4z^3 - az - b\} =: E(\mathbb{C})$$

$$a = -60 G_4(\Lambda) =: -g_2(\Lambda)$$
$$b = -140 G_6(\Lambda) =: -g_3(\Lambda)$$

Def. Weierstrass $\wp$-func. of Λ

$$\wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

for $z \notin \Lambda$

$\rightsquigarrow$ in lectures we saw:

Prop. (1) Any meromorphic ell. func. is a rational func. of $\wp_\Lambda$ & $\wp_\Lambda'$

(2) $\wp_\Lambda'(z)^2 = 4\wp_\Lambda(z)^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda)$ ☆

§ Elliptic integrals

$$\Lambda := w_1\mathbb{Z} \oplus w_2\mathbb{Z}$$

$$\phi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$$
$$z \longmapsto (\wp(z), \wp'(z))$$

*how can we define $E(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C})$?

Fact: $\wp(z+w_1) = \wp(z) = \wp(z+w_2)$ & $\wp(z) = \wp(-z)$

$\wp'(z+w_1) = \wp'(z) = \wp'(z+w_2)$

$\Rightarrow (\wp(z), \wp'(z))$ only depends on the coset z mod Λ

$E : y^2 = x^3 + Ax + B$ ell. curve

$\omega = \frac{dx}{y}$ is a holom. differential form on E

$\rightsquigarrow$ we want a map like $\begin{cases} E(\mathbb{C}) \longrightarrow \mathbb{C} \\ P \overset{?}{\longmapsto} \int_0^P \omega \end{cases}$

what path?

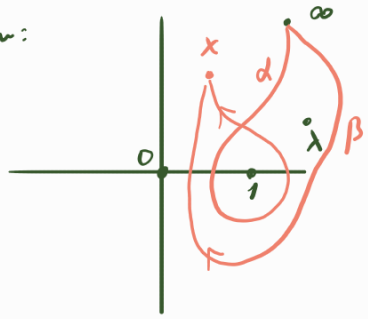
$\begin{cases} E(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C}) \\ (x,y) \longmapsto x \end{cases}$ double cover ramified precisely at $0, 1, \lambda, \infty \in \mathbb{P}^1(\mathbb{C})$

where $y^2 = x(x-1)(x-\lambda)$ (Legendre form)

$\rightsquigarrow$ we want to compute the integral

$$\int_0^x \frac{dt}{\sqrt{t(t-1)(t-\lambda)}}$$

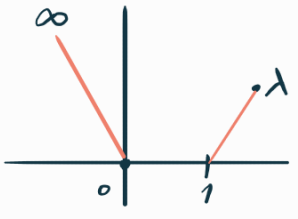
problem:



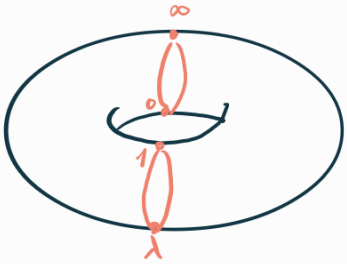
not path-indep. ($\sqrt{\ }$ not single valued)

$\rightsquigarrow$ could be $\int_\alpha \omega \neq \int_\beta \omega$

Solution: make branch cuts & glue them together along these cuts

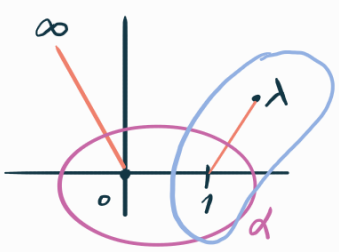


$\Rightarrow$

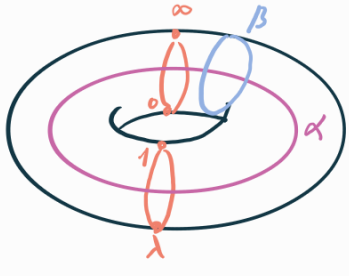


i.e.

$\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$



$\Rightarrow$



$$\omega_1 := \int_\alpha \omega \qquad \omega_2 := \int_\beta \omega$$

$\Rightarrow \int_0^P \omega$ is well-Def. up to addition of a # of the form $n_1\omega_1 + n_2\omega_2$ (any two paths from O to P differ by a path homologous to $n_1\alpha + n_2\beta$) for some $n_i \in \mathbb{Z}$

$\Rightarrow$ $E(\mathbb{C}) \longrightarrow \mathbb{C}/\Lambda$

$P \longmapsto \int_0^P \omega \pmod{\Lambda}$ well-Def ✓

[Fact: ω is translation-invariant

$$\Rightarrow \int_0^{P+Q} \omega \equiv \int_0^P \omega + \int_P^{P+Q} \omega \equiv \int_0^P \omega + \int_0^Q \omega \pmod{\Lambda}$$

Proposition - (1) φ_Λ is bijective

(2) The polynomial

$$X^3 - 60\,G_4(\Lambda)\,X - 140\,G_6(\Lambda)$$

in $\mathbb{C}[X]$ has no multiple root

(3) Conversely, for any a, b in $\mathbb{C}$ with $X^3 + aX + b$ without multiple root, there is a Λ s.t.

$$\begin{cases} a = -60\,G_4(\Lambda) \\ b = -140\,G_6(\Lambda) \end{cases}$$

and Λ is unique if one takes isomorphism into account properly.

proof: (1)

Claim: ϕ is bijective

injective:

$$\phi(z_1) = \phi(z_2)$$

assume first $2z_1 \notin \Lambda$

$\Rightarrow \wp(z) - \wp(z_1)$ ell. func. of order 2 vanishing at $z_1, -z_1$ & z_2

Since $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z} \Rightarrow$ two of $z_1, -z_1, z_2$ are congruent mod Λ

Since $2z_1 \notin \Lambda \Rightarrow z_2 \equiv \pm z_1 \pmod{\Lambda}$

$$\Rightarrow \wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm \wp'(z_1)$$

$$\Rightarrow z_1 \equiv z_2 \pmod{\Lambda}$$

If $2z_1 \in \Lambda$

$\Rightarrow \wp(z) - \wp(z_1)$ has a double zero at z_1 & vanishes at z_2

$\Rightarrow$ (same argument) $z_2 \equiv z_1 \pmod{\Lambda}$ ✓

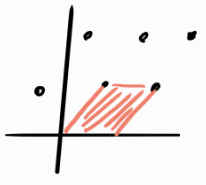
surjective: $(x, y) \in E(\mathbb{C})$ (20)

$\Rightarrow \wp(z) - x$ is a non-const. ell. func.

[**Prop.** An ell. func. w/ no zeros is const.

$f(z)$ holom. ell. func.

$D :=$ fund. parall. for Λ



f periodic $\Rightarrow \sup_{z \in \mathbb{C}} |f(z)| = \sup_{z \in \bar{D}} |f(z)|$

f cont. & $\bar{D}$ cpt. $\Rightarrow |f(z)|$ bdd. on $\bar{D}$

$\Rightarrow f$ bdd. on all of $\mathbb{C}$

(Liouville) $\Rightarrow f$ const.

f has no zeros $\Rightarrow 1/f$ holom. $\Rightarrow$ const. □

$\Rightarrow \wp(z) - x$ has a zero, say $z = a$

$\Rightarrow \wp(a) = x$

$\rightsquigarrow y^2 = x^3 - Ax - B \Rightarrow \wp'(a)^2 = y^2$

So replacing a by $-a$ if necessary, get $\wp'(a) = y$

$\Rightarrow \phi(a) = (x, y)$ ✓

(2) $\omega_3 := \omega_1 + \omega_2$, $\quad f(x) := 4x^3 - g_2 x - g_3$

in lectures: $\wp'(z)$ is an odd ell. func.

$$\wp'\left(\frac{\omega_i}{2}\right) = -\wp'\left(\frac{-\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right)$$

$\Rightarrow \wp'\left(\frac{\omega_i}{2}\right) = 0$

Since $\wp'(z)^2 = 4\wp(z)^3 - 60 G_4 \wp(z) - 140 G_6, \quad \forall z \in \mathbb{C}/\Lambda$

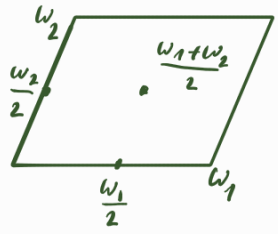
$\Rightarrow f\left(\wp\left(\frac{\omega_i}{2}\right)\right) = 0$

$\rightsquigarrow$ to show: these $\wp\left(\frac{\omega_i}{2}\right)$ are distinct

$\wp(z) - \wp\left(\frac{\omega_i}{2}\right)$ is even $\Rightarrow$ it has at least a double zero at $z = \frac{\omega_i}{2}$

↑ ell. func. of order 2 $\rightsquigarrow$ it has only these zeros in a fund. ▱

$\Rightarrow \wp\left(\frac{\omega_i}{2}\right) \neq \wp\left(\frac{\omega_j}{2}\right)$ for $i \neq j$



§ Group structure on ell. curves

E ell. curve $y^2 = x^3 + ax + b$ / K field

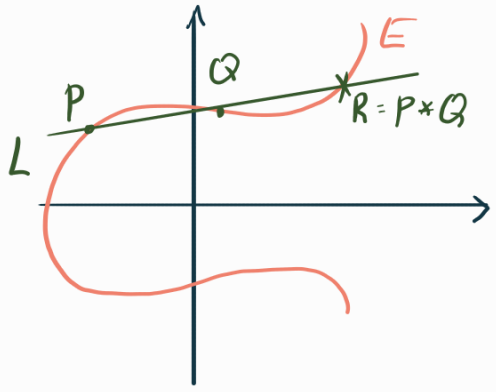
E is rational if it has rational coeff.'s

ex. $X^3 + Y^3 = 1$

Q. does it have rational solutions?
how do we find rational pts.?

(Bezout's Thm.) Every line cuts an ell. curve in exactly 3 pts.

If we know 2 rational pts on E, we can find a third one:

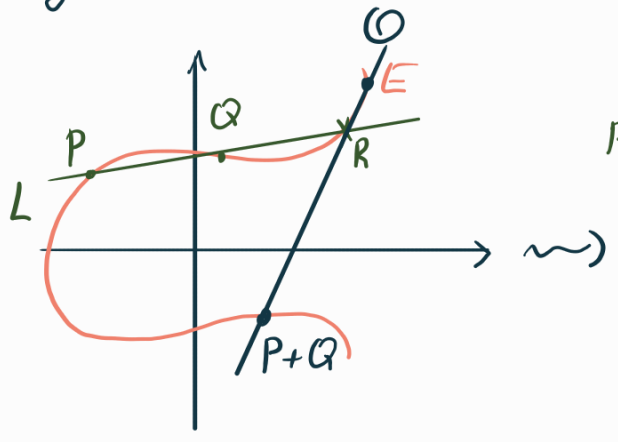


P, Q rational $\Rightarrow$ R rational

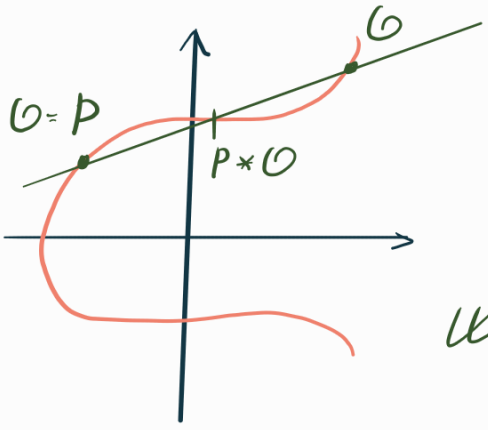
↑ line through P & Q rational

* does this form an additive gp.?
identity elem.?

Say our curve has a rational pt. $\mathcal{O}$



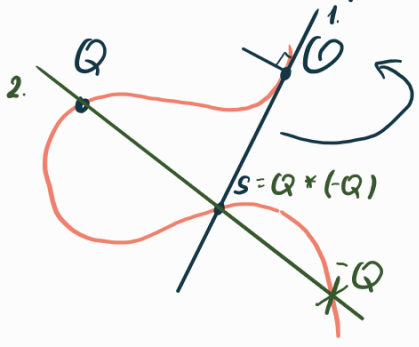
$\rightsquigarrow$



$\mathcal{O}$ identity

[Fact: $P + Q = Q + P$

inverses:



line meets $\mathcal{O}$ in two pts $\Rightarrow$ $Q - Q = \mathcal{O}$

Exercise: $(P+Q)+R = P+(Q+R)$

$\rightsquigarrow$ get an additive group

q. what if we choose another O' instead of O as identity?

$$P \longmapsto P + O'$$

is an isom. $(E, O, +) \longrightarrow (E, O', +')$, where

$$P +' Q = P + Q - O'$$

[(Mordell's thm.) If a non-singular rational plane cubic curve has a rational pt., then the gp. of rat. pts. is finitely generated.

Group law of non-singular cubic:

write eqn. in form:

$$y^2 = x^3 + ax^2 + bx + c$$

homogenize $x = \frac{X}{Z}$ $y = \frac{Y}{Z}$

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

$\rightsquigarrow$ at line $Z=0$ get $X^3 = 0$ $\rightsquigarrow$ triple root $X=0$

$\rightsquigarrow$ cubic meets line at ∞ in 3 pts.

(this pt. is a non-sing. pt.; look at the partial derivatives there)

*call this pt. O; it is a rational pt. (identity elem.)