Elliptic functions and elliptic curves: 1840-1870

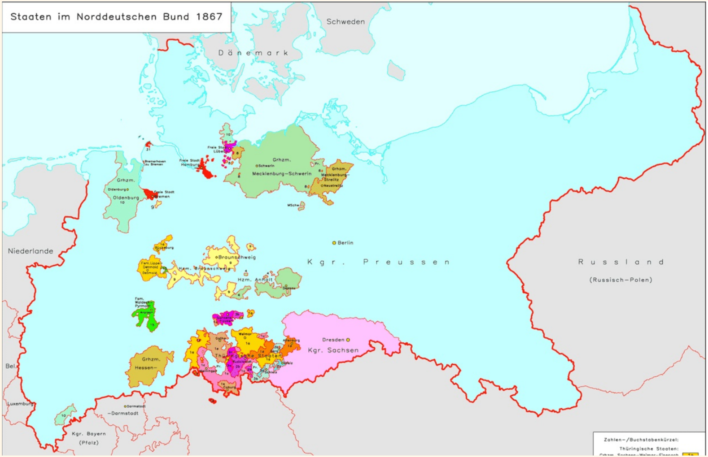
2017

Structure

1. Ten minutes context of mathematics in the 19th century
2. Brief reminder of results of the last lecture
3. Weierstrass on elliptic functions and elliptic curves.
4. Riemann on elliptic functions

Guide: Stillwell, *Mathematics and its History*, third ed, Ch. 15-16.

Map of Prussia 1867: the center of the world of mathematics



The reform of the universities in Prussia after 1815

Inspired by Wilhelm von Humboldt (1767-1835)

Education based on neo-humanistic ideals: academic freedom, pure research, Bildung, etc. Anti-French.

Systematic policy for appointing researchers as university professors. Research often shared in lectures to advanced students ("seminarium")

Students who finished at universities could get jobs at Gymnasia and continue with scientific research

This system made Germany the center of the mathematical world until 1933.

Personal memory (1983-1984)

Otto Neugebauer (1899-1990), manager of the Göttingen Mathematical Institute in 1933, when the Nazis took over.

Structure of this series of lectures

ellipse: Apollonius of Perga ($y^2 = px - \frac{p}{d}x^2$, something misses = Greek: elleipei)

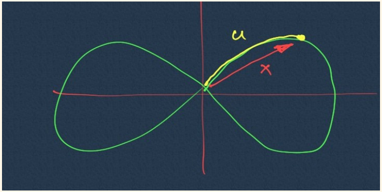
elliptic integrals, arc-length of an ellipse; also arc length of lemniscate

elliptic functions: inverses of such integrals

elliptic curves: curves of genus 1 (what this means will become clear)

Results from the previous lecture by Steven Wepster: Elliptic functions

we start with lemniscate



$(x^2 + y^2)^2 = x^2 - y^2$

polar coordinates $r^2 = cos 2\theta$

Arc length is elliptic integral
$$u(x) = \int_0^x \frac{dt}{\sqrt{1 - t^4}}$$

Elliptic function $x(u) = sl(u)$ periodic with period 2ω length of lemniscate.

"sin lemn"

Some more results from $u(x) = \int_0^x \frac{dt}{\sqrt{1-t^4}}$, $x(u) = sl(u)$

$sl(u(x)) = x$ so $sl'(u(x)) \cdot u'(x) = 1$ so

$sl'(u) = \frac{1}{u'(x)} = \sqrt{1-x^4} = \sqrt{1-sl(u)^4}$

In modern terms, this provides a parametrisation
$x = sl(u), y = sl'(u)$
for the curve $y = \sqrt{1-x^4}$, $y^2 = (1-x^4)$.

Note that this (elliptic) curve is not the same as the lemniscate.

Some more results from $u(x) = \int_0^x \frac{dt}{\sqrt{1-t^4}}$, $x(u) = sl(u)$

Addition theorem (Euler, using some very clever substitution):

$$\int_0^x \frac{dt}{\sqrt{1-t^4}} + \int_0^y \frac{dt}{\sqrt{1-t^4}} = \int_0^z \frac{dt}{\sqrt{1-t^4}}$$

with $z = \dfrac{x\sqrt{1-y^4} + y\sqrt{1-x^4}}{1+x^2y^2}$

This translates into property $sl(u+v) = \dfrac{sl(u)sl'(v) + sl(v)sl'(u)}{1+sl(u)^2 sl(v)^2}$.

compare $\sin(u+v) = \sin u \cos v + sinv \cos u$.

Carl Friedrich Gauss (1777-1855).

WEIRD (for me): Double periodicity (Gauss)

Magic Play with integrals:

$$\int_0^{ix} \frac{d(t)}{\sqrt{1-t^4}} = \int_0^{ix} \frac{d(iz)}{\sqrt{1-(iz)^4}} = i\int_0^{x} \frac{d(z)}{\sqrt{1-z^4}}$$

Therefote if $sl(u) = x$, then $sl(iu) = ix$.

So $sl(iu + 2i\omega) = i \cdot sl(u + 2\omega) = i \cdot sl(u) = sl(iu)$, hence there is a second period $2i\omega$.

What does this mean, if anything, for a non-genius?
See also Abel. In the mid-nineteenth century, complex function theory developed. We will assume that all functions are defined on the complex plane.

Karl Weierstrass (1815-1897).

Weierstrass, 1867, Vorlesungen über die Theorie der elliptischen Funktionen (1863), in published form (1915) 322 pages. Algebraic approach.

1. Start with $\int \frac{ds}{\sqrt{P(s)}}$ with $P(s)$ any polynomial of degree 3 or 4 without quadratic factor, s complex.
By a suitable transformation $s = \frac{at+b}{ct+d}$ this can be transformed to $\int \frac{dt}{\sqrt{4t^3 - g_2 t - g_3}}$ for constants g_2, g_3.

PAUSE: EXERCISE.

Put $u(x) = \int_{x_0}^{x} \frac{dt}{\sqrt{4t^3 - g_2 t - g_3}}$.

Suppose that the inverse function $x(u)$ exists (this is an elliptic function).

Try to compute $\frac{dx(u)}{du}$ and find a differential equation for it.

Hint: differentiate $x(u(x)) = x$.

Weierstrass, 1867, Vorlesungen über die Theorie der elliptischen Funktionen (1863).

2. Put $u = \int_{x_0}^{x} \frac{dt}{\sqrt{4t^3 - g_2 t - g_3}}$ then the inverse x(u) satisfies the differential equation $(\frac{dx}{du})^2 = 4x^3 - g_2 x - g_3$ as above (for the lemniscate integral).

Weierstrass, 1867, ctd. Introduction of the P-function (German form: $\wp$).

3. Trick: put $z(u) = \frac{1}{x(u)}$, then $(\frac{dz}{du})^2 = 4z - g_2 z^3 - g_3 z^4$.

Now take the solution $z(u)$ such that $z(0) = 0$. This can be developed in a power series of the form $z = u^2 + c_4 u^4 + \dots$.

Weierstrass now defines $\wp(u) = 1/z(u)$ and shows $\wp(u) = \frac{1}{u^2} + \frac{1}{20} g_2 u^2 + \frac{1}{28} g_3 u^4 + \dots$. We now have an elliptic function! The $\wp$-function is Weierstrass's main elliptic function, the basis of his theory.

Note: $x(u) = \wp(u)$ is a solution of $(\frac{dx}{du})^2 = 4x^3 - g_2 x - g_3$. Therefore in modern terms, $x = \wp(u), y = \wp'(u)$ is a parametrisation of $y^2 = 4x^3 - g_2 x - g_3$. Weierstrass does not mention curves.

Weierstrass, 1867, ctd. Very rich but complicated material.

4. From the integral, Weierstrass also finds (by the right substitution of variables) an "addition theorem" of the following form (p. 25).

$$\wp(u+v) = \frac{(\wp u + \wp v)(2\wp u \wp v - \frac{1}{2}g_3) - g_2 - \wp' u \cdot \wp' v}{2(\wp u - \wp v)^2}$$

5. Weierstrass shows that the $\wp$ function is periodic with periods $2\omega_1$ and $2\omega_2$. The periods are found as follows:

$\wp\omega_1 = e_1$ and $\wp\omega_2 = e_2$ with e_1 and e_2 two of the zeroes of the polynomial, i.e.
$4x^3 - g_2 x - g_3 = 4(x - e_1)(x - e_2)(x - e_3)$.

Weierstrass, 1867, ctd. Very rich but complicated material.

4. From the integral, Weierstrass also finds (by the right substitution of variables) an "addition theorem" of the following form (p. 25).

$$\wp(u+v) = \frac{(\wp u + \wp v)(2\wp u \wp v - \frac{1}{2}g_3) - g_2 - \wp' u \cdot \wp' v}{2(\wp u - \wp v)^2}$$

5. Weierstrass shows that the $\wp$ function is periodic with periods $2\omega_1$ and $2\omega_2$. The periods are found as follows:

$\wp\omega_1 = e_1$ and $\wp\omega_2 = e_2$ with e_1 and e_2 two of the zeroes of the polynomial, i.e.
$4x^3 - g_2 x - g_3 = 4(x - e_1)(x - e_2)(x - e_3)$.
Does the choice matter?

Weierstrass, 1867, ctd.

6. Weierstrass shows in complicated ways (p. 120)

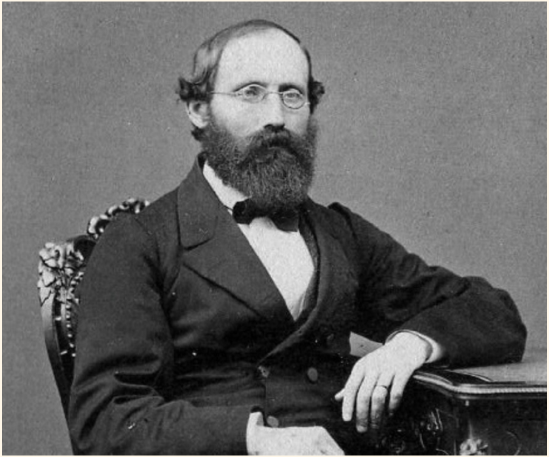
$$\wp u = \frac{1}{u^2} + \Sigma\left(\frac{1}{(u - 2m\omega_1 - 2n\omega_2)^2} - \frac{1}{(2m\omega_1 + 2n\omega_2)^2}\right)$$

where the summation is over all integer pairs m, n which are not both zero. From this one can see (again!) that $\wp$ is doubly periodic.

And there is a lot more!

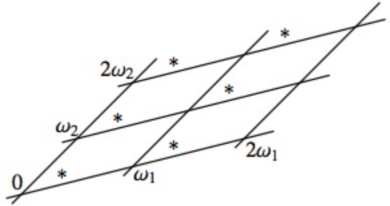
All of this must have been true but dry lectures. Lots of analytic work, little or no geometric insight.

Bernhard Riemann (1826-1866).



Riemann's geometric interpretation of elliptic functions.

Modern preliminary remark:



Since the elliptic functions are doubly periodic with periods ω_1 and ω_2, one can regard them as functions defined on the surface of a torus.

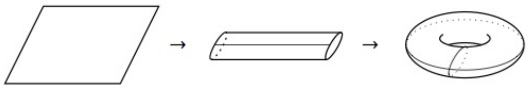
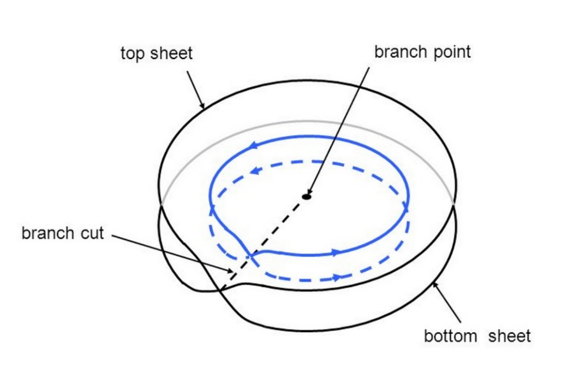


Figure 16.3: Construction of a torus by pasting

Riemann's idea of a Riemann surface for complex differentiable functions (in his 1851 dissertation).

Example: how to extend $z \to \sqrt{z}$ to a (single-valued) continuous function.



Riemann's idea of a Riemann surface.

Example: how to extend $z \to \sqrt{z}$ to a (single-valued) continuous function.

Make domain consisting of two copies A and B of $\mathbb{C}$ with a "slit" running from 0 to infinity along the negative real axis.
On A put $f(re^{i\phi}) = \sqrt{r}e^{i\phi/2}$. On B put $f(re^{i\phi}) = -\sqrt{r}e^{i\phi/2}$.

"Paste" the slit of A to B and the slit of B to A.

Then f is continuous on the new domain.

0 is called branch point, the slit a branch cut.
On A $\sqrt{1} = 1, \sqrt{-1} = i$, $f(z) = \sqrt{z}$. On B, $\sqrt{1} = -1, \sqrt{-1} = -i$, $f(z) = -\sqrt{z}$.

Notes.

1. This is Riemann's idea of a Riemann surface in his 1851 dissertation (a domain of a function, not the image of a multi-valued function).
2. The "slit" can also leave the branch point in any direction you like if you define the function in an appropriate way.
3. The same surface can be used for functions of $\sqrt{z}$. for example $\frac{1}{\sqrt{z}}$.

Example of 2: another "square root", continuous function $f(z)$ such that $f(z) = z^2$, "slit" positive imaginary axis: two sheets A and B

On A put $f(re^{i\phi}) = \sqrt{r}e^{i\frac{\phi}{2}}$ for $-\pi < \phi \leq \frac{\pi}{2}$
$f(re^{i\phi}) = \sqrt{r}e^{i(\frac{\phi}{2}-\pi)}$ for $-\frac{\pi}{2} < \phi \leq \pi$.

On B put the opposite
$f(re^{i\phi}) = \sqrt{r}e^{i(\frac{\phi}{2}-\pi)}$ for $-\pi < \phi \leq \frac{\pi}{2}$
$f(re^{i\phi}) = \sqrt{r}e^{i(\frac{\phi}{2})}$ for $-\frac{\pi}{2} < \phi \leq \pi$.

Riemann surface and ∞.

One point ∞ is added to the complex plane.
To study $f(z)$ near $z = \infty$, look at $f(1/w)$ near w=0.

For $f(z) = \sqrt{z}$, $f(1/w) = \frac{1}{\sqrt{w}}$ so ∞ is another branch point for $\sqrt{z}$.

The complex plain plus the point at infinity can be visualized as a sphere.

End of example: Riemann surface for $\sqrt{z}$.

The Riemann surface for $\sqrt{z}$ is two spheres, patched together along the slit from 0 to ∞.

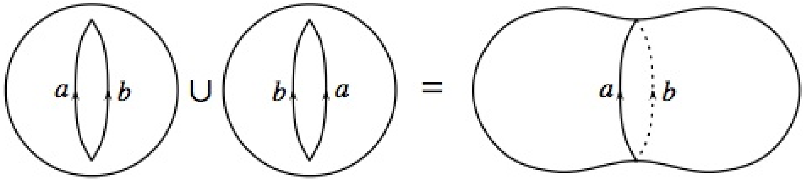


Figure 15.10: Joining the separated sheets

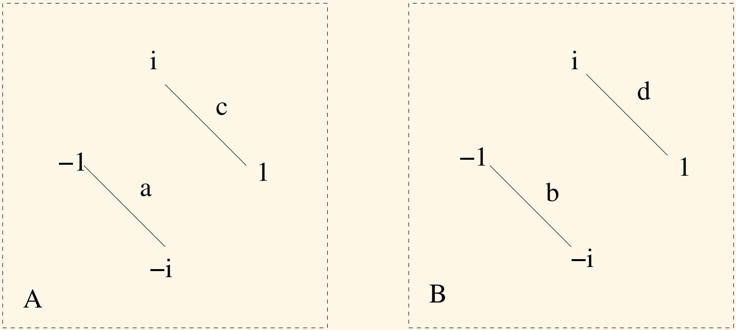
Double periodicity of elliptic functions, as seen by means of Riemann surfaces. Example: sl(u).

If $u = \int_0^x \dfrac{dt}{\sqrt{1-t^4}}$,then $x = sl(u)$

(Cauchy's theorem) Integral $\int_0^x \frac{dt}{\sqrt{1-t^4}}$ along two (decent) paths from 0 to x is the same, if $f(t) = \frac{1}{\sqrt{1-t^4}}$ is everywhere complex differentiable in the interior and if the two paths are contractable to one point.
Problems: zeros of $1 - t^4$, and square root is not continuous everywhere.

Riemann surface of $f(t) = \frac{1}{\sqrt{1-t^4}}$

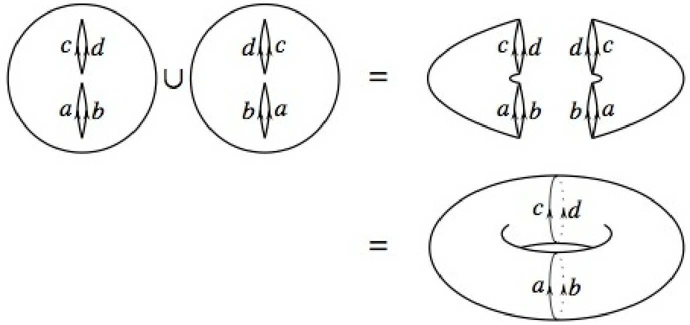
Two sheets A and B, with branch points (1, i, -1, -i) (where the function is just like $\frac{1}{\sqrt{z}}$ at $z = 0$), and two slits from 1 to i and from -1 to -i. A and B are pasted together at these slits.



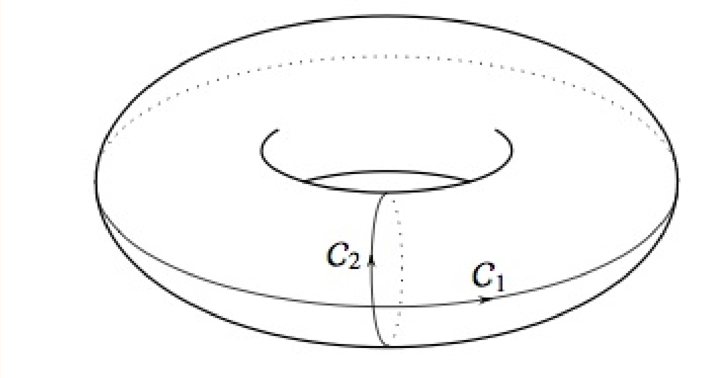
One has to integrate f on this domain. *Note: slit a and b are not pasted together, but slit a is pasted to an open boundary of B from which slit b is deleted, etc. and b is pasted to an open boundary of a from which slit A is deleted.*

Riemann surface of $f(t) = \frac{1}{\sqrt{1-t^4}}$

Torus.



Riemann surface of $f(t) = \frac{1}{\sqrt{1-t^4}}$: Paths from 0 to x



to any path from 0 to x, one can add a extra path like C_1, and a extra path like C_2.
Therefore, if $x = sl(u)$, then also $x = sl(u + \omega_1)$ and $x = sl(u + \omega_2)$ where
$\omega_i = \int_{\mathcal{C}_i} \frac{dt}{\sqrt{1-t^4}}$.
These extra paths can also be added multiple times, and in both directions, so $sl(u) = sl(u + m\omega_1 + n\omega_2)$ for integers m, n.

PAUSE: EXERCISE on the Riemann surface of $f(t) = \frac{1}{\sqrt{1-t^4}}$

Draw two curves C_1 and C_2 on the torus in the two sheets A and B of the Riemann surface.

Riemann surface of $f(t) = \frac{1}{\sqrt{4t^3 - g_2 t - g_3}}$

Also a torus (the three branch points are the zeros of the polynomial, the fourth branch point is at infinity).
Hence also periodicity of Weierstrass's $\wp$- function can be seen without any work.

Summary and later history

For "elliptic curves" we have

- parametrisation: $x = sl(u), y = sl'(u)$ for $y^2 = (1 - x^4)$, $x = \wp(u), y = \wp'(u)$ for $y^2 = 4x^3 - g_2 x - g_3$.
- Riemann surface is a torus. This property was later used to define elliptic curves.
- Addition theorem returned later in "group structure" on the curve (starting with investigations by Clebsch, 1860s.)
- Also for finite fields; much more modern theory, now also many applications in cryptography
- I do not know who first used the name "elliptic curves"

“So what”? Or: why I like this story.

- Contrasting mathematical styles (algebraic, geometric) and interplay between these styles.
- As a non-genius one can try to understand the work of some genius (Gauss, Riemann) and the reactions on it.
- Pure mathematics (elliptic curves) can be important in later applications (cryptography) after a long time (> 100 y.).
- It makes sense to invest in science! (German success story)
- Harold Edwards, “A normal form for elliptic curves” *Bull. Am. Math. Soc.* 44 (2007), 393-422, new math inspired by history.

“So what”? More.

- Changing contexts (compare goals/intentions of Bernoullis, Gauss, Abel, Weierstrass etc)
- Shifting focus on mathematical objects: construction, arc length, addition theorems, inverse functions, periodicity, series, Riemann surfaces, parametrisation of curves
- ...
- ...

A modern distorted view of history, from a course on elliptic functions (1999).

1. INTRODUCTION

In integral calculus, one considers various functions that are somewhat arbitrarily defined as inverses to standard functions like the sine and cosine and their hyperbolic analogues because they have the pleasant property of furnishing primitive functions for algebraic integrals like $\int \frac{dt}{\sqrt{1-t^2}}$ and $\int \frac{dt}{\sqrt{1+t^2}}$. These functions enlarge the class of integrals that can be computed explicitly, albeit in the form of inverses to transcendental functions. The kind of integral that arises when one allows the integrand to contain expressions of the form $\sqrt{f(t)}$, where $f(t)$ is a polynomial of degree 3 or 4, is called *elliptic*. Primitive functions for such integrals can be obtained in the form of inverses to so-called *elliptic functions*. In this section we describe this extension of integral calculus and show that the situation is very much similar to the more familiar case of the inverse trigonometric functions that occurs when f has degree 2. This similarity extends to number theoretic aspects of the

Sources and readings 1

General: John Stillwell, *Mathematics and its History*, third edition, New York 2010, Ch. 15-16. See for the historical justification of the lecture also Felix Klein, *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert* ed. R. Courant und O. Neugebauer, Berlin 1926, p. 257.
Jeremy Gray, *The real and the complex: a history of analysis in the 19th century* see Ch. 16, Ch. 17.3 (to be used with some caution).
More technicalities are found in the chapter on elliptic functions and curves in Jean Dieudonné, *Abrégé d'histoire des mathématiques* 1700-1900, Paris 1978, vol. 2, pp. 1-72.

Sources and readings 2

Weierstrass: His *Vorlesungen über die Theorie der elliptischen Functionen* (Berlin 1915) is vol. 5 in his *Mathematische Werke*, available online.

Riemann: The dissertation "Grundlagen für eine allgemeine Theorie der Functionen einer veränderlichen complexen Grösse" (Göttingen 1851) is contained in the collected works and also available online in a transcription by D.R.Wilkins.

Elliptic functions in H. Stahl, *Elliptische Funktionen*: Vorlesungen von B. Riemann. Leipzig: Teubner, 1899 (not contained in Riemann's Complete Works, but available online).

A nice visualisation of Riemann surfaces is http://slideplayer.com/slide/10930265/

Students who really cannot read German (because they do not know Dutch) and who wish to read some Riemann can consult the 19-th century English translations ofhis lecture "Über die Hypothesen, welche der Geometrie zu Grunde liegen" (1854) by W. K. Clifford, available online at http://www.maths.tcd.ie/pub/HistMath/People/Riemann/Geom/

Download this presentation

www.jphogendijk.nl/talks/elliptic2.pdf