12 September 2023

MAT 4800

<u>Affine elliptic curve:</u>

$\{(x,y)\in\mathbb{R}^2 : y^2 = x^3+1\}$

<u>(Projective) elliptic curve:</u>

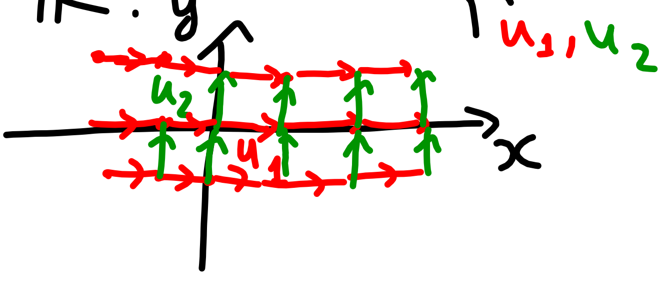
A lattice $\Gamma \subseteq \mathbb{C}$ is a set of the form:

$\Gamma_{u_1,u_2} = \{ m u_1 + n u_2 : m,n \in \mathbb{Z} \}$

Here $u_1, u_2 \in \mathbb{C}$ are ~~indep~~ linearly independent over $\mathbb{R}$.

Meaning: if $\alpha,\beta \in \mathbb{R}$, $(\alpha,\beta) \neq (0,0) \Rightarrow \alpha u_1 + \beta u_2 \neq 0$.

<u>Example:</u> $\{u_1 = 1, u_2 = i\}$ are ~~a lat~~ linearly independent over $\mathbb{R}$.



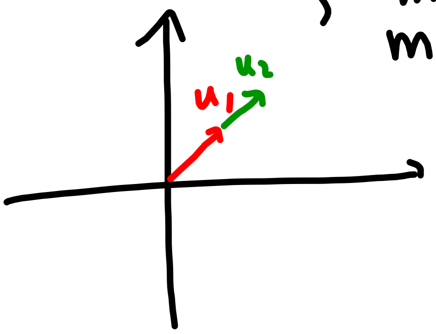
Non-example: $u_1 = 1 + i$,
$u_2 = \pi + i\pi$.

$\alpha = \pi, \beta = -1$:

$\alpha u_1 + \beta u_2 = 0$.

Not give us a lattice.

$\{ m u_1 + n u_2 : m, n \in \mathbb{Z} \}$ will belong to a line $\{x = y\}$.

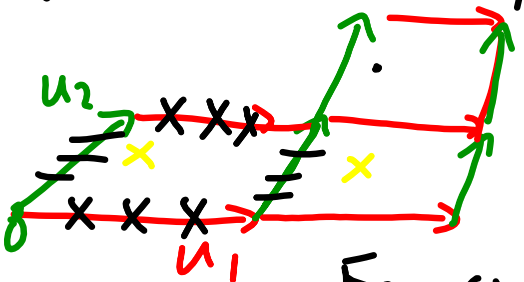


Thm: If we have a lattice Γ, we can construct a compact Riemann surface E as follows:

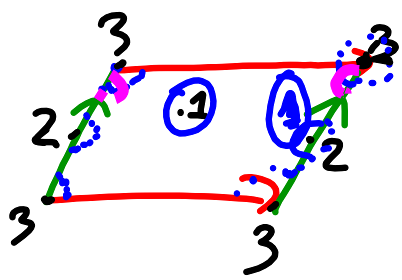
$$E = \mathbb{C} / \sim_\Gamma$$

$z_1 \sim_\Gamma z_2$ iff $z_1 - z_2 \in \Gamma$.

(Usually we write $E = \mathbb{C}/\Gamma$.)



Compactness easy: For any sequence, show that it has a subsequence that converges.



For points of type 1 (in the interior of the fundamental domain): choose a one like on the picture.

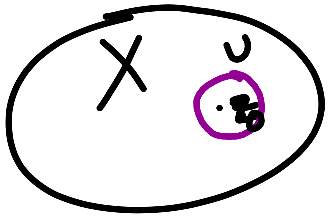
Transition function is holomorphic

(Thm: If X is a RS, $Z \subseteq X$ closed discrete set, & $f: X \setminus Z \to \mathbb{C}$ is a holomorphic function so that $\forall z \in Z$, z is not an essential singularity then f extends to $\tilde{f}: X \to \mathbb{P}^1$ holomorphically.

Z is discrete if $\forall z \in Z$, ~~an open set $U \subseteq Z$~~ then z is open set.

$\mathbb{Z}, \mathbb{N}$: discrete sets.)

Proof: Need to show only that f extends to z_0 for every $z_0 \in Z$.



$f: U \setminus \{z_0\} \to \mathbb{C}$ holomorphic.

z_0 is not essential singularity

$$\Rightarrow \begin{cases} \lim_{z \to z_0} f(z) = \alpha \leftarrow \text{finite (Case 1)} \\ \lim_{z \to z_0} |f(z)| = \infty \quad \text{(Case 2)} \end{cases}$$

Case 1: By Riemann removable singularity $\Rightarrow$ f extends to

$$\hat{f} : U \to \mathbb{C}$$
$$z_0 \mapsto \alpha$$

holomorphically.

Case 2: Claim: $\hat{f} : U \to \mathbb{P}^1$
$$z_0 \to \infty$$
is holomorphic.

Choose the coordinate chart V near $\boxed{\infty}$ given by:

$$V \to \mathbb{C}$$
$$w \mapsto \frac{1}{w}$$

We need to show that

$$g = \hat{f} : U \to \mathbb{P}^1 \to \mathbb{C}$$
$$z \to f(z) \to \frac{1}{f(z)}$$
$$z_0 \to \infty \to 0$$

is holomorphic near z_0.

$g : U \setminus z_0 \to \mathbb{C}$ is holomorphic & $\lim_{z \to z_0} g(z_0) = 0 \Rightarrow$ Riemann Removable Theorem.

<u>Example</u>: $f(z) = z^3 + 2z + 1 : \mathbb{C} \to \mathbb{C}$

~~(The funda~~

Extend to $\hat{f} : \mathbb{P}^1 \to \mathbb{P}^1$

What is the multiplicity of $\hat{f} = \infty$ at $z_0 = \infty$?

(The Fundamental Theorem of Algebra.)

Choose a chart on $\mathbb{P}^1$ which maps ∞ to 0.

$$\begin{tikzcd} z \quad U_\infty \arrow[r, "\hat{f}"] \arrow[d] & U_\infty \arrow[d] \\ w = \frac{1}{z} \arrow[r, "g = ?"'] & w = \frac{1}{z} \end{tikzcd}$$

$$g(w) = \frac{1}{f\left(\frac{1}{w}\right)} = \frac{1}{\left(\frac{1}{w}\right)^3 + \frac{2}{w} + 1} = \frac{w^3}{w^3 + 2w^2 + 1}$$

$z = \infty \iff w = 0$.

Want to know the multiplicity of the function $g(w)$ at $w = 0$.

So we need to write $g(w)$ in power series.

Geometric series:

if $|s| < 1$ then:

$$\frac{1}{1+s} = 1 - s + s^2 - s^3 + \dots$$

If $|w|$ is small then $s = w^3 + 2w^2$ satisfies $|s| < 1$

$$\frac{1}{w^3+2w^2+1} = 1 - (w^3+2w^2) + (w^3+2w^2)^2 - (w^3+2w^2)^3 + \dots$$

$$g(w) = w^3\left(1 - (w^3+2w^2) + (w^3+2w^2)^2 \dots\right)$$
$$= w^3 + \text{h.o.t.}$$

So multiplicity of $g(w)$ at $w=0$ is $3 =$ degree of f.

$$f^{-1}(\infty) = \infty.$$

Thm (local model of holomorphic functions): compact RS,

If $f : X \to Y$ holomorphic non-constant

then $\forall\, y_1, y_2$: $\# f^{-1}(y_1) = \# f^{-1}(y_2)$.

<u>Abel - Ruffini</u>: There is no formula to find roots of a general polynomial of degree at least 5.

$$az^2 + bz + c = 0 \quad (a \neq 0)$$

$$\Rightarrow \quad z_1, z_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Meaning: We can only find approximate roots of polynomials.

Even $\sqrt{2}$ cannot be precisely computed by computers.

A well known method to solve equation is Newton's method.

If you want to solve:

$$P(z) = 0.$$

You choose randomly z_0. Then you construct a sequence:

$$z_{n+1} = z_n - \frac{P(z_n)}{P'(z_n)}$$

Hope $\{z_n\}$ converges to a root of $P(z) = 0$. Sometimes it does. Sometimes it does not.

How to compute $\sqrt{2}$?

$\sqrt{2}$ is a root of $z^2 - 2 = 0$

Newton's method is:

$$z_{n+1} = z_n - \frac{z_n^2 - 2}{2 z_n}.$$

(This is how computers compute $\sqrt{2}$.)

* Come back to elliptic curve:

$$E = \mathbb{C}/\Gamma$$

<u>Q</u>: if $f : E \to \mathbb{C}$ is holomorphic must it be a constant?

(Maximum principle)

<u>Q</u>. (Abel, Jacobi, Lagrange...)

What are holomorphic functions $f : E \to \mathbb{P}^1$?

$$\begin{tikzcd} \mathbb{C} \arrow[d, "\pi"'] \arrow[dr, "F = f\circ\pi \text{ holomorphic}"] & \\ E = \mathbb{C}/\Gamma \arrow[r, "f"'] & \mathbb{P}^1 \end{tikzcd}$$

holomorphic, holomorphic

F must be doubly periodic, with periodics in Γ.

$$F(z + \gamma) = F(z) \ \forall \gamma \in \Gamma.$$

(Periodic function like $\cos(z)$ periodics are $2\pi\mathbb{Z}$)

$\cos(z+\gamma) = \cos(z)$
$\forall\, \gamma \in 2\pi\mathbb{Z}$.

Look at your HW.

<u>Weierstrass embedding for elliptic curves:</u>

$\exists$ a doubly meromorphic function
$\wp : \mathbb{C} \to \mathbb{P}^1$
$\Rightarrow \tilde{\wp} : E \to \mathbb{P}^1$ holomorphic

so that
$$E \to \mathbb{P}^2$$
$$z \longmapsto [\wp(z) ; \wp'(z) : 1]$$

gives us an embedding of E into $\mathbb{P}^2$.

Here is an algebraic description of a holomorphic function from E to $\mathbb{P}^1$:

Affine elliptic curve:

$E_{aff} : \{ y^2 = x^3 + 1 \}$

(in Weierstrass description:
$x = \wp(z)$, $y = \wp'(z)$)

In this case, Weierstrass function is:

$E_{aff} \ni (x;y) \longrightarrow x$

$$E_{aff} = \{ (x,y) \in \mathbb{C}^2 : y^2 = x^3 + 1 \}$$

$$\begin{array}{ccc} E_{aff} & & (x,y) \\ f \downarrow & & \downarrow \\ \mathbb{C} & & x \end{array} \quad \text{Weierstrass map}$$

Degree = ? $\quad 2 = f^{-1}(x_0)$

$$= \{ (x,y) \in \mathbb{C}^2 : y^2 = x^3 + 1,\ x = x_0 \}$$

$$= \# \{ y : y^2 = x_0^3 + 1 \}$$

So for most points, $\# f^{-1}(x_0) = 2$. except for some exceptional points. $\# f^{-1}(x_0) = 1$ or 0.