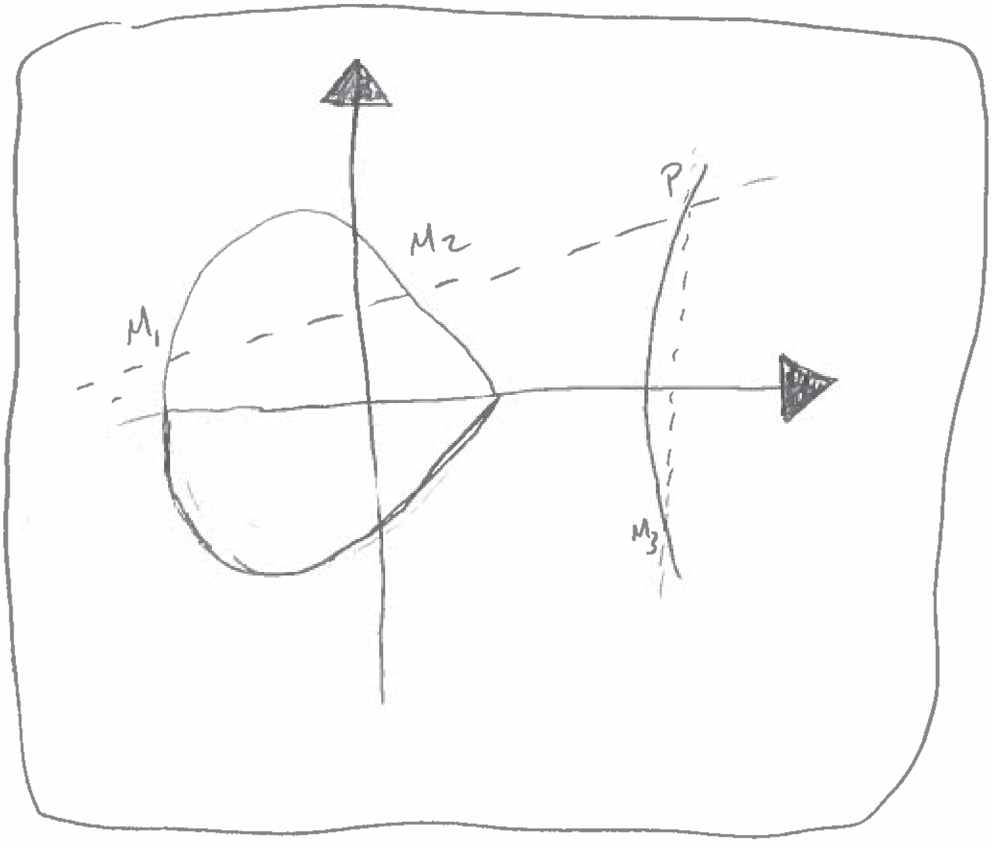
Elliptic Curves Seminar — 2017

{University of South Carolina}



[(Rob)
— Robert Vandermolen's
notes...]

PDF found here:

people.math.sc.edu/alicial/seminars/curvesS17.html

Elliptic curves Seminar : Date:

organizer : Alicia LaMarche

participants : Alicia LaMarche, Alex Duncan, Josiah Jeremiah , Kenn Sheng , Robert Vandermolen

presenter : Robert Vandermolen

---

prologue: we set our scene in the sitting room of a small jazz bar. In this room gathers a curious group of academics, sitting in leather armchairs around a table decorated with loose sheets of paper, pens, pencils, chalk, erasers, and an assortment of ~~the~~ bartender's latest experiments. The 4 walls enclosing our band into this room have chalk boards fastened to them with faint remembrance of past discussions hastily erased, as the members had slowly joined the group throughout the night.

No one there remembers ever who poses the question, yet as if calling a session of parliament to order, a dark man slumped in his seat, which is slightly back from the group lowers his drink from his lips and steps quietly to the board closest to his chair. The room slowly calms and attention is brought to him.

"So the question has been raised..."

(writing) → 'What is meant by an Elliptic Curve?'

"How should we proceed ?"

Aside: a small table is next to the chair of this now standing man with a small notebook left open next to a mechanical pencil, a bourbon pour neat and a glass ashtray with a partially smoked cigarette, still burning. In the small notebook one can see a sketch of what appears to be two spheres made from chicken wire with a creased sheet pulled tightly over the top of these spheres, we poorly reproduce it here for the curious reader:

Chapter 1: Curves

The name "Elliptic Curve" appears, by sight alone, to consist of an adjective "Elliptic" and a noun "curve". In Mathematics we all use nouns to indicate some class of objects and use the adjectives to mean some subclass. So before describing the properties which make this class elliptic let us first define the class which defines the noun.

The lexicon: we all have an intuitive meaning for the word curve, and even a loose picture which is conjured to mind when one says: "curve", a squiggle drawn on a piece of paper, I am sure:

(as our mind imagines as this piece of paper where the squiggle "lives")

as we seldom do let us begin to build our lexicon with "space" to play, for ours tonight we will mean a topological space for "space" as we are all accustomed with this vocabulary.

Motivation: As from the lexicon of our primary school education we would consider a curve as drawn (lives in) on the Carthesian plane, as a function $C: \mathbb{R} \to \mathbb{R}^2$

Thus in the topological lexicon a curve is a element of the closed sets, which is a kin to the line through some sort of mapping. As is in $\mathbb{R}$ we will say a line, and thus a curve has "dimension 1" once we equip our space with a proper topology. (and means of dimension)
Now as we all show an affinity towards algebra let us narrow this lexicon to $\mathbb{A}^n_k$ for some field k, with it's canonical Zariski topology.

- A hand rises...

let us ~~begin by~~ now recalling some basic notations of $\mathbb{A}^n_k$ and the Zariski topology

- hand lowers...

→ This discussion continues till the participants agree that they have been here long enough for one night.

→ They return the next night and a new person quickly stands and gives a speech (This presentation is given later in the notes...) how elliptic curves were motivated by integrals and ellipses, and the same problem [illegible] Riemann surfaces into their lexicon...

..... many nights later...

Chapter 2:

→[This is given w/ author's notes]

$\boxed{\text{def}^{\underline{n}}}$ let k be a field, we will denote $\mathbb{P}^{n-1}_k$ as the $(n-1)^{th}$ projective space over k, defined as $\text{Proj } k[x_1 - x_{n-1}] \subseteq \text{Spec } k[x_1 - x_{n-1}]$ where the closed sets are defined for $p \in \mathbb{P}^{n-1}_k$ as

$$V(p) = \{ x \in \mathbb{A}^n_k = \text{Spec } k[x_1 - x_n] : \hat{f} \equiv 0 \bmod x \ \ \forall f \in p \}$$

{in some lexicon these are called the projective varieties.}

→ every hand raises except the first man that stood

→ for the rest of the night they argue and the first man that stood scribbles alone in his notebook. I assume more spheres and sheets with scribbles dancing on the sheets.

"The end"

{Break}

Another night, one of participants stands in as now is the general state, yelling, children, of this room and in a scolding tone declares:

"If none of us can agree on vocabulary can we ever hope to to describe what is meant by an elliptic curve?"

name calling ensues where some participants referring to other participants chosen lexicon as sophmoric and inadequate for such a deep subject as elliptic curves.

→ This was the last night they met.

→ The man that stood first moved to a cabin far outside of town and died in his sleep when his cabin caught fire from a hastily extinguished cigarette, all of his notebooks were lost to the fire.

→ after this first man died the remaining group that felt as if their lexicon of varieties was superior to all other's lexicon decided to meet at a well lit room on campus and impress each other with this lexicon, eventually one of them wrote a book

[This is also left in the notes]

{night 2 from the string}

Elliptic Curves seminar:

presenter: Robert Vandermolen

Title: Elliptic Functions

History: "From the second half of the seventeenth century onwards, much attention was devoted to certain integrals, which, it seemed, could not be evaluated using so-called 'elementary' functions. These were known as elliptic integrals, since they included the integral

$$\int \sqrt{\frac{a^2-ex^2}{a^2-x^2}}\, dx$$

giving the circumference of the ellipse $(x^2/a^2)+(y^2/b^2)=1$, where $e=1-(b^2/a^2)$.

In the late 1790's, Gauss noticed that, just as the inverse functions of the integrals $\int \frac{dx}{1+x^2}$ and $\int \frac{dx}{\sqrt{1-x^2}}$

give simply periodic trig. functions, $\tan x$, $\sin x$ the inverse functions of certain elliptic integrals, such as

$$\int \frac{dx}{\sqrt{1-x^4}}$$ give doubly periodic

functions."

— pg. 72 "Complex Functions" – Jones & Singerman

Aside: we will be taking a diversion from the strict algebraic properties of elliptic curves and projective space, to take a more geometric view in the world of $\mathbb{C}$ instead of an arbitrary algebraically closed field.

Thank you's:

I'd like to thank all the participants of this seminar, and a special thank you to Alicia for her work in organizing and upkeep of the website.

Aside (if needed)

[The Riemann Sphere Σ] {one motivation for the name projective space}

"Joke" definition: it's the one-point compactification of the complex plane...

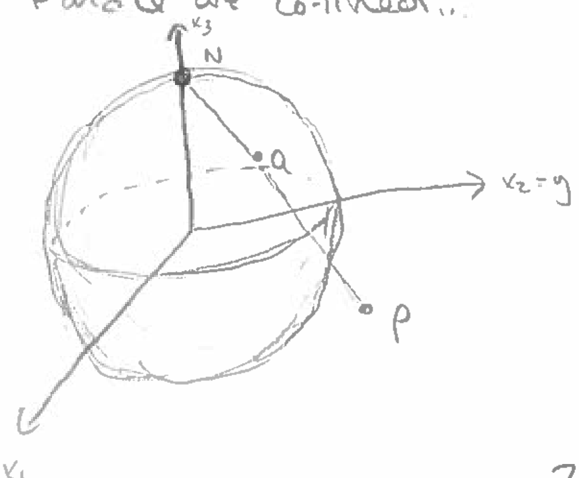
{I call this a joke because it sort of feels like the "joke" definition of a group being: "is a groupoid with one object"}

{yet let's present the presentation that I believe motivates the word projective}

(all from "complex functions" by Jones and Singerman)

The stereographic projection of the complex plane:

Consider the 2-sphere $S^2 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1^2 + x_2^2 + x_3^2 = 1\}$ in $\mathbb{R}^3$ and identify the complex plane $\mathbb{C}$ w/ the plane $x_3 = 0$, by identifying $z = x + iy$ $(x, y \in \mathbb{R})$ with $(x, y, 0)$ for all $z \in \mathbb{C}$. Denote $N = (0,0,1)$ as the "North Pole" of S^2 then the stereographic projection from N gives a bijective map $\pi : S^2 \setminus \{N\} \to \mathbb{C}$, defined by $Q \mapsto P$, where $P \in \mathbb{C}$, $Q \in S^2 \setminus \{N\}$, and P and Q are co-linear...



* if homeomorphic's details are wanted do that too *

$$\left\{ \Sigma := \mathbb{C} \cup \{\infty\} \cong S^2 \right\}$$

- Thus we have our motivation for our first definition.

Riemann Sphere...

def^n A meromorphic function $f: \mathbb{C} \to \Sigma$ is elliptic with respect to a lattice $\Omega \subseteq \mathbb{C}$ when f is doubly periodic w/ respect to Ω, that is, when

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

So that each $\omega \in \Omega$ is a period of f.

* [define lattice] * [define doubly periodic]
* [define meromorphic]
* [define/talk about Σ] (it's just projective space..) previous page "Aside"

* for this page just say "Recall Jeremiah's presentation" *

Question: given a lattice $\Omega \subseteq \mathbb{C}$ can we make an elliptic function, which is doubly periodic w/ respect to Ω?

Answer: yes!

only non-zero

(*) prove convergence?

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega}{}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

→ now in foresight, we will be investigating the relationship between $\wp(z)$ and $\wp'(z)$, so it is helpful to explore this derivative further...

→ (*) yet first we will prove convergence and zeros and poles:
(well this entails going into lattices too much...)

→ So I'd have to just tell you all this as "Facts"

To see said "Facts" look at Southwick notes on-line

here oh... here!

people.math.sc.edu/alicia/seminar/...

As Requested:

How is a complex elliptic curve a Torus: people.math.sc.edu/alitzel/seminar/tan517.html

So from the "facts" given last time we have that an elliptic curve is for a choice of lattice Ω

$$E := \{(x,y) \in \mathbb{C} \times \mathbb{C} : y^2 = 4x^3 - g_2 x - g_3\} \approx \{(\wp(z), \wp'(z)) : z \in \mathbb{C}\}$$ Fact (4)

leave on the board!

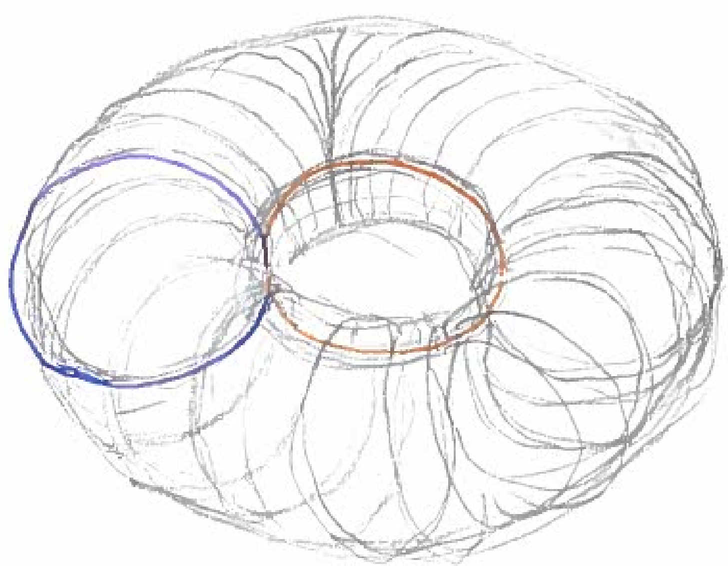
So first what's a Torus?

- A Donut (well, the surface of a donut!)

One drawing "people" "always" draw:

(The one I'll draw on the board)

My favorite:



Note it's $S^1 \times S^1$

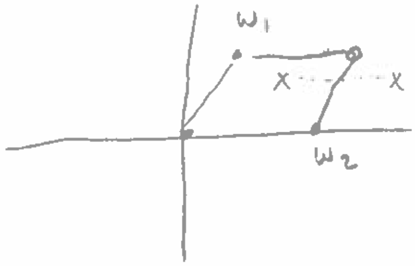
{circle} x {circle}

∴ Claim:

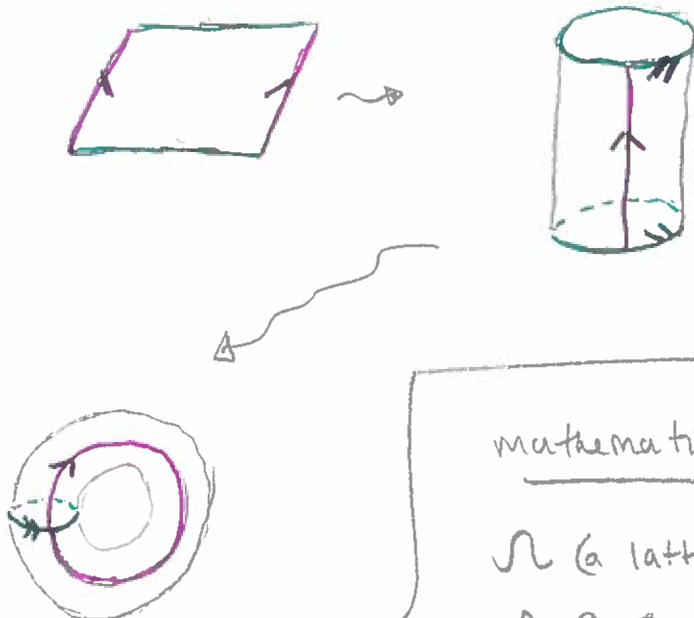
$T := S^1 \times S^1 \cong \mathbb{C}/\Lambda$ for Λ a lattice

* explain here how to parameterize the inside of this "block"

pictorially:



So



mathematically:

Λ (a lattice) is subgroup under addition of $\mathbb{C}$ so $\mathbb{C}/\Lambda$ makes sense as a group under addition (all subgroups are normal)

So to build the isomorphism just parameterize S^1 by $\theta_i \in [0, 2\pi)$

then $(\theta_1, \theta_2) \longmapsto g(\theta_1)\omega_1 + g(\theta_2)\omega_2$ [ω_1 and ω_2 generate Λ]

where $g : [0, 2\pi) \to [0, 1)$, as $\theta \mapsto \frac{\theta}{2\pi}$

which is clearly an isomorphism and hence our mapping is!

---

and hence $\mathbb{C}/\Lambda \cong E$ $\boxed{\text{what?}}$

well using fact (*) [still on board!]

$\wp(z)$ is 1-1 w/ $\mathbb{C}/\Lambda$ since doubly periodic

My question: how is this the definition of elliptic curve that Alicia gave on the First day?

Recall: (from Alicia) [from the first day]
↳ people.math.sc.edu/allicial/seminars/curvesS17.html

def$^{\underline{n}}$) "An elliptic curve is a smooth projective curve of genus 1"
↳ w/ a specified point $\mathcal{O}$ ← she wrote this all over her notes!

---

let us unpack this definition in our case:

def$^{\underline{n}}$ A curve in a topological space, is a closed subset with dimension 1

{ one quickly notices that the definition of curve changes as one changes their definition of dimension... }
* but using our standard one (homeomorphic to a unit) we get it's 1-dim for the torus over $\mathbb{C}$ *

def$^{\underline{n}}$ A projective curve is a curve where one's topological space is projective.

{ notice the space we have been in for these examples is Σ - the Riemann Sphere i.e. $\mathbb{P}^1_{\mathbb{C}}$ ... } * if you haven't talk about this...

"colloquial" def$^{\underline{n}}$ The genus of a torus is the number of "holes"...

{ i.e. the Torus has genus 1! }

$\underline{\text{def}^{\underline{n}}}$ A smooth curve is one that is infinitely differentiable.

{note our $\wp(z)$ has this property...
thus E has this property!}

---

* So our curve $E = \{(x,y) \in \Sigma \times \Sigma : y^2 = 4x^3 - g_2x - g_3\}$ *
is indeed an elliptic curve!

{note: our specified point is the 1 @ infinity!}

[* describe "think" it now one may has dimension 2, but not over $\mathbb{C}$ *]

So let's generalize this idea (and get what an elliptic curve "is")

what do we want/need:

want:

for the curve to still be defined by a cubic polynomial

like:

"$y^2 = x^3 + ax + b$"

what about the need...