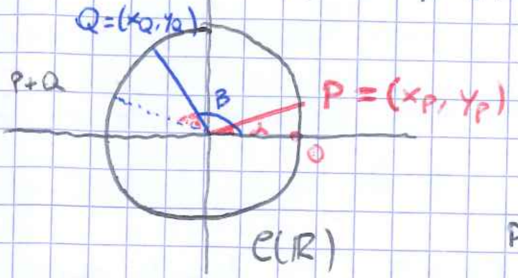
ELLIPTIC CURVES OVER $\mathbb{C}$

Roughly speaking, an elliptic curve is an algebraic curve with an "algebraic group structure" on it.

$$\mathcal{C}: x^2 + y^2 = 1.$$



$$P = (x_P, y_P) = (\cos(\alpha), \sin(\alpha))$$

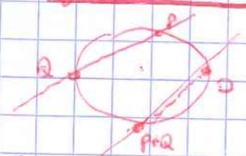
$$Q = (x_Q, y_Q) = (\cos(\beta), \sin(\beta))$$

$$P+Q = (\cos(\alpha+\beta), \sin(\alpha+\beta))$$

$$= (\cos\alpha \cos\beta - \sin\alpha \sin\beta, \sin\alpha \cos\beta + \sin\beta \cos\alpha)$$

$$= (x_P x_Q - y_P y_Q, x_Q y_P + x_P y_Q).$$

Geometric description



polynomial expressions!

The fact that the group law on $\mathcal{C}(\mathbb{R})$ is algebraic follows from the addition formulas for trigonometric functions. These also work for the holomorphic extensions $\sin, \cos : \mathbb{C} \longrightarrow \mathbb{C}$.
Since $\sin$ and $\cos$ are 2π-periodic, we get

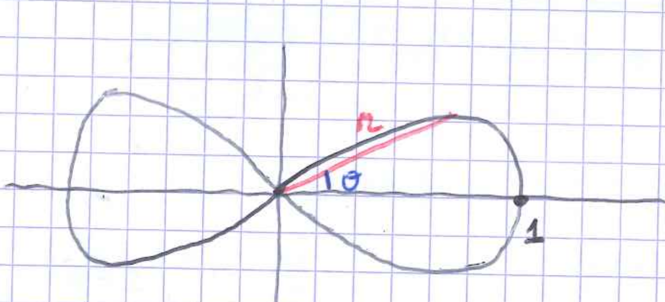
$$\longrightarrow \mathbb{C}/_{2\pi\mathbb{Z}} \xrightarrow{\sim} \mathcal{C}(\mathbb{C})$$

$$z \longmapsto (\cos z, \sin z)$$

naturally a group

group by "transport of structure".

Similar functions were discovered by Jakob Bernoulli in 1694 while studying the problem of the Paracentric Isochrone (Leibniz 1689):



Lemniscate:

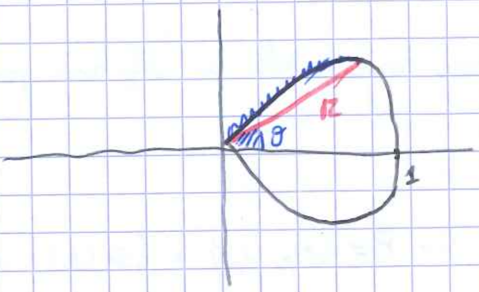
$$\begin{cases} (x^2+y^2)^2 = x^2 - y^2 \\ r^2 = \cos(2\theta) \end{cases} \leftarrow \text{polar} \quad \begin{cases} x = r\cos\theta \\ y = r\sin\theta \end{cases}$$

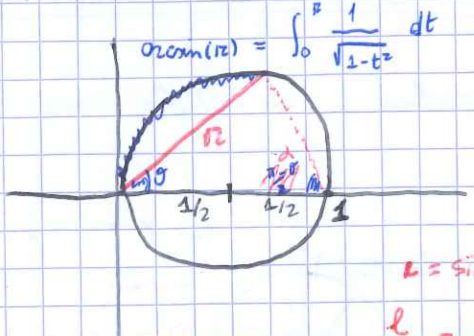
One discovers that for $0 \leq r_0 \leq 1$

arc length () $= \displaystyle\int_0^{r_0} \frac{1}{\sqrt{1-t^4}}\,dt = S(r) \in [0, \tfrac{\omega}{2}]$

↑ For $r_0 = 1$ we have $\displaystyle\int_0^1 \frac{1}{\sqrt{\dots}}\,dt = \frac{\omega}{2}$ $\quad \omega \simeq 2.622$

Analogy





$r = \sin(\alpha) \Rightarrow \alpha = \arcsin(r)$

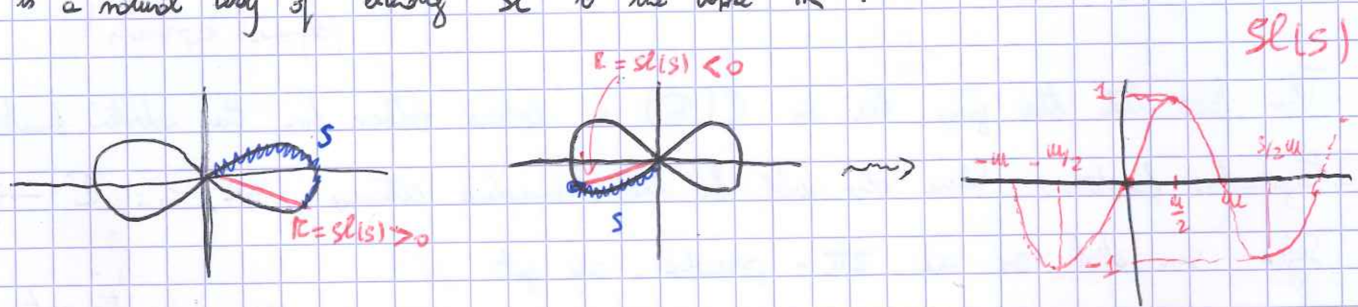
$\frac{l}{2\alpha} = \frac{\pi}{2\pi} \Rightarrow l = \alpha.$

This inspires us to consider

$$sl := S^{-1} : [0, \tfrac{\varpi}{2}] \longrightarrow [0, 1] \qquad \underline{\text{lemniscate sine}}.$$

We have : $r = sl(s) \Leftrightarrow s = \int_0^r \frac{1}{\sqrt{1-t^4}}\,dt$.

There is a natural way of extending sl to the whole $\mathbb{R}$:



$sl : \mathbb{R} \longrightarrow [-1, 1]$ periodic with period 2ϖ.

<u>Differentiability</u> : sl is infinitely differentiable and we have $sl'(s)^2 = 1 - sl^4(s)$

$(\sin^2(s) + \cos^2(s) = 1)$

<u>Addition formulas</u> :

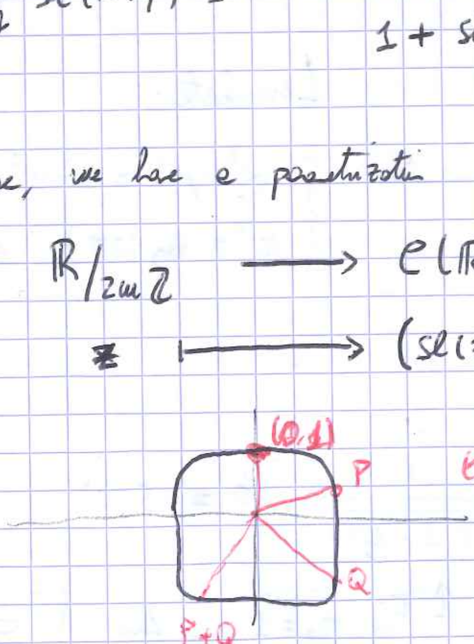
$$sl(x+y) = \frac{sl(x)\,sl'(y) + sl(y)\,sl'(x)}{1 + sl^2(x)\,sl^2(y)}$$

$(\sin(x+y) = \sin x \cos y + \sin y \cos x)$

similar formula for $sl'(x+y)$.

As in the circle case, we have a parametrization

$$\mathbb{R}/_{2\varpi\mathbb{Z}} \longrightarrow \mathcal{C}(\mathbb{R}) \qquad \mathcal{C} : y^2 = 1 - x^4$$
$$z \longmapsto (sl(z), sl'(z))$$



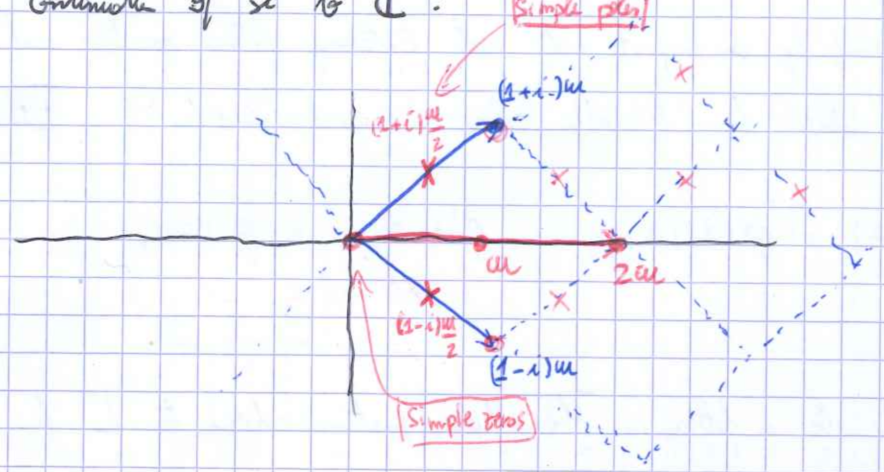
group law by transport of structure.

However, the situation becomes very different over $\mathbb{C}$: noticing that

$$\int_0^{ir} \frac{1}{\sqrt{1-t^4}}\,dt \underset{t=iu}{=} i \underbrace{\int_0^{r} \frac{1}{\sqrt{1-u^4}}\,du}_{y}$$

$r = sl(y)$. Apply sl both sides: $\underset{= i\,sl(y)}{ir} = sl(iy)$

suggests us that we could define $sl(iy) = i\,sl(y)$ $\forall y \in \mathbb{R}$. If we do this and then we apply the addition formula above to define $sl(x+iy) = sl(z)$ we obtain a meromorphic continuation of sl to $\mathbb{C}$:



Doubly periodic

Def: A lattice $L \subseteq \mathbb{C}$ is a subgroup of $\mathbb{C}$ of the form $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ where $\omega_1, \omega_2 \in \mathbb{C}$ are $\mathbb{R}$-linearly independent. An elliptic function f (wrt L) is a meromorphic function on $\mathbb{C}$ s.t

$$f(z+\omega) = f(z) \qquad \forall z \in \underset{\text{pole} + \omega = \text{pole}}{\mathbb{C}^*}, \ \omega \in L.$$

In the same spirit as with the circle, we may write a parametrization

$$\mathbb{C}/L \longrightarrow \mathcal{C}(\mathbb{C}) \cup \{P_{1,\infty}, P_{2,\infty}\}$$

$y^2 = 1-x^4$ — What is this??

$$z \bmod L \longmapsto (sl(z), sl'(z))$$

$$(1 \pm i)\frac{\varpi}{2} \longmapsto P_{1,\infty}, \ P_{2,\infty}.$$

Attention: The projective closure $\overline{\mathcal{C}} \subseteq \mathbb{P}^2_{\mathbb{C}}$ given by $y^2z^2 = z^4 - x^4$ has a unique point at infinity (with $z=0$), $P_\infty = [0:1:0]$. However, this is singular. It can be desingularized by replacing it with 2 "points" $P_{1,\infty}, P_{2,\infty}$.

We still get a projective curve but not plane anymore...

Is there a way to find a <u>plane curve</u> that is parametrised by $\mathbb{C}/L$? and that acquires an algebraic group structure via this parametrization?

<u>Def</u>: Let $L \subseteq \mathbb{C}$ be a lattice. The <u>Weierstrass $\wp$-function</u> associated to L is

$$\wp_L(z) = \frac{1}{z^2} + \sum_{\lambda \in L\setminus\{0\}} \left[\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right]$$

The above series converges uniformly on compact sets not containing lattice points and defines an elliptic function for the lattice L (double pole at each $w \in L$). ~~Thus~~ We have

$$\wp(-z) = \wp(z) \quad , \quad \wp'(-z) = -\wp'(z).$$

still elliptic function.

<u>Theorem</u>: Let $L \subseteq \mathbb{C}$ be a lattice. The elliptic functions relative to L form a field $\mathbb{C}(L)$ and we have $\mathbb{C}(L) = \mathbb{C}(\wp_L, \wp_L')$.

<u>Example</u>: For $L = (1+i)\varpi\mathbb{Z} + (1-i)\varpi\mathbb{Z}$ we have

$$sl(z) = -2\frac{\wp_L(z)}{\wp_L'(z)} \quad (1) \quad , \quad sl'(z) = \frac{4\wp_L(z)^2 - 1}{4\wp_L(z)^2 + 1}$$

Substituting this into the equation $sl'(z)^2 = 1 - sl^4(z)$ we get

$$\wp_L'(z)^4 = \wp_L(z)^2 (4\wp_L(z)^2 + 1)^2 \Rightarrow \wp_L'(z)^2 = \pm \wp_L(z)(4\wp_L(z)^2 + 1)$$

Looking at the Laurent expansion in 0 of both sides, we see that we need to choose the $+$ sign. Thus

$$\wp_L'(z)^2 = 4\wp_L(z)^3 + \wp_L(z)$$

We then have a parametrization

$$\begin{aligned} \mathbb{C}/L &\longrightarrow E(\mathbb{C}) \qquad E: y^2 = 4x^3 + x \\ 0 \neq z \bmod L &\longmapsto (\wp(z), \wp'(z)) \\ 0 \bmod L &\longmapsto \infty = [0:1:0] \end{aligned}$$

← smooth!

∎

This works more generally: writing

$$\wp_L(z) = \frac{1}{z^2} + \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^2}\left[\frac{1}{(1-z/\omega)^2} - 1\right] = \ldots$$

product of two geometric series

$$= \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1)\, G_{2k+2}\, z^{2k} \qquad \text{where} \quad G_m = \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^m}$$

$m \geq 2$.

one also obtains the Laurent series expansion for $\wp_L'(z)$. Setting

$$g_2 := 60\, G_4 \qquad \text{and} \qquad g_3 = 140\, G_6$$

← $g_2 = g_2(L)$
$g_3 = g_3(L)$.

one discovers that the function

$$\varphi(z) = (\wp_L'(z))^2 - 4(\wp_L(z))^3 + g_2\, \wp_L(z) + g_3$$

does not have poles in $\mathbb{C}$ and is 0 in 0. Liouville $\Rightarrow$ $\varphi(z) \equiv 0$.

Hence

$$\boxed{\wp_L'(z)^2 = 4\wp_L(z)^3 - g_2\, \wp_L(z) - g_3}$$

We get a complex parametrization of the projective curve

$$E: \; y^2 = 4x^3 - g_2 x - g_3.$$

← 1 point at ∞.

One can show that the discriminant $\Delta(4x^3 - g_2 x - g_3) \neq 0$. In particular this implies that E is smooth.

2

"**Def**": An <u>elliptic curve over $\mathbb{C}$</u> is the projective plane curve given by

$$y^2 = 4x^3 - Ax - B \qquad A, B \in \mathbb{C}$$

where the cubic polynomial in x does not have multiple roots (i.e. $A^3 - 27B^2 \neq 0$).

Thm ← Uniformization: $\forall A, B \in \mathbb{C}$ with $A^3 - 27B^2 \neq 0$ there exists a unique lattice $L \subseteq \mathbb{C}$ with $g_2(L) = A$, $g_3(L) = B$

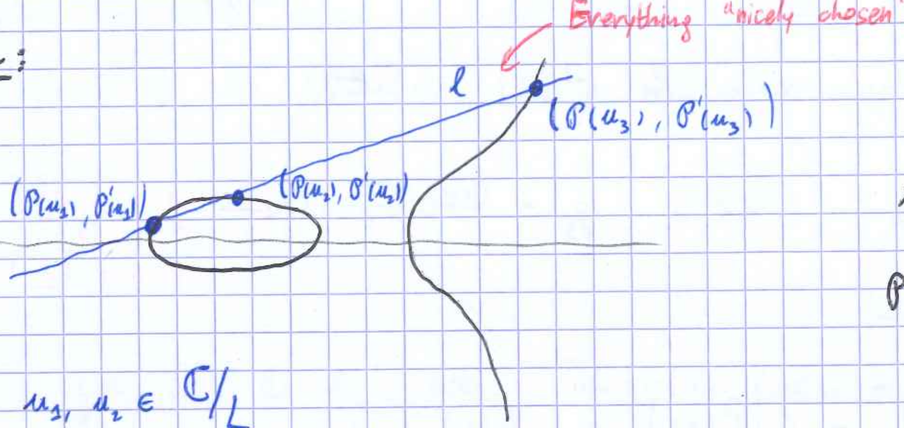
In particular, every elliptic curve $E/\mathbb{C}$ admits a complex analytic parametrization by $(\wp_L, \wp'_L)$ for some L.

Can we transport via

$$\mathbb{C}/L \xrightarrow[(\wp,\wp')]{} E(\mathbb{C})$$

the group structure on $\mathbb{C}/L$ to an algebraic group structure on $E(\mathbb{C})$? **Yes!**

Idea:



$u_1, u_2 \in \mathbb{C}/L$

If $\ell : y = ax + b$ then u_3 is a zero of $\wp'(z) - (a\wp(z) + b)$.

triple pole at 0

$\Rightarrow$ 3 zeros in $\mathbb{C}/L$

u_1, u_2, u_3

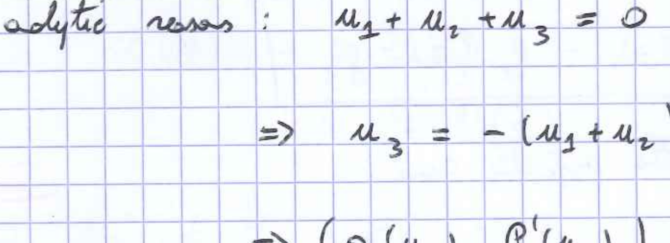
By analytic reasons: $u_1 + u_2 + u_3 = 0$ in $\mathbb{C}/L$

$$\Rightarrow u_3 = -(u_1 + u_2)$$

$$\Rightarrow (\wp(u_3), \wp'(u_3)) = (\wp(-(u_1+u_2)), \wp'(-(u_1+u_2)))$$

$$= (\wp(u_1+u_2), -\wp'(u_1+u_2))$$

$\Rightarrow (\wp(u_1+u_2), \wp'(u_1+u_2))$ is the symmetric to $(\wp(u_3), \wp'(u_3))$ wrt the x-axis.



Geometric group law

$\Rightarrow$ algebraic!

Neutral element $= [\wp(0), \wp'(0)] = \infty$
$= [0:1:0]$.